

# IITM Journal of Management and IT

## SOUVENIR

### National Conference on Emerging Trends in Information Technology- Cyber Security: A Panoramic View

Volume 6

Issue 1

January-June, 2015

## CONTENTS

### Research Papers & Articles

	Page No.
● FIRE: Firefox for Computer Society Incident Reporting and Coordination - <i>Ashutosh Bahuguna</i>	3-11
● Nine Steps to Indian Security, Confidentiality Privacy & Technology in Cyber Space - <i>Rajiv Kumar Singh</i>	12-16
● Security Vulnerabilities in 'Future of the Web' - IPv6 Protocol Suite - <i>Navneet Kaur Popli, Anup Girdhar</i>	17-20
● A Study to Examine Cyber Forensic: Trends and Patterns in India - <i>Shruti Verma, Saurbh Mehta</i>	21-25
● General View on the Aspects of Cryptography - <i>Amit Kumar, Sonia Kumari</i>	26-32
● A Scalable Server Architecture for Mobile Presence Services in Social Network Applications - <i>A. Radha Krishna, K. Chandra Sekharaiah</i>	33-39
● "Aadhar" Management System - <i>Ameer Ulla Siddiqui, Hare Krishna Singh</i>	40-43
● A Survey on Honeypots Security - <i>Sonia Kumari, Amit Kumar</i>	44-50
● Security Features of User's Online Social Networks - <i>A. Radha Krishna, K. Chandra Sekharaiah</i>	51-58
● Cyber Security in India: Problems and Prospects - <i>Sushma Devi, Mohd. Aarif Rather</i>	59-68
● An Analysis on Improvement of Website Ranking Using Joomla - <i>Kirti Nigam, Satyam Saxena, Nargish Gupta</i>	69-72
● Network Security - Authentication Methods and Firewall - <i>Minal Dhankar</i>	73-79

	Page No.
● Cyber Security in Biometrics Using Fingerprints - <i>Priyanka Rattan, Ritika Kapoor</i>	80-85
● The Online Murder: Death via Hacked Internet Connected Technologies - <i>Nishtha Girotra, Raghunatha Sethupathy</i>	86-89
● Future Towards Danger: The Terror of Cyber Attacks - <i>Kanika Sharma, Tanvi Bhalla</i>	90-94
● Method for Storing User Password Securely - <i>Gunjan Jha, Navneet Popli</i>	95-99
● Security Issues in Bluetooth Technology - A Review - <i>Menal Dr., Sumeet Gill</i>	100-103
● Detection of Terrorism Activities Using Face Recognition Technique - <i>Garima Bhatia, Mansi</i>	104-111
● Cloud Security: A Concerning Issue - <i>Apurva Aggarwal, Shalini Sharma</i>	112-115
● Hand Recognition System Design - <i>Harleen Kaur, Simranjeet Kaur</i>	116-119
● Infrared Thermal Imaging - <i>Amit Sharma, Nidhi Jindal</i>	120-122
● Cyber Forensic: Introducing A New Approach to Studying Cyber Forensic and Various Tools to Prevent Cybercrimes - <i>B. Vanlasiama, Nitesh Jha</i>	123-128
● Cybercrime and Information Warfare - The New Arenas for WAR - <i>Anwesha Pathak, Rohit Sharma</i>	129-134
● Legislation Vulnerabilities, Threats and Counter Measures in Wireless Network Security - <i>Kushagra Dhingra, Ankit Verma</i>	135-139
● Cyber Ethics in Security Application in The Modern Era of Internet - <i>Megha Sharma, Sanchit Mittal, Ankit Verma</i>	140-143
● Comparison of AES and DES - <i>Shruti Kumari, Gautam Kumar</i>	144-146
● Social Networking Security Loopholes - <i>Shelly Taneja, Shalini Rawat</i>	147-151
● Cloud Computing: Vulnerabilities, Privacy and Legislation - <i>Amit Kiran, Priyam Lizmay Cherian</i>	152-156
● The Exigency in Accretion of Cyber Warfare Legislation - <i>Raman Solanki, Ankit Verma</i>	157-163
● Cyber Terrorism - An International Phenomena and An Eminent Threat - <i>Binny Pal Singh, Ankit Verma</i>	164-168

# FIRe: Firefox for Computer Security Incident Reporting and Coordination

Ashutosh Bahuguna\*

---

## Abstract

Information Security breaches are on the increase and adversaries are regularly coming up with new tools and techniques to compromise the information infrastructure. Effective incident information sharing and coordination during incident resolution is crucial for thwarting the cyber attack and protecting the critical assets of organization and nation. It is observed from the current means and methods employed by various national Computer Security Incident Response Teams (CSIRT) and Information Sharing and Analysis Centers (ISAC) that there is need for improvement in the incident reporting and coordination means & methods, relying only few available means like unsecured email communication is insufficient in countering cyber attacks. FIRe (Firefox for Incident Reporting) is developed to provide reporting organization, a single window solution for incident reporting & coordination activities with CSIRTs (National & Sectoral) during incident resolution process. FIRe is a customized Firefox browser with extensions developed to enable the organizations to share the incident information in standardize format with the national and/or sectoral CSIRTs. FIRe provides the functionalities to communicate & coordinate during the incident resolution. FIRe also integrated tools for secure communication, sensitive information labeling, real time interaction with handler & analyst and database of stakeholder point of contacts. Operational testing of FIRe is planned in upcoming national cyber security exercise 2015 to be conducted by Indian Computer Emergency Response Team (CERT-In). Learning's of exercise and feedback of participating organizations with respect to FIRe will be used for improving the tool.

**Keywords:** Computer Emergency Response Team (CERT); Computer Security Incident Response Team (CSIRT); Incident Reporting; Incident Handling; Incident Coordination; Indicators of Compromise (IOC)

---

## Introduction

A security incident is defined as an adverse event in an information system and/or network that pose a threat to computer or network security. In other words, an incident is any event that causes, or may cause a breach of information security in respect of availability, integrity and confidentiality. Examples of such incidents could be unauthorized access to information system, disruption of data, denial of services/availability, misuse of system resources, malwares and others. Large scale cyber incidents may overwhelm government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of the magnitude may threaten lives, economy and

national security. Rapid identification, incident information exchange and coordinated response can mitigate the damage caused by malicious cyberspace activity.

A significant cyber incident requires increased national and/or sectoral coordination. Study of different incident reporting and coordination means & methods adopted by CSIRTs worldwide reveals that there is lack of standardize formats, channels & methods, (to) report the incidents to CSIRT, (for) incident information exchange with CSIRTs & stakeholders and (for) coordination with CSIRT during incident resolution. It is also observed that there is only few instances where means for real time coordination for incident resolution is implemented. It comes finally to regional coordination bodies or national CSIRT to enable sectoral CSIRTs and organizations under their purview for improved incident reporting and coordination activities.

---

## Ashutosh Bahuguna\*

Scientist, Department of Electronics & IT,  
Ministry of Communication & IT Electronics  
Niketan, 6-CGO Complex, New Delhi-110003

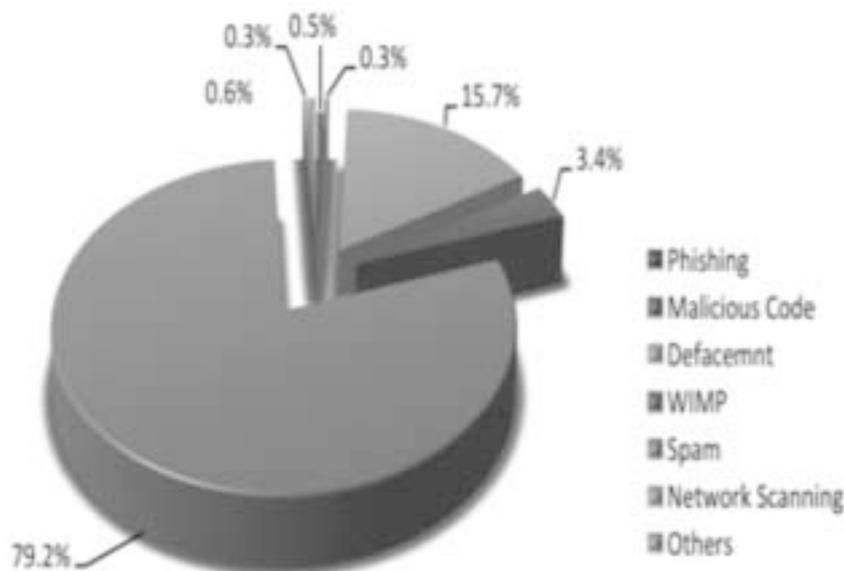
FIRe (Firefox for Incident Reporting), an extended Firefox browser is developed with objective to standardize and enhance the incident reporting and coordination activities, it provides features for secure email communication, web-form based incident reporting, Instant messaging for coordination during incident resolution, information sensitivity labeling, access to centralized point of contact database of relevant stakeholders and sharing of Indicators of compromise (IoC). In summary, FIRe is a tool to enable reporting party for better coordination & communication with national or/and sectoral CSIRT's during incident resolution process. There is notable effort by European Union Agency for Network and Information Security (ENISA) [1] in standardization of incident reporting across European union. ENISA also developed a tool Cyber Incident Reporting and Analysis System (CIRAS) [2][3], as per Article 13a: guidelines for incident reporting [2][3], for online incident reporting to replace the electronics forms email exchange in incident reporting. FIRe is not only a incident reporting system but a tool with purpose of improving coordination & communication in handling cyber attacks.

This paper discuss need for improvement in incident reporting & coordination means & methods, objectives & features of FIRe tool and operational

testing of FIRe in exercise scenarios. Study of implemented means & mediums by various national CSIRT's for facilitating coordination & communications between reporting entities and national CSIRT are also presented in this paper. The rest of the paper is organized as follows. Section 2 is about need and challenges of Computer Security Incidents Reporting. Section 3 discuss current computer security incident reporting practices and solutions at various national CERT's/CSIRT. In Section 4 FIRe functionality details are provided. Section 5 is about operational testing of FIRe in upcoming cyber security exercise. Finally section 6 concludes the paper with future roadmap for FIRe.

### Computer Security Incidents Reporting

National and sectoral CSIRT's also known as Computer Emergency Response Teams (CERT's) are the national or sectoral nodal agencies for responding to the cyber security incidents [4]. National/Sectoral CSIRT's are using multiple channels for gathering the information related to the incidents impacting cyberspace under their purview. By reporting computer security incidents to CSIRT's, the organizations and users receive coordination with other entities & technical assistance in timely resolving of incidents. This also help national/sectoral CSIRT's to correlate the incidents thus reported and analyze them; draw inferences;



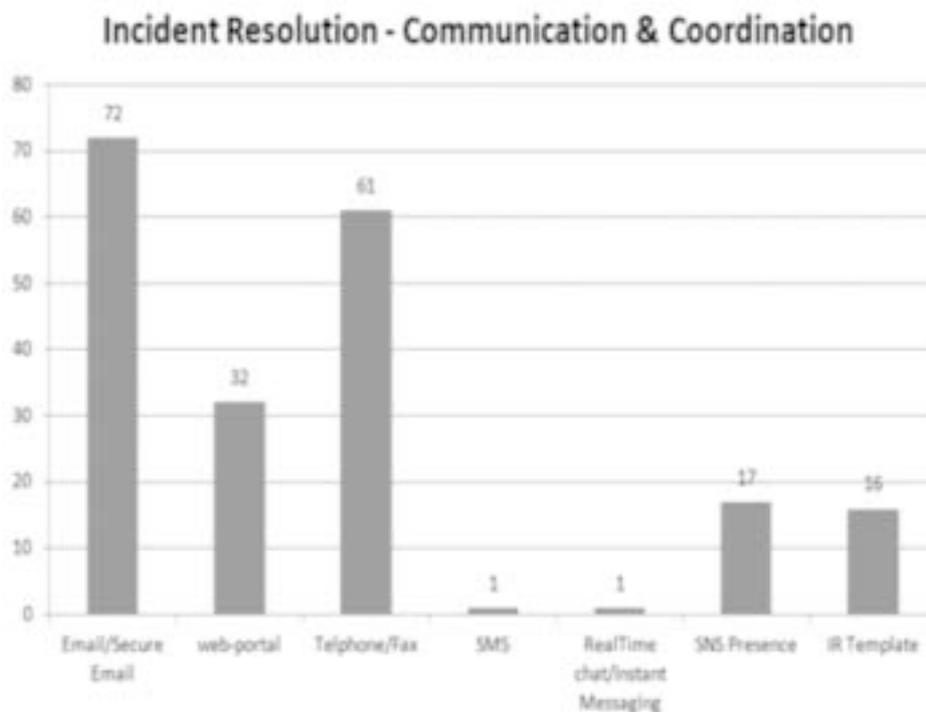
**Figure 1. Cyber Intrusion During February, 2014.**

disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents in future. Incident reporting need to be encouraged and supported by effective means of reporting & coordination tools and platforms.

CSIRTs are handling incidents reported and also monitoring the different sources for the incident information. Figure 1 is the breakup of incident reported & tracked by CERT-In in month of February, 2014 (Public Report: Monthly\_report\_CERT-In\_Feb\_2014) [5]. Most of the incidents in category Malicious code, Spam, Website Intrusion & Malware Propagation (WIMP) and defacement are tracked from various different sources. Study of the “incidents reported” and “incidents tracked” from other sources infer that large number of incidents (more than 70% percentage of incidents) remains unreported because of various possible reasons to organizations or users like lack of trust, lack of clarity and standard operating procedures for sharing information with external parties, reputation issues and others.

Trust of community on National and sectoral CSIRTs is vital for incident reporting and information sharing

to CSIRT. Many organizations consider information sharing to external organizations as damaging to themselves, trusted CSIRTs (national and sectoral) are only hope for organizations to have help in incident resolution without any risk of damage to reporting party [6]. Organization or user reluctant to share incident information due to the confidentiality of data, legal and policy issues [7], reputation of organization, lack of trust or unwillingness to share data should be encouraged to share Indicators of Compromise (IoC) [8] instead of complete event data. Effectiveness of response actions of national CSIRT, for defending against cyber attacks, fundamentally depends upon percentage of incidents reported and tracked by CSIRT. To reduce the figure of unreported incidents, CSIRTs community need to focus on encouraging incident reporting & information exchange by developing and implementing the effective solutions for supporting communication & coordination activities during incident resolution. Streamlining the incident reporting process by standardization of incident data and incident reporting means would also improve operational efficiency of the CSIRT [9].



**Figure 2. Incident Reporting and Coordination Solutions**

## Computer Security Incident Reporting Practices And Solutions

This section presents the main findings of the study on incident reporting & coordination means implemented by various national CSIRTs. Figure 2 presents result of the study, results are based on study of communication & coordination methods of 82 national and regional CSIRT [10]. Web-portals for incident reporting and incident reporting template (IR template) are efforts to enable the users to report the incident with required useful information about the incident, however these methods are not widely implemented. Among 82 CSIRTs, 17 CSIRTs are using social networking sites (SNS) like Twitter, LinkedIn and Facebook as a channel for interaction, which is again not a significant figure.

It is noteworthy that today also email and telephone/ fax are the main categories of communication channels in use followed by web-portals for incident reporting. There is a need of effective solution for enabling standardized incident reporting, real time interaction, information exchange & coordination activities. Real time communication & coordination enable analyst-to-analyst level interaction, rapid exchange of ideas &

technical details and enhance trust & willingness for information sharing with external entities and national CSIRT, surprisingly only one CSIRT implemented the real time coordination solution for incident resolution & Short Message Service (SMS) based incident reporting. Looking at complex nature of current cyber security threat landscape, it is require to develop effective mechanism & means for incident reporting, communication & coordination activities during incident resolution and tools for supporting these activities.

### Fire (Firefox For Incident Reporting)

FIRE is a customized Mozilla Firefox [11] browser which includes extensions for supporting incident reporting & incident resolution activities. Supporting server side applications like incident database, Internet Relay Chat (IRC) server [12], point of contact database need to be setup at CSIRTs. FIRE is developed with following 5 main objectives :

- to explore the options for improving community-to-CSIRT communication & coordination in cyber security incident resolution.
- Real Time coordination in incidents as required.



**Figure 3. FIRE V 1.0 Screenshot.**  
*Extensions and Functionalities of FIRE*  
*Secure Email- Pretty Good Privacy (PGP)*

- c. Provide platform for real-time Analyst-to-Analyst coordination.
- d. Enable rapid exchange of ideas & technical details.
- e. Enhance trust & willingness to share information.

Incident contains confidential details and various CSIRTs provide Pretty Good Privacy (PGP)[13] public

key for secure email communication (refer to section 3). Mailvelope 0.9.0 [14] is used with FIRE V 1.0 to provide key generation, key management and integration facility with email service providers for secure email communication with CSIRTs and other entities as required during incident reporting & resolution phases.



**Figure 4. Secure Email Communication-Mailvelope.**

### **Information Sharing-Traffic Light Protocol (TLP)**

TLP [15] is used by various international CERTs for marking confidential information by incident reporter and ensures controlled disclosure. It make use of four colors (Red, Amber, Green, and White) to classify information according to sensitivity, refer figure 4 (Source: US-CERT). FIRE ensures marking of information as per TLP in incident reporting, IoC sharing and during real time coordination.

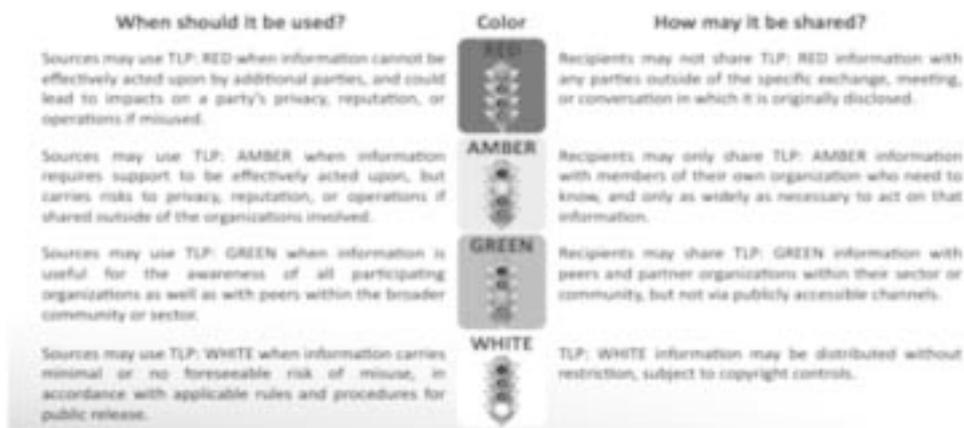
### *Real Time Coordination-Internet Relay Chat (IRC)*

Internet Relay Chat(IRC) [12] provides real time group chat facility. Instant Messaging (IM) and IRC are useful in incident resolution for analyst-to-analyst

coordination, informal and fast sharing of ideas & technical details. FIRE v 1.0 uses Chatzilla 0.9.90.1 [17] as IRC client. In FIRE V 2.0, it is proposed to include common instant messaging (IM) client that would support IRC, XMPP/Jabber [18] and IM web services.

### *Incident Reporting Portal*

This feature enable web-based secure incident reporting as per incident reporting form of CERT-In [19] to national/sectoral CSIRTs. This system improves collection of required incident related information. Incident reporting portal reduces the time required for resolving the incident and also improve efficiency of CSIRT.



**Figure 5. Information Sharing Traffic Light Protocol (Source: US-CERT[16]).**

*Sharing Indicators of Compromise (IoC)*

IoC are artifacts that indicate a computer security incident. IoC typically includes IP addresses, MD5 hashes of files, other attributes of malicious files, URL of botnets. IoC provides fast threat information exchange for early intrusion detection and threat data correlation at CSIRT. Organizations unwilling to share complete incident information should be encouraged to share IoC. FIRE provide portal for sharing the IoC with trusted entities.

*Integration of cyber threat management systems like Collective Intelligence Framework (CIF) client in FIRE*

FIRE will provide client interface for accessing threat management system-Collective Intelligence Framework (CIF). "CIF allows you to combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route). The most common types of threat intelligence warehoused in CIF are IP addresses, domains and urls that are observed to



**Figure 6. Internet Relay Chat(IRC) client- Chatzilla.**



**Figure 7. Incident Reporting Portal.**

be related to malicious activity” (source: Google-code-CIF description)[20]. This functionality will allow access to threat information shared by community and collected by cif from various sources on internet, as configured by CSIRT like malwaredomainlist [21] and spamhaus [22].

*Security advisory, vulnerability and alert notes by feed reader to the subscribers*

During study of means of communication implemented by CSIRTs (refer section 3), it is observed that various CSIRTs implemented feeds for sharing vulnerability report, security alert and advisory. Sage 1.5.2 [23] is implemented with FIRE for RSS and Atom feed aggregation.

*Dashboard for sharing internet weather based on NetFlow sensors data*

FIRE display Internet weather – “current observed threat level” based on the data collected by the network sensors and network data analysis systems implemented by CSIRT at national level or by sectoral CSIRT for specific sector.

*Stakeholders and service provider’s point of contacts (PoC) Database.*

Coordination with various domestic and international entities is required to resolve the incident. Organizations usually maintain details of PoC in their security plan, however the database is limited to few entities & service providers and may not include PoC

**Table 1. FIRE functionality Implementation [Yes(Y), No(N), Not Applicable (NA)].**

Functionality/Version	FIRE V1.0	FIRE V2.0
Secure Email	Y	Y
Information Classification -TLP	Y	Y
Real Time Coordination-IRC client	Y	NA
Real Time Coordination-Common IM Client	N	Y
Incident Reporting Portal	Y	Y
Sharing Indicators of Compromise	Y	Y
Cyber Threat Management Systems-Integration	N	Y
Feeds-Security advisories, alerts from CSIRTs to users	N	Y
Point of Contact Database	N	Y

of vectors involved in particular incident. FIRE will provide access to the centralized database of PoCs maintained by CSIT.

FIRE version 2.0 is planned for development after evaluation of FIRE 1.0 in upcoming cyber security exercise, discussed in next section. Table below provides snapshot of features implemented/proposed to implement in respective versions of tool.

### Fire in Cyber Security Exercise

Indian Computer Emergency Response Team (CERT-In) is conducting national cyber security exercises (CSE) on periodic basis targeting various sectors of the Indian economy. The purpose of exercises is to provide opportunity to the participating organizations to test their preparedness in combating cyber attacks by means of preparation, detection, reporting, coordination & communication, mitigation and response actions. Cyber security exercises also provide opportunity to improve coordination & communication activities among national CERT, sectoral CERTs, stakeholders and service providers. It is proposed to include FIRE in forthcoming exercise as a one window solution for incident reporting, Instant Messaging, secure email communication, sharing artifacts & logs and Point of contacts database

of CERTs/stakeholders/agencies/service providers. Cyber security exercise will provide platform for FIRE operational testing. Learning & feedback of exercise observer team and participating organizations will be used to improve the FIRE before releasing it for community use.

### Conclusion

Author believe that FIRE will have positive impact in incident reporting and resolution activities. FIRE will improve coordination and communication among organizations, sectoral CSIRTs, service providers and national CSIRT. Browser plugin based implementation made it platform independent and easy to setup. It will improve the operational efficiency of CSIRT by flourishing culture of standardize coordination & communication in incident reporting and resolution. FIRE can be further enhanced with functionality to collect threat information and incident information from international partners and vendors. National/sectoral CSIRT may add the functionality for pushing vulnerability reports, critical threat alerts, malware alerts, network flow analysis trends to the sector or organizations using the FIRE. FIRE evaluation in upcoming cyber security exercise will definitely lead us further.

### References

1. European Union Agency for Network and Information Security (ENISA), <http://www.enisa.europa.eu/>.
2. European Union Agency for Network and Information Security (ENISA): Annual Incident Reports 2012. Analysis of Article 13a incident reports.
3. ENISA: Article 13a Expert Group portal. <https://resilience.enisa.europa.eu/article-13>.
4. Moira J. West-Brown, Don Stikvoort, and Kalus-Peter Kossakowski: *Handbook for Computer Security Incident Response Teams(CSIRTs)*.CMU/SEI-2003-HB-002.
5. CERT-In Monthly Report, <http://www.cert-in.org.in/>.
6. KimoonJeong, Junhyung Park, Minsoo Kim, BongNam Noh: A Security Coordination Model for an Inter-Organizational Information Incidents Response Supporting Forensic Process. *IEEE Fourth International Conference on Networked Computing and Advanced Information Management (2008)*.
7. Hennin, S., Control System Cyber Incident Reporting Protocol. *IEEE, Technologies for Homeland Security (2008)*.
8. Indicators of Compromise (IoC), <https://www.mandiant.com/blog/tag/openioc/>.
9. James R. Antonides, Donald N. Benjamin, Daniel P. Feldpausch, and Jeffrey S. Salem, USCC :Streamlining the US Army Network Incident Reporting System. *Proceedings of the 2008 IEEE Systems and Information Engineering Design Symposium*.

10. CERT/CC: <http://www.cert.org/incident-management/national-csirts/national-csirts.cfm>.
11. Mozilla Firefox. <http://www.mozilla.org/>.
12. Internet Relay Chat (IRC). <http://tools.ietf.org/html/rfc1459.html>.
13. PGP: <http://www.ietf.org/rfc/rfc2440.txt>.
14. Mailvelope: <https://www.mailvelope.com/>.
15. Information Sharing Traffic Layer Protocol (ISTLP): <https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/information-disclosure>.
16. United States Computer Emergency Readiness Team (US-CERT). <https://www.us-cert.gov/>.
17. ChatZilla. <https://addons.mozilla.org/en-US/firefox/addon/chatzilla/>.
18. XMPP/Jabber. <http://www.ietf.org/rfc/rfc3920.txt>.
19. Indian Computer Emergency Response Team (CERT-In). <http://www.cert-in.org.in>.
20. Collective Intelligence Framework. <https://code.google.com/p/collective-intelligence-framework/>.
21. malwaredomainlist. <http://www.malwaredomainlist.com/>.
22. Spamhaus. <http://www.spamhaus.org/>.
23. Sage 1.5.2. <https://addons.mozilla.org/en-US/firefox/addon/sage/>.

# Nine Steps to Indian Security, Confidentiality Privacy & Technology in Cyber Space

Rajeev Kumar Singh\*

---

## Abstract

The increasing dependency on cyber space has cropped up concerns associated with understanding the potency of cyber risks which are to a larger extent unguarded and unsecured as the technology is volatile. Cyber security is one of the most critical issues the India faces today. The threats are real and the need is pressing. Despite the best intention of those involved with previous cyber legislative efforts, aAct 2008 Amendment has introduced various beneficial changes into the IT Act, 2000, yet they are not enough to tackle the increasingly growing menace. Cyberspace's dynamic nature must be acknowledged and addressed by policies that are equally dynamic. There is an urgent need to become the technological advancement and cyber-security, wherein intelligentsia has to anticipate, prepare, act, and respond to the cyber risks in all asrata of human life, so as to guarantee effective e-governance, e-commerce and e-communications, thus, protecting cyber space where netizen's safety and security is ensured.

**Keywords:** Cyber Crime, Cyber Security, Electronic Signature

---

## Introduction

The Indian faces significant cyber security threats includes denial of service, defacement of websites, spam, websites compromise and malware propagation, computer virus and warms, pornography, cyber-squatting and phishing.

A Cyber-crime is now a biggerthreat to India Inc than physical crime. In a recent survey by IBM, a greater number of companies (44%) listedcyber-crime as a bigger threat to their profitability than physical crime (31%). But the available statistics fails to throw actual light upon the real facets of the menace as many cyber-crimes goes unnoticed and unregistered, due to various reasons including lack of legal awareness, a partly of the law enforcement agencies etc. But the facts that cyber- crimes

areincreasing in multitude and are becoming insidiously computer cannot be denied.

The cyber security status quo is unstable, especially when considering the enormous and growing scope of these threats. To mitigate these threats, this paper

provides a framework that may provide safeguarding in cyber space to individuals citizens.

Through dynamic and cost effective solution we can make cyber space a safer and more productive place for Indian citizens to pursue the prime minister dreams.

Failure to take responsible action, however, learns the Indian vulnerable to verity of threat. Nation-states such as China, Pakistan, South Korea are more than willing to steal or destroy Indian digital property to further their power or prestige. Non state actors such as Indian Muzzahidin and Hezbollah have also shown the capability to employ cyber methodologies and criminal organizations from around the world, and have acted as hired guns as well as on their own, using cyber tools as their weapon of choice.

In response to the security threats, the Russia, China Israel and North Korea have set up their own cyber armies. America has also established a new cyber command. However, it is unclear what steps have been taken by the Government of India to establish a defence service against cyber-attacks.

In addition to these issues of security for nations and corporations, Indian enacted IT Act in the year 2000, which however failed in effectively tackling cyber-

---

**Rajeev Kumar Singh\***

Research Scholar  
Chankya National Law University  
Patna, Bihar

crimes as it was more inclined towards facilitating electronic commerce. However the amendments made to the original Act through the IT (Amendment) Act of 2008 has brought some changes into the cyber law framework of the country. It has brought forth considerable reformations in the existing law, thereby making cyber-crime a much more serious offence than it was perceived earlier important changes brought in through the amendments.

- Permitting interception of message form mobile phones, computers and other communication devices,
- Blocking of websites in the interest of National security.
- The setting up of a cyber-appellate tribunal.

The amendment has attempted to fill in the gaps which existed in the earlier 2000 enactment. The current Indian IT Law covers provisions relating to cyber frauds and other wrongs committed while using electronic commerce, breach of confidentiality, leakage of data, etc., which were left outside the purview of the earlier enactment. Certain terms left unexplained under the parent law has now been interpreted and explained under the new law, thus giving a wider scope for its application.

Developing challenges that are today's cyber environment. Additionally, any legislation must provide robust protection for privacy and individual freedoms. There are some key components that need to be included in truly effective cyber legislation.

1. **Essential to set up some more agencies like "Cyber police station" specially entrusted with different tasks associated with combating cyber-crime:** Existing agencies involved with the task of combating cyber-crimes in India are an enough. It is essential to set up some more agencies specifically entrusted with efficient tasks associated with combating cyber-crimes which must however work in co-ordination with each other to achieve the ultimate objective. This can be done by establishing separate agencies on the lines of "National Infrastructure Protection Centre" of US. A separate centre to take up complains of cyber-crimes over the internet must

be set up similar to the "Internet Fraud complaint centre" of US. The department of Justice of US has also setup a separate specialised unit "Computer Crime and Intellectual Property section" to address issues of cyber-crimes. It evaluates problems of cyber-crimes and makes law and policies essential to address such problems. On the other hand, regular police officers are not technically trained to successfully investigate cyber-crimes. There is thus an urgent need in all states, through the country. In addition special acquaintance and training of police officers of regular police stations should also be ensured.

2. **Advocating for private sector efforts to promote general awareness, education and training across India:** The Indian people not recognised like American people that there is a problem with securing the cyber domains. The American people hear about it regularly on the news, abstractly, that is there. Here is an urgent need of private entities, nongovernmental organizations, along with universities and other research institutes, ought to play a much more active and prominent role in supporting personal cyber safety and community –centric program. Here, must also be viable programs of professional base –level training that is encouraged for the general Non- IT workforce. Since, every job now involves the use of digital dives in some aspects of work; the general workforce must receive continuing education. Apart from this, urgent need of teaching of cyber security as component in school and colleges.
3. **Increase the numbers of IT professionals with security certification:** Information security certification like the certified information systems security professions (CISSP) and the certified information security managers (CISM) may represent the minimum level of training that a cyber-security professions needs.
4. **Develop more IT leaders with cyber security expertise:** The India needs more qualified personal in this fields, and specifically in to advanced cyber skill sets, such as code writing, defensive procedures, deep packet inspection, and big data

analysis techniques. A major effort must be made to find the sort of people who can flourish in this field, and give them the opportunity to pursue the high quality education they require.

**5. Cyber security beyond the borders:** The various packets of information tracking over the innumerable remarks in the World Wide Web are not specified as to where they are tracking or who is on the other side of the computer screen. Cyber security is not now, and never will be, issues that our country can solve alone. The solution will require a concentered- and ongoing- collaboration between the Indian a like-minded free nations. Treaties and global governance do not contain bad actors, and should thus not be the focus of Indian or International cyber security efforts. Instead, the India must work with other friendly nations to later bad cyber behavior by raising the costs of such behavior. The first step to effectively conducting a fruitful strategy is to determine an Indian domestic policy on cyber security. I would be foolish to jump into international negotiates until the India has the kind of national conversation that sorts out definitional and policy positions. However, it would be just as foolish to ignore the need to make international connections and establish cooperative relationship in this field. Both should be done as soon as is practical.

**6. Need of legal clarification of scope of certain provisions of IT Act (including section 65, 66A and 66F):** it is essential to regularly update and amend pertinent legal provisions, so that changes in technology affecting the effected implementation of law can be dealt. This call for consistent legal research and development activities and periodical review and revision of law. In addition already existing law and provisions must be properly defined and interpreted to deal with cyber- crimes so that no crimes goes unpunished for the reasons of “insufficiency in law and legal terms and provisions. Whenever It law’sprovisions are silent or fails to address a particular cyber-crime or a related issues , the existing criminal law including IPC and other appropriate enactments must be interpreted to apply and deal with such a crime.

Ultimate aim of the law must be to tackle all tippers of cyber-crimes, whether covered under the existingspeciallaw, or not, however by constructing interpreting existing provisions of law. Absence of punishingprovisions in IT Act should not be the ground for acquittalof cyber criminals. This mindexpanded interpretations of terms like “property” in Indian Panel code and requiredexpansion of provisions relating to criminal trespass, mischief, theft, etc. So that it incarcerates new technical features of crimes. The criminal procedure code must be amended so as to facilitate the gathering of evidence and investigation of cyber cries.

**7. Focus on Electronic Signature, Encryption, Monitoring, decryption and Interception in view of National Security:**

- a. An interesting side-effect of the challenge posed by electronic Signatures is that the question of whether a seal can function as a signature becomes relevant. The reason for this is that many of the electronic signature technologies require the signatory to use a numerical key to produce the signature. The smallest useful key area minimum of 56 bit in length, offering a range of numbers between approximately 563,000,000,000,000 and 72,000,000,000,000,000 in decimal notation. These key are too small for adequate security, however, and 128 bit or large r key are more desirable. Number of this size is not easily memorable or easily keyed in without error, and so the key are normally stored on some physical device, such as a memory stick or a smart card.
- b. The recent Amendments to the IT Act, 2000, nearly a decade after the Act came into force; promise to take electronic commerce to the next level by making introducing the concept of technological neutrality. Since electronic signatures are no longer necessarily based on asymmetric cryptology, technical advancement can easily be implemented. These technological advances are most likely

- to make electronic signature easier and more secure to use.
- c. In the matter of encryption, all over an interesting question is whether the presence of encryption renders the underlying information confidential. As a starting point it would see that if a person goes to the length of encrypting information the information must have a quality about it that is deserving of protection. However there is no authority in law that holds that the mere presence of encryption renders the underlying information confidential. In the case of *Mars UK Ltd. Vs Teknowledge Ltd.*, which concerned a coin discriminator mechanism for the sorting of coins in coin operated machines, the defendant reserved engineered the mechanism, a process that required the decryption of encryption program code. One was the question before the court was whether the presence of encryption put the defendant on notice that the encrypted information was confidential.
  - d. In the matter of Interception, Decryption and monitoring, one of the controversial provisions that has been engrafted into the I.T Act, 2000 by the amendments through the I.T (Amendment) Act, 2008, is the substitution of section 69 that in its new *avatar* grants certain authorities also the power of interception, decryption and monitoring electronic contents including communications (e-mail, online chat or mobile phone communication) “for investigation of any offence” under the sun as against the traditional powers that were highly restricted on few grounds such as, in the interest of the sovereignty or integrity of India.
  - e. The amendment Act does not deal with the procedure and safeguard for monitoring and collecting traffic data or information by the Central Govt. may prescribe the modes or methods of encryption. As yet no policies or guidelines have been issued pursuant to the power set forth in section 84A.
  - f. The IT Act 2008 allows the central government to intercept computer communication for investigation of any offence. Section 26 of the Indian Post office Act 1898 grants the government the power to intercept letter or postal articles on the happening of any public emergency or in the interest of public safety or tranquility. Section 5 (2) of the Indian Telegraph Act, 1885 empower the government to intercept land line and mobile phones on the occurrence of any public emergency, in the interest of public safety, Sovereignty and integrity of India, security of state, friendly relation with foreign states, public order, or for preventing incitement of the commission of an offence. However the IT amendment Act enlarges of the power of the central government to embrace interception of information transmitted through any computer resource for the purpose of investigation of any offence. The provision is also vague about the procedure and safeguards that need to be employed when such interception or monitoring or decryption is carried out.
  - g. The standing committee on information technology, while reviewing the bill, observed that ‘public order’ and ‘police’ are state subjects as per schedule VII of the Constitutions and that the IT Bill should confer powers of interception on the state governments also in tune with the provisions of section 5(2) of the Indian Telegraph Act, 1885. Therefore interception of information should be for the perception of certain cognizable offence in addition to the already prescribes grounds, instead of the broad sweeping term of ‘the commission of any cognizable offence or for investment of any office’ used in the Act.
  - h. The Amendment Act does not deal with the procedure and safeguard for monitoring and collecting traffic data or information by the Central Government it further does not define the procedure and safeguard subject to with blocking access by public to any

information through any computer resource may be carried out.

- i. Lack of harmonized definition of the cyber-crimes and lack of international cooperation in tacking the menace is the other problems which require immediate solution.

#### 8. Use of “Adhar” in social networking sites to prevention of child:

There is a social sites especially porn site creates a page to clarification of age of person able to view the prono graphic image etc. But i the case of 90 percent child below age below than 18 years use pornographic image. This is the major issues for social networking sites. Here is a technique to use “Adhar” to cleafication of actual age by take an Adhar number by user.

#### 9. Hurdles in the path of combating cyber-crimes:

There is a lack of consensus exists among jurists regarding the definition, nature, ambit and types of cyber- crimes and this is in fat one of the elementary problem affecting combating of cyber-crimes. An act of cyber- crimes is not accept as a “ criminal wrong “ by all , further which law has to deals with the menace is another issues lacing consensus amongst members of legal fraternity. According to some jurists, cyber- crimes are new but traditional crimes committed with the use of new technology and thus they does not require any new or separate law as the traditional criminal itself is sufficient to deal with them, on the other

hand, according to some other jurists, cyber-crimes are new forms of crime, having different nature and impact compared to traditional crimes and requires new and separate laws enacted specifically to deal with its investigations and inquires. Though today we have specific provisions dealing with cyber- crimes in Indian It Act, yet many police as well as judicial officers hesitate to register or otherwise deal with the cyber- crimes under it and prefer to do so under IPC, the traditional criminal law of India.

### Conclusions

Use of Information Technology in all spheres has helped e-commerce, International connectivity and communication. But if misused, it can affect the security of nations as well as International community including the security of individuals. More need to be done in order to effectively tackle the growing problem of cyber-crimes. A safe cyber world need a proactive approach to be adopt jointly by Government, Industry Individuals and public at large, which includes adopting and enforcing effective legal provisions, which can effecting counter all forms of cyber-crimes.

“Healthy growth of Information Technology requires a secure environment which can only be ensured by adequate legal provisions and suitable enforcement measures.”

### References

1. <http://www.cert.in.org/knowledgebase/annaulreport/annualreport08.pdf>.
2. Aparna Viswanathan: Cyber Law-Indian and Internatinla perspective, Butterworthswadhwa, LexisNexis, Nagpur, P. 23.
3. Nikhil Pahwa, ‘Indian’s information Technology (Amendment) Bill passed by Lok Sabha’, <http://www.medianama.com/2008/12/223-indians-inforamtion-technology-amedment-bill-passed-by-lok-sabha>.
4. The Centre assesses and investigates important threats and incidents relating to intrusion of critical infrastructure.
5. In Us, this Centre established by FBI offers a Central repository system to take up complaints, relating to internet fraud and such information’s to quantity fraud patterns and provide timely statistical data of such frauds.
6. Surya Senthil and Lakshmiddev: Manual of Cyber Laws, Aditya Book company, Chennai, P. 14.
7. Economic and political weekly, “Dithering over cyber law”, Vol 34, No 20 [May 15, 1999] at P 115.

# Security Vulnerabilities in 'Future of the Web' - IPv6 Protocol Suite

Navneet Kaur Popli\*  
Dr. Anup Girdhar\*\*

---

## Abstract

The concept of 'Web' has been possible because of interconnection of devices and these interconnections have been possible because of a network layer protocol- IPv4. Internet Protocol Version 4 (IPv4) has been in existence for about 20 years and was responsible for revolutionizing the Internet. Lately, however the number of devices on the network has increased manifolds. IPv4 has not been able to cope up. It has been running out of addresses. Thus IPv6 has come into picture with an enormous address space, solving the address problem for many years in the future. IPv6 has become the future of the web. In fact with the idea of 'always connected' devices, millions of systems are connected to the web at the same time. Only a protocol like IPv6 can support such a huge number of devices.

But IPv6 comes with its own set of security concerns. These are largely unexplored and therefore most of the network administrators are still wary of deploying IPv6 over their networks. This paper covers the vulnerabilities and security threats to IPv6 and their possible solutions.

**Keywords:** Web security, IPv4, IPv6, Vulnerabilities.

---

## Introduction

IPv6 was defined in RFC 2460 in mid 1990's. It was designed to be the next generation Internet Protocol address standard which would supplement and then finally replace the IPv4 protocol suite used in the Internet presently [1].

IPv6 gives huge scalability because it uses 128 bits for addressing[2]. This means we have 340 undecillion ( $3.4 \times 10^{38}$ ) addresses i.e. about 52 Trillion Trillion addresses per person if the population of the world is 6.5 billion [3] currently.

Not only does IPv6 provide a big range of addresses, it also gives high Quality of Service (QoS), end-to-end networking, high degree of mobile connectivity and many other benefits.

---

### Navneet Kaur Popli\*

Assistant Professor (IT),  
MERI, GGSIPU, New Delhi.

### Dr. Anup Girdhar\*\*

Research Guide  
CEO-Founder, Sedulity Solutions and Technologies

## IPv6 Address

IPv6 Address is a 128 bit address consisting of 8 sections, each 2 bytes in length[4]. Example

FDDA:AB94:0064:3610:000F:CCFF:0000:FFFF

Is an IPv6 address. It can be abbreviated by dropping the leading 0's

FDDA:AB94:64:3610:F:CCFF:0:FFFF

Consecutive 0's can be replaced with a double semicolon.

FABC:0:0:0:0:AABB:0:FFFF

Can be abbreviated as

FAC::AABB:0:FFFF

## Transitioning

IPv6 can work with IPv4 so that transitioning becomes smoother and the already existing IPv4 infrastructure can be used.

Three strategies are used for this transitioning[4]:

1. Dual Stack
2. Tunneling
3. Header Translation

*Dual stack*-For smooth from IPv4 to IPv6, every system supports both IPv4 and IPv6 protocol stacks, and according to the type of communication, use the appropriate stack.

*Tunneling*- This is a situation where source and destination support only IPv6 but the underlying network support IPv4. Then the IPv6 packet is encapsulated inside the IPv4 packet for transmission.

*Header Translation*- This is a situation where one host is IPv6 and the other host is IPv4. So the header format of IPv6 has to be completely translated to IPv4 to be understood by the destination.

### IPv6 Attacks

IPv6 was considered to be a very secure protocol because IPSec was mandatory in the original protocol. The Authentication Header provides data integrity and data authentication for the whole packet. The IPv6 Encapsulating Security Payload header provides confidentiality, authentication and data integrity to the encapsulated payload. The security features in IPv6 can be used to prevent various network attack methods including IP spoofing, some Denial of Service attacks (where IP Spoofing has been employed), data modification and sniffing activity. However, issues with the security features still exist, concerning IKE, PKI and the strength of the encryption algorithms used for global interoperability[7].

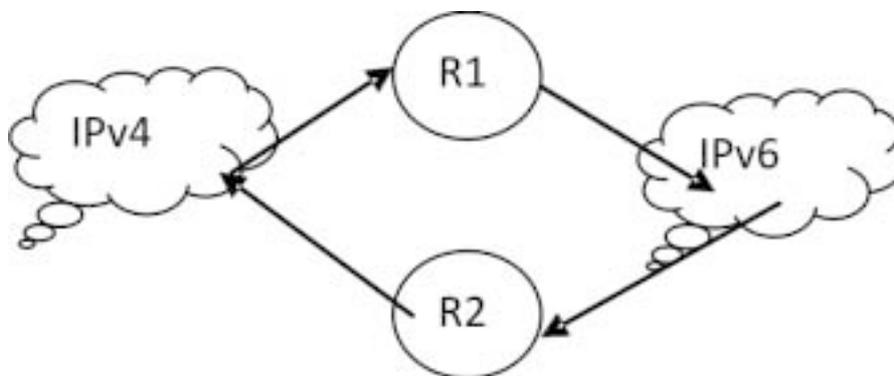
Today however, IPSec is optional in the current versions of IPv6. This makes IPv6 all the more vulnerable to security threats. There are a number of attacks that will be discussed in the paper[8]:

1. Attacks against IPv6
  - a. Transitioning Attacks
    - i. Dual Stack Attacks
    - ii. Tunneling Attacks
    - iii. Header Translation Attacks
  - b. Multicast Attacks
  - c. Extension Header Attacks
2. Attacks Against ICMPv6
  - a. Router Advertisement Spoofing
  - b. Router Advertisement Flooding
  - c. Neighbor Solicitation/Advertisement Spoofing
  - d. Duplicate Address Detection

#### *Dual-stack attacks:*

With the advantage of a smooth 4to6 transition through Dual Stack mechanism, it has its own security pitfalls also. For example, if there is a worm that has infected a host in a network, it will work by searching other hosts in the same subnet. Then it will spread by infecting those vulnerable hosts also. If the network is only IPv4, searching is done using 'Brute Force Scan'. This may take time in a large subnet. One may feel that IPv6 subnets which are huge ( $2^{64}$ ) may be safe from this attack. However that's not the case. A worm in IPv6 uses ICMPv6 multicast ping. This is an echo request to multicast address, e.g. FF02::1 to discover on-link nodes. Well known multicast addresses like these make it easier to find key systems within a network e.g. FF05::2 is a site-

local all routers address. Hence spreading of a worm would be faster in a dual stack network than in native IPv4 network. [5]



**Figure 1. Tunneling Attack**

### *Tunneling Attacks*

For tunneling, each end point of the tunnel must know its peer IP address before sending a packet to it. If the end points are pre-configured with IPv4 addresses then, considering huge sizes of IPv6 networks, it will become extremely difficult for the network administrator to manually configure these addresses.[6]

Thus Automatic Tunnels are introduced. Here, an end point's IPv4 address is computationally derived from the destination's IPv6 address. All the end points assume that once a packet arrives at the tunnel, its destination is also part of the tunnel. For example if we consider ISATAP (Inter-Site automatic Tunnel Addressing Protocol) tunnels, every end point has an IPv6 address of the following format:

<tunnel prefix><constantstring><IPv4 address>

all end points.

Routing Loop Attack can be introduced in these tunnels. Refer to Figure 1, the attacker exploits the fact that R2 does not know that R1 does not configure addresses from Prf2(tunnel prefix of R2) and that R1 does not know that R2 does not configure addresses from Prf1(tunnel prefix of R1). The IPv4 network acts as a shared link layer for the two tunnels. Hence, the packet is repeatedly forwarded by both routers [9].

### *Header Translation Attack*

Header translation is performed by a router which does a 6to4 or 4to6 translation of the headers. 'End to End Authentication' and 'Encrypted Security Payload' option of IPv6 are not present in IPv4. 'AH' shows integrity and 'ESP' shows integrity and confidentiality of the packet. Once these IPSec options are removed, the packet becomes very insecure and prone to attacks.

### *Multicast attacks*

IPv6 protocol does not support broadcast communication but it does support multicast communication. However there are some special addresses which can be very dangerous. An 'All Nodes

' address is FF02::1, 'All Router' address is FF05::2 and 'All DHCP Server' address is FF05::5. These addresses enable an attacker to identify important resources on a network and attack them.

### *Extension Header attacks*

An IPv6 packet has a simpler header so that routing can be performed efficiently. The size of the header is fixed (40 bytes) and the options come as extension headers after the main header. Thus the router does not have to check all the extension headers. Although they need to check the Hop-by-Hop option.[10]Firewalls that should enforce their security policy must recognize and parse through all existing extension headers since the upper-layer protocol information reside in the last header. An attacker is able to chain lots of extension headers in order to pass through firewalls. He can also cause a denial of service attack, if an intermediary device or a host is not capable of processing lots of chained extension headers and might fail.

In addition to the above attacks, the Padn option in the Hop-by-Hop Extension header can be converted into a covert channel. Padn option is normally used for alignment purposes and has a string of 0's. An attacker can put malicious data in this option.

### *Router Advertisement Spoofing*

If a rogue router starts sending spoofed router advertisement messages, all the nodes will update their routing tables with the new information which they have no way of verifying. Thus the rogue router now becomes one of their default routers, if the nodes communicate to the internet, the rogue router acts as a 'Man In the Middle' and can intercept all traffic.

### *Router Advertisement Flooding*

During stateless auto configuration of addresses, new machines create unique addresses using network prefix provided by a router. This is done using Router Solicitation and Router Advertisement messages. However, an IPv6 device can be part of multiple networks(no upper limit). Therefore a RA Flooding attack can be launched by a rogue server which floods the network by RA Advertisement messages. Normally a node on the network has no way of authenticating a server. This causes the CPU to generate countless IPv6

addresses. This can cause a system to hang and in fact this attack can bring down a network within seconds.

#### *Neighbor Solicitation/ Advertisement Spoofing*

IPv6 uses ICMP messages for discovery of neighboring devices on a network. These are multicast 'Neighbor Solicitation' and 'Neighbor Discovery' messages. An attacker can spoof these messages. He can send a fake binding of IP+MAC address. The IP address is that of a valid node but MAC address is that of the attacker. The victim node will update their Neighbor Cache which binds MAC addresses to IP addresses when they receive spoofed IP packets, which they cannot verify.[11] Thus the attacker can intercept all messages between the nodes by this method. Also a Denial of Service (DoS) attack can be administered by providing an invalid link layer address.

#### *Duplicate Address Detection Attack*

Duplicate Address Detection (DAD) is a technique during address auto configuration phase in which during the process of SLAAC, a node creates a unique IPv6 address on its own . It creates a local address using its MAC address and the link local address. It then multicasts this message, called a DAD message, to the entire network to check for duplicity. If the address is unique the router responds back with the

network prefix. This prefix along with the MAC address becomes a unique IPv6 address for a device.

An attacker can launch a Denial of Service attack if he answers to all DAD messages from a new node which is in the process of getting an IPv6 address assigned. The node thinks that this address is a duplicate one as is used by some other node. Thus it can never get an IP address and thus cannot become part of the network until the attacker stops the attack.

### **Conclusions**

IPv6 is no doubt the next generation in networking and no quick fix in IPv4 can slow down the evolution of IPv6. With its revolutionizing features and a never ending address space, IPv6 is welcoming the future with open arms. However the implementation is riddled with a number of security challenges which, if ignored can lead to disastrous consequences. Thus following the paradigm of 'Better safe than sorry', network administrators must take all the vulnerabilities in consideration and take adequate steps to safeguard themselves. A number of white collared hackers along with many other people from the industry are exposing new vulnerabilities of IPv6 everyday and are also giving solutions for protection. We must be fully prepared to embrace IPv6 but with complete security in place.

### **References**

1. Minoli, D. Kouns, J., *Security in an IPv6 Environment*, CRC Press, USA, 2009.
2. Davies, J., *Understanding IPv6*, 2nd edition, Microsoft Press, USA, 2011.
3. Hogg, S., Vyncke, E., *IPv6 Security*, Cisco Press, USA, 2009.
4. Foruzan, A. Behrouz, *TCP/IP Protocol Suite*, Third Edition, TataMcGraw-Hill Company, 2012.
5. Mayer Karl, Fritsche Wolfgang, *Security models and dual-stack (IPv6/IPv4) implications*, IABG, 2010.
6. Gabi Nakibly, *Security Vulnerabilities of IPv6 Tunnels*, InfoSecInstitute, 2014.
7. PennyHermannSeton, *Security Features in IPv6*, SANS Institute InfoSec Reading Room, 2002.
8. Weber Johannes, *IPv6 Security-An Overview*, Ripe Network Coordination Center, 2013.
9. G.Nakibly, F.Templin,, *Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations*, Internet Engineering Task Force (IETF):RFC 6324, August 2011.
10. Naidu.PSantosh, PatchaAmulya, *IPv6: Threats Posed By Multicast Packets, Extension Headers and Their Counter Measures*, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 15, Issue 2 (Nov. - Dec. 2013), PP 66-75, www.iosrjournals.org
11. RaghavanArun, *Secure Neighbour Discovery*, ReportCS625: Advanced Computer Networks.

# A Study to Examine Cyber Forensic: Trends and Patterns in India

Ms. Shruti Verma\*

Dr. Saurabh Mehta\*\*

---

## Abstract

Cyber forensics is a technique which is used to examine and analyze the computer system for some evidence which can be presented in the court of law as a proof to solve a cyber crime case and give the punishment to the criminal. India being the democratic nation finds difficult to strike a proper balance between the legal and the judicial system. Police and the law enforcement agencies still believe in the legacy system and are reluctant to follow the new suit. In this paper an attempt is made to show the current scenario of the cyber forensics in India, difficulties faced by the police dept and legal dept. This paper also briefs about the trends and patterns of the Indian cyber forensic.

**Keywords:** Cyber Crime, Cyber Forensic

---

## Introduction

In India the field of cyber forensics is very new and fresh. People are not aware about the term cyber forensics and its use. Gradually the nation is getting digitized, with fast connecting networks, easy internet availability and acceptance of the user. Cyber crime is also nurturing under the umbrella of growing technology. And this develops the need of cyber forensics in the system. But unfortunately in India cyber forensics is not implemented to the optimum level. Cyber forensics is an art which is required to detect the hints, clues and evidences from the digital data about the cyber crime to show the proof in the court of law and help the judicial system to take correct and precise decision against the criminal and help the victim. Cyber forensics can also help in prevention of criminal activities. Unlike traditional crimes cyber crimes are very sophisticated and fast, at the same time it is difficult to find an evidence about the cyber crime as the digital evidences can be

---

### Ms. Shruti Verma\*

Research Scholar at JIT University, Jhunjhunu  
Assistant Professor at SPN Doshi Women's  
College affiliated to SNDT Women's University

### Dr. Saurabh Mehta\*\*

Associate Professor and Head of Dept. at  
Vidyalankar Institute of Technology affiliated to  
Mumbai University

easily destroyed. So the job of cyber forensic is very crucial, finding out the digital evidence from the computer system confiscated. Indian legal system somehow fail to adopt the concept of cyber forensics and still follow the legacy pattern to solve the cyber crimes, this does not gives accurate evidences and projects unjust results in the court of law so the victim is given no justice and criminal is set free. The process of forensics is very slow in India because of various legal and judicial factors this delays the hearing of the case. There are so many cases still are pending and criminals are set free to commit few more crimes. We have adopted the idea and concept cyber space but we need to change our approach towards cyber forensics.

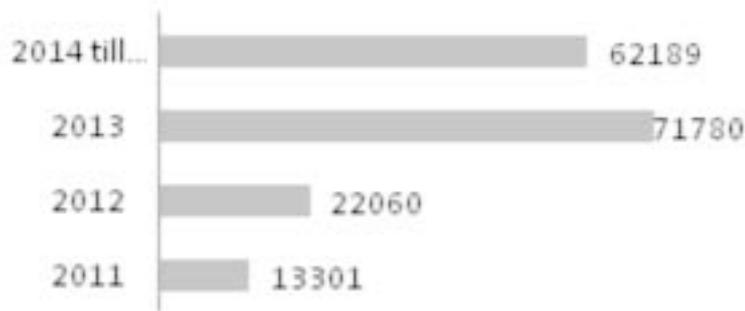
## Trend in India

In India point of consideration is the legal and judicial systems and there working which seems to be out dated, with the advent of cyber crimes there exists a need to change the current policies and construct a new techno-legal framework to combat cyber crime with the use of latest forensic technologies. Crimes like facebook account hacking, and email spoofing is very common in India but due to poor law enforcement and weak legal implications the criminal is set free to commit another crime. The cyber crime conviction rate is very less in India, where as the cyber crimes have increased in India. It can be the fear to get

into the legal proceedings or the disappointment with the quality of services provided Indian internet users do not prefer filing the case with the police, less than 50 % of cyber crime cases are registered with the police dept. this set the criminal free for another crime.

Cyber attacks in India are done by other countries like China, Pakistan, US, Nigeria, UAE, Brazil etc. Crimes

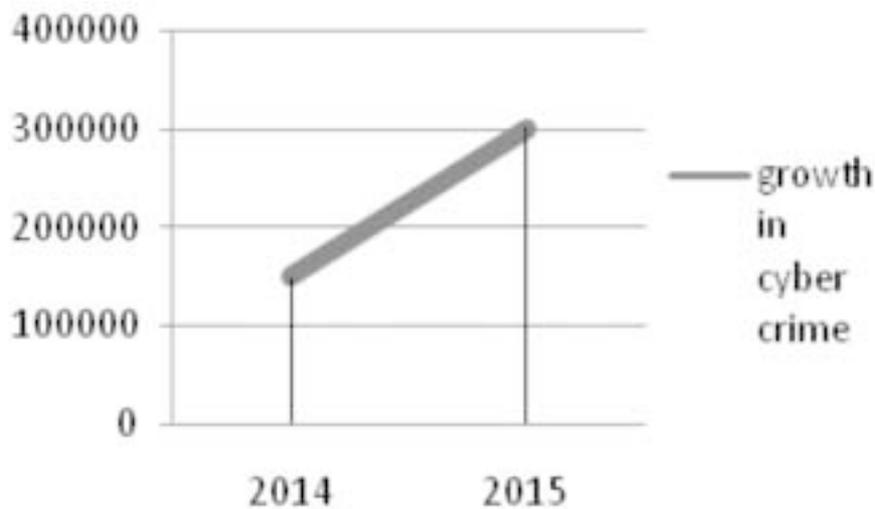
like phishing, email frauds, credit/debit card frauds, identity theft, virus etc. are very common in India. Home minister Mr. Rajnath Singh has conveyed the need of having strong cyber law monitoring and stringent cyber security. This can be achieved only if there is proper infrastructure available with proper mindset.



**Figure 1. Total No. of Cyber Crime Reported [1]**

The trends in this relation are not very good, above graph gives a clear picture of the drastic rise in cyber crime in last 4 years. Cyber crimes reported in the year 2011 are merely 13301 in contrast cyber crime

reported in year 2014 till May is 62189 which might have touched the figure of 149254 approx. till the year end. It estimated that by 2015 cyber crime reported will be around 300000. <sup>[1][2]</sup>



**Figure 2. Sharp growth in Cyber Crime [2]**

It is very much evident that increase in cyber crime will definitely raise the demand of forensics labs and implementation of cyber forensics in the investigation process. Forensics will find the evidence from the digital data at the optimum level and give accurate results; this will help the court to give proper judgment.

**Cyber Forensics: A Process**

- i. As soon as the crime is reported and is registered with the police, investigation starts and data is collected from the place of crime / computer system and is examined using forensic techniques.

- ii. The computer system seized is examined thoroughly to find out the digital data which can act as evidence.
- iii. Important data which can help as a clue or evidence can remain hidden in different file formats like deleted files, hidden files, password protected files, log files, system files etc.
- iv. After all the information is gathered from the computer system original form of evidence is recovered. It must very importantly kept in mind that never to harm the originally recovered data while applying forensics.
- v. Create a mirror image of the original evidence using different mechanism like bit stream etc. and use this mirror image of the original evidence. Never tamper the original copy of evidence for investigation.
- vi. Digital evidences are highly volatile and can be easily misinterpreted so care must be taken be.
- vii. Enough supporting data/information must be gathered before presenting the digital evidence in front of the court of law.

### **Packaging, Transportation and Storage [3]**

Packaging is the process which is done after the computer system is seized at the crime spot. This computer system needs to be packaged properly so that no information is lost. Following steps must be taken care of –

- i. Ensure that the electronic device seized is kept away from the magnetic field, static electricity as this may harm and erase the data inside the system.
- ii. Computer system and the electronic devices seized during the investigation must be labeled, documented and numbered properly.
- iii. Avoid bending or scratches on the electronic devices as this may corrupt the data stored.
- iv. Pack the electronic devices in paper, paper box, and non static plastic bags.

Transportation is the process of carrying the digital evidence from the place of seizure to the place where something can be done about it (cyber forensic labs).

- i. Care must be taken that the digital evidence are carried and transported with care over long distances.
- ii. Extreme weather conditions like too much of heat, cold, moisture can harm the digital data, hence avoid prolonged storage of digital data.
- iii. Avoid shocks and vibrations during transportation.

Data which is collected while investigation is required to be stored for some period of time till the court proceedings do not end. And ultimate care must be taken that this data is not tampered by any means in due course of time otherwise it may change the judgment completely.

- i. Try to store the evidence in the secure place where it cannot be tampered purposely or incidentally.
- ii. Storage place must be dry and with accurate weather conditions like appropriate heat, light, coolness and moisture.
- iii. Batteries have limited life so always keep a note that prolonged storage can harm the important evidences like date, time etc. as if the battery gets weak and then is corrupt the system configuration may change the date and time settings.

### **Outlook of Cyber Forensics in India [4][5]–**

The status of Cyber forensics in India can be viewed from three different angles which are equally important for the growth of the industry.

#### **i. Parliament –**

In India cyber forensics is still a developing field which is somehow getting less importance by our government.

As of now there are no rules and regulation drawn for cyber forensics this makes it difficult to collect the evidences.

The parliament are not very much interested in focusing on the techno-legal issues faced by cyber security, cyber forensics and cyber law.

There are many officials still unaware about the working of digital technology if these key officials of the country are reluctant towards the

technology then its impact will be seen on the growth and development rate of the country.

## ii. **Judicial system**

Judicial system are struggling in giving the judgments because of unstructured cyber law.

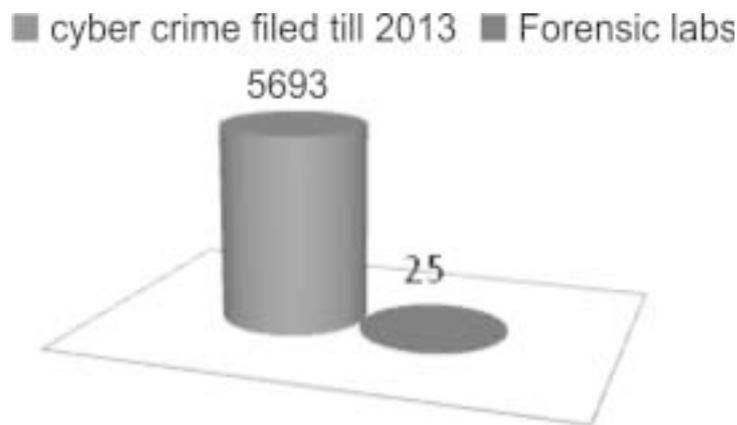
As the Indian cyber law consists of some loopholes it becomes difficult for the judiciary system to take a decision.

## iii. **Police System**

As there are no standard procedures set up to collect the evidence and proceed with forensic.

The police have to face troubles and crisis, also the infrastructural limitation adds to the cause.

India is facing the problem of inadequate research and development infrastructure. The mindset of the people needs to be changed. Current status of Indian forensic labs is –



**Figure 3. Cyber Crime v/s Forensics Lab [6]**

From the above graph even if assume that every state is having at least one cyber forensic lab the ratio of the cyber crime committed and the forensic lab is very poor.

India needs to develop well equipped cyber forensics lab in every major police head quarters. The cyber forensic labs cannot get set up in one strike there has to be a step by step process which is time consuming. There is an absolute need of cyber forensic training institutes in India. There is a need to make policy and train the Police, Lawyers, Judges as well as common man. Education system of India should develop young once with the scientific and research mindset from the school levels.

India needs to concentrate on the development of the legal framework and structured procedures to solve the crime cases and complete the forensics in order to combat cyber crimes.

## **Suggestions and Recommendations**

i. India needs to work in the direction of re framing and re constructing the cyber law.

ii. India needs to formulate the cyber forensics rules and regulation and must have a framework to regulate the policies.

iii. Immediate attention should be drawn towards creating awareness about the cyber forensics among the professionals and the police.

iv. Police Modernization and well equipped infrastructure.

v. Regulations and guidelines for effective investigations.

vi. Scientific approach towards digital data/ evidence.

vii. Research and development mindset should be maintained and inculcated among the young generations.

viii. Government should invest in the infra-structural arrangements for the training and lab equipments.

## References

1. Cert-in reports over 62000 cyber attacks till May 2014 <http://www.livemint.com/Politics/NNuFBA3F2iX4kxIXqKaX2K/CERTIn-reports-over-62000-cyber-attacks-till-May-2014.html>
2. Cyber crimes likely to double to 3 lakhs in 2015 [http://articles.economictimes.indiatimes.com/2015-01-05/news/57705670\\_1\\_cyber-crimes-online-banking-pin-and-account-number](http://articles.economictimes.indiatimes.com/2015-01-05/news/57705670_1_cyber-crimes-online-banking-pin-and-account-number)
3. Rohas N., "Understanding Computer Forensics", Asian school of cyber law, 2009
4. International ICT Policies and Strategies <http://ictps.blogspot.in/2011/06/cyber-forensics-laws-in-india.html>
5. Cyber Forensics and Indian Approach <http://ptlb.in/cfrci/?p=15>
6. Indian Government Agency Received <http://www.medianama.com/2014/12/223-cybercrime-india-2014/>
7. Kazi M., Farooque G., Parab G., "Intellectual Property Rights & Cyber Laws", vipul prakashan, june 2013
8. Cyber Forensic Investigation Solutions in India Are Needed - <http://ptlb.in/cfrci/?p=9>
9. Cyber Forensics <http://www.cyberlawsindia.net/computerforensics1.html>

# General View on the Aspects of Cryptography

Amit Kumar\*

Sonia Kumari\*\*

---

## Abstract

This paper provides the summary of cryptography & the areas where it is used or applied. Information Security is the method or the process to secure the information or data from unauthorized access. Cryptography is one of the methods to protect the data by making the data unreadable from all except users belongs to the category of sender or receiver. Cryptography is the process of secret writing that hides the content of information from all except the sender and the receiver. As the use of technology increase, the probability of cyber-attack may be increase. So cryptography is kind of process that make sure about the data authentication, unauthorized access of data, confidentiality of data and integrity of data.

**Keywords:** Cryptography, Electronic Signature, Hashes, Virtual Private Network

---

## Introduction

Information security plays a vital role during internet communication. When the sender send the data via internet communication channel, there is a probability of loss of data, stealing of data etc. So to protect the data, there are no of methods and cryptography is one of the methods that have a capability to protect the data. Data Security is absolutely essential when communication is carried between lacs of people daily on the internet. There are various cryptography methods that provide the way for secure e-commerce and e-payment on the unsecure channel of internet and protecting passwords. Cryptography is the necessary for protecting the information or in other word for secure communication. This paper provides the types of cryptography and their application.

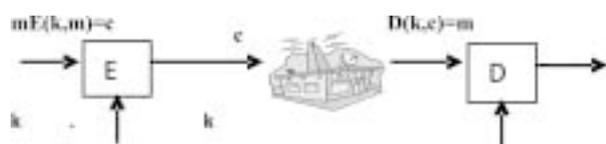
## Cryptography

The word cryptography comes from the Greek words  $\kappaρυπτος$  (hidden or secret) and  $\gammaραφω$  (writing)[1]. The basic service provided by cryptography is the capability to send information between sender and receiver in a way that prevents the information by making it

unreadable from others except sender and receiver. It also provides other services, such as

- Integrity checking—reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source
- Authentication—verifying someone's (or something's) identity But back to the traditional use of cryptography.
- Non-Repudiation—particularly important for financial or e-commerce applications.
- Confidentiality—the biggest concern will be to keep information private.

Original form of message is known as plaintext or cleartext. The meaningless information is known as ciphertext. The process for producing ciphertext from plaintext is known as encryption. The reverse of encryption is called decryption.



E, D: cipher     k: secret key (e.g. 128 bits)  
m, c: plaintext, ciphertext

### Figure 1. Process of encryption & decryption

Encryption is the transformation of data into some unreadable or meaningless form. Its purpose is to

---

**Amit Kumar\***

Scientific Assistant (Adhoc)  
IGIPSS, B-Block, Vikaspuri, Delhi

**Sonia Kumari\*\***

Assistant Professor (Adhoc)  
IGIPSS, B-Block, Vikaspuri, Delhi

ensure privacy by keeping the data hidden from all except sender and receiver. Decryption is the reverse of encryption. It is the transformation of encrypted data back into some intelligible and meaningful form. Encryption and decryption require the use of some secret information, which is a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes about *any* network, particularly the Internet.

### Various Types of Cryptography

#### Public Key Cryptography

*Public-key cryptography* has been said to be the most significant new development in cryptography. Modern PKC was first described publicly by Stanford University professor Martin Hellman in 1976 [2]. PKC is also called *asymmetric encryption*, uses a pair of keys for encryption and decryption as shown in figure 2.



Figure 2: PKC Figure

**PKC** uses two keys, one for encryption and the other for decryption.

With public key cryptography, keys work in pairs of matched public and private keys. The major advantage asymmetric encryption offers over symmetric key cryptography is that senders and receivers do not have to communicate keys up front. Provided the private key is kept secret, confidential communication is possible using the public keys. Encryption and decryption are two mathematical functions that are inverses of each other.

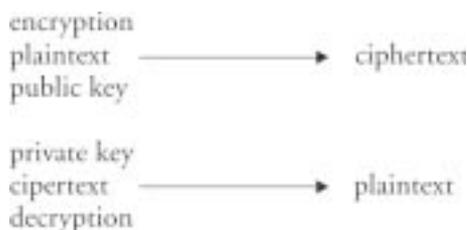


Figure 3: PKC using two keys

There is another thing one can do with public key technology, which is to generate a digital signature on a message. A digital signature is an additional number associated with a message.

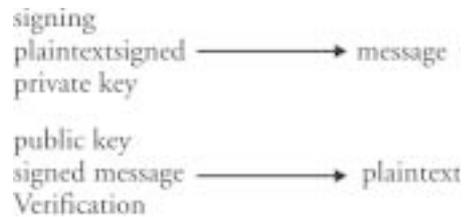


Figure 4: PKC using digital signature

#### Translucent Cryptography

In this scheme the government can decrypt some of the messages, but not all. Only  $p$  fraction of message can be decrypted and  $1-p$  cannot be decrypted.

#### Symmetric Key Cryptography

*Symmetric key* cryptography is also known as Secret key cryptography. In this method of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the key that are used by sender and decrypted by the same key that is used by the receiver. Key must be shared between the sender and receiver as shown in figure 5.



Figure 5: Symmetric key

**SKC** uses a single key “key A” both encryption and decryption.

This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people.

Secret key cryptography schemes are categorized in either *stream ciphers* or *block ciphers*. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block.

## Hashes

Hash functions take data of an arbitrary length (and possibly a key or password) and generate a fixed-length hash based on this input. Hash functions used in cryptography have the property that it is easy to calculate the hash, but difficult or impossible to re-generate the original input if only the hash value is known. In addition, hash functions useful for cryptography have the property that it is difficult to craft an initial input such that the hash will match a specific desired value.

MD5 and SHA-1 are common hashing algorithms used today. These algorithms are considered weak (see below) and are likely to be replaced after a process similar to the AES selection. New applications should consider using SHA-256 instead of these weaker algorithms [3].

## Application of Cryptography

There are number of cryptographic algorithms available that are used to solve the problem related to data confidentiality, data integrity, data secrecy and authentication of data and user. User uses the various algorithms according to the requirement of the work.

### Privacy in Transmission

Current privacy systems for transmission of data use a private key for transforming the data because it is the quicker method with overhead and reasonable assurance.

In case of the number of communicating parties is small, key distribution is done periodically and maintenance of key is based on physical security of the keys.

In case of the number of parties is large, electronic key distribution is used. Usually, key distribution was done with a special key-distribution-key (also known as a master-key) maintained by all parties in secrecy over a longer period of time than the keys used for a particular transaction. The "session-key" is generated at random either by one of the parties or by a trusted third party and distributed using the master-key.

The problem with master-key systems is that if the master-key is successfully attacked, the entire system collapses. Similarly, if any of the parties under a given

master-key decides to attack the system, they can forge all messages throughout the entire system.

With the advent of public-key systems, privacy can be maintained without a common master-key or a large number of keys. Instead, if B wants to communicate with A, B sends A a session-key encrypted with A's public key. A decrypts the session-key and uses that over the period of the transaction.

### Privacy in Storage

Privacy in storage is basically maintained by a one-key system where the user provides the key to the computer at the beginning of a session, and the system then takes care of encryption and decryption throughout the course of normal use. For an example, numbers of hardware devices are available for personal computers to automatically encrypt all information that stored on disk. When the computer is turned on, the user must enter a secret key to the encryption & decryption the hardware. The information cannot be meaningful without key, so even if the disk is stolen, the information on it will not be readable or useable because it is meaningless without the secret key [5].

But there is also a problem in privacy of storage. If the user forgets a key, all information that is encrypted with that key becomes permanently unusable. The information is encrypted while in storage, not when in use. If the encryption and decryption are done in software, or if the key is stored anywhere in the file of system, the system may be circumvented by an attacker [6].

### Integrity in Transmission

Mainly users of communication systems are not as much concerned about secrecy as about integrity. In an electronic funds transfer, the amount sent from one account to another in public domain. How bank is managed and maintained about proper transfers can be made in a proper way. If an active tapper could introduce a false transfer, funds would be moved any other account. Cryptographic techniques are widely used to assure that intentional or accidental modification of transmitted information does not cause erroneous actions to take place.

A technique for assuring integrity is to perform a checksum of the information being transmitted and

also transmit the checksum in encrypted form. Once the information and encrypted checksum are received, the information is again checksummed and compared to the transmitted checksum after decryption. If the checksums agree, there is a high possibility that the message is unaltered. Unfortunately, this scheme is too simple to be of practical value as it is easily forged. So designing strong cryptographic checksums is therefore important to the assurance of integrity.

### **Integrity in Storage**

The mean of assuring integrity of stored information has been access control. Access control means locks and keys, guards, and other mechanisms of a physical or logical. The spread of computer viruses has changed this to a significantly, and the use of cryptographic checksums for assuring the integrity of stored information is becoming widespread.

### **Authentication of Identity**

Simple passwords have been used for hundreds of years to prove identity. More complex protocols such as sequences of secret keys exchanged between sets of end users. Cryptography is the theory and practice of using passwords, and modern systems also use strong cryptographic transforms in conjunction with physical properties of individuals and shared secrets to provide highly reliable authentication of identity.

Practice of Using good passwords falls into the field known as key selection. In essence, a password is a secret key for any cryptosystem that allows encryption and decryption of everything that the password allows access to.

The selection of keys has historically been a cause of cryptosystem failure. Although we know from Shannon that  $H(K)$  is maximized for a key chosen with an equal probability of each possible value (i.e. at random), in practice when people choose keys, they choose easy password that easy to remember, and therefore not at random. This is most dramatically demonstrated in the poor selection that people make of passwords.

On many systems, passwords are stored in encrypted form with read access available to all so that programs wishing to check passwords needn't be run by privileged users. A side benefit is that the plaintext

passwords don't appear anywhere in the system, so an accidental leak of information doesn't compromise system wide protection.

For passwords allowing numbers, lower case letters and special symbols, this goes up considerably. Studies over the years have consistently indicated that key selection by those without knowledge of protection is very poor. In a recent study, 21% of the users on a computer system had 1 character passwords, with up to 85% having passwords of 1/2 the maximum allowable length, and 92% having passwords of 4 characters or less. These results are quite typical, and dramatically demonstrate that 92% of all passwords could be guessed on a typical system in just over an hour.

### **Credential Systems**

A credential is a document that introduces one party to another by referencing a commonly known trusted party. For example, when credit is applied for, references are usually requested. The credit of the references is checked and they are contacted to determine the creditworthiness of the applicant. A driver's license is a form of credential, as is a passport.

Electronic credentials are designed to allow the credence of a claim to be verified electronically. Although no purely electronic credentialing systems are in widespread use at this time, many such systems are being integrated into the smart-card systems in widespread use in Europe. A smart-card is simply a credit-card shaped computer that performs cryptographic functions and stores secret information.

### **Electronic Signatures**

Electronic signatures, like their physical counterparts, are a means of providing a legally binding transaction between two or more parties. To be as useful as a physical signature, electronic signatures must be at least as hard to forge, at least as easy to use, and accepted in a court of law as binding upon all parties to the transaction.

### **Electronic Cash**

There are patents under force throughout the world today to allow electronic information to replace cash money for financial transactions between individual accounts. Such a system involves using cryptography to keep the assets of nations in electronic form. Clearly

the ability to forge such a system would allow national economies to be destroyed in an instant. The pressure for integrity in such a system is staggering.

### **Threshold Systems**

Threshold systems are systems designed to allow use only if a minimal number of parties agree to said use. For example, in a nuclear arms situation, you might want a system wherein three out of five members of the Joint Chiefs of Staff agree. Almost threshold systems are based on encryption with keys which are distributed in parts. The most common technique for partitioning a key into parts is to form the key as the solution to  $N$  equations in  $N$  unknowns. If  $N$  independent equations are known, the key can be determined by solving the simultaneous equations. If less than  $N$  equations are known, the key can be any value since there is still an independent variable in the equations. Any number can be chosen for  $N$  and equations can be held by separate individuals. The same general concept can be used to form arbitrary combinations of key requirements by forming ORs and ANDs of encryptions using different sets of keys for different combinations of key holders. The major difficulties with such a system lie in the key distribution problem and the large number of keys necessary to achieve arbitrary key holder combinations [6].

### **Systems Using Changing Keys**

Shannon has shown to us that given enough reuse of a key, it can eventually be determined. It is common practice to regularly change keys to limit the exposure due to successful attack on any given key. A common misconception is that changing a key much more often than the average time required for break the cryptosystem, provides an increased margin of safety.

If we chose the key at random, and that the attacker can check a given percentage of the keys before a key change are made, it is only a matter of time before one of the keys checked by the attacker happens to correspond to one of the random keys. If the attacker chooses keys to attack at random without replacement over the period of key usage, and begins again at the beginning of each period, it is 50% likely that a currently valid key will be found by the time required to try 50% of the total number of keys, regardless of key changes. Thus if a PC could try all the DES keys

in 10 years, it would be 50% likely that a successful attack could be launched in 5 years of effort. The real benefit of key changes is that the time over which a broken key is useful is limited to the time till the next key change. This is called limiting the exposure from a stolen key [7].

### **Hardware to Support Cryptography**

Basically in history, cryptography has been carried out through the use of cryptographic devices. The use of these devices derives from the difficulty in performing cryptographic transforms manually, the severe nature of errors that result from the lack of redundancy in many cryptographic systems, and the need to make the breaking of codes computationally difficult.

In WWII, the ENIGMA machine was used by the Germans to encode messages, and one of the first computers ever built was the BOMB, which was designed to break ENIGMA cryptograms. Modern supercomputers are used primarily by the NSA to achieve the computational advantage necessary to break many modern cryptosystems. The CRAY could be easily used to break most password enciphering systems, RSA systems with keys of length under about 80 are seriously threatened by the CRAY, and even the DES can be attacked by using special purpose computer hardware. Many devices have emerged in the marketplace for the use of cryptography to encrypt transmissions, act as cryptographic keys for authentication of identification, protect so called debit cards and smart cards, and implementing electronic cash money systems [8].

### **Cryptography in Daily Life**

#### **Emails**

Today, we live in a modern world with the technology. We send emails for general communication with friends, business communication within the companies or with the person whose email address we have. Normally people send billions of emails daily either for the business communication or friendly communication. We deliver the emails through the internet that is a huge big network consisting of a thousands of computers, nodes etc. A number of people like to steal data from others, sometimes it may be for fun, but the data is the main important thing of

any organization. Loss of data is very dangerous for any organization. The first three countries in the highest number of internet users list [8]:

1. China
2. USA
3. JAPAN

There is millions of user who use email service on internet. So the question comes, how do emails get protected while they are being sent?

We all need secure communication. To secure the email service that can be possible if the all connections between routers and routers need to be secured. That is done by using the technique data encryption. There are two methods for this security [9].

1. Use PGP (Pretty Good Privacy). It is a method to secure email, a standard in cryptographically secure emails. It is used with MIME Security.
2. Sender secure their website self, recipient has a username and password. Recipient read the data after logging into the website.

Usually, ISPs can encrypt the process of communication between the sender and receiver by using TLS and SASL protocol. Email server is also using this kind of protection between each other.

TLS is used in different circumstances. TLS is used with POP3 & IMAP services. If HTTP is protected by TLS, it provides more security than simple HTTP.

TLS (Transport Layer Security) and SSL (Secure Layer Security) are very same. Basically TLS is the successor of SSL. They are used for messages, emails, browsing etc. These protocols are used by everyone who use the internet. TLS plays a very important role on the internet. HTTP, FTP, SMTP, NNTP are protocols with TLS protection. TLS uses protocol which is known as reliable connection (like TCP). TLS is commonly used with HTTP to create HTTPS.

In case of VPN, TLS is used to tunneling an entire network. There is number of users use FTP (File Transfer Protocol) for transfer of data between two nodes. There are no of FTP servers and clients available on the Internet. These tools ease our work. If we use the client side, we can manage or organize our download. If we use the server side, manage the user

who can download. FTP use usernames and passwords for the protection but it is vulnerable. FTP is built in a way which provides ability for users on the same network as the transfer is being processed to sniff data including: username, password and files. There is no built-in security or data encryption. A well-known solution for this security problem is to use either SFTP OR FTPS [10].

## VPN

**VPN (Virtual Private Network)** is a virtual computer network. It used virtual circuits or open connections to have the network together. It has a special security system. Authentication is required before connecting with VPN. If we are a trusted user, have a right to access to resources.

Secure VPNs are designed to provide privacy for the users. The essentiality of this consists in cryptographic tunneling protocols. Secure Virtual private Network ensures message integrity, confidentiality and sender authentication.

We use cell phone and telephone to communicate each other. Telephones transmit electric signals over a communication channel that is telephone network. But the problem is that it can easily be eavesdropped. Eavesdroppers require only three things [10] [11] [12]

- a. a pickup device,
- b. a transmission channel
- c. Listening device.

The pickup device is commonly a microphone or a video camera. These devices are used to record sound or to capture video images which later to be converted to electric signals. Data transmit through a link which may be a wire or a radio transmission. A listening device allows monitoring, recording or retransmitting signals.

Mobile phones are used by almost every second man on the earth. Through mobile phones, we use no of services like SMS, MMS, EMAIL, INTERNET, and GAMING AND BLUETOOTH. To protect our self against eavesdropping, we can use the cell phone encrypting devices [13].

## Conclusion

In this research paper we have analyzed of different areas where cryptography is used in our daily activities.

As a normal user, we can easily find cryptography everywhere around us. Emails and Internet are used by more and more people every day. We cannot feel or imagine our lives without it. And all of these work and services are secured based on different types of algorithms of cryptography. The use of technology

is increase in great percentage for daily activities. As the use of technology increase, the probability of steal of data over the untrusted communication channel is also increase. So to prevent the data, different types of encryption & decryption techniques are used.

## References

1. Spenciner, mike, Perlman,r, and aufman.c. “*Network Security:Private Communications in a Public World*”, chapter 2, accessed on December, 23, 2014 on internet.
2. Goyal, Shivangi, “*A survey on the Applications of Cryptography*”, in International Journal of Science and Technology Vol. 1 No. 3, March, 2012, pp. 137-140.
3. Marwaha, Mohit, Bedi Rajeev and Singh, t., “*Comparative Analysis of Cryptographic Algorithm* “, in International Journal of Advanced Engineering Technology, Int J Adv Engg Tech/iv/iii/July-Sep., 2013 pp. 16-18.
4. Gupta, V., and Singh, G., *Advanced Cryptography algorithm for improving data security*, in International Journal of Advanced Research in Computer Science and Software Engineering, volume 2, Issue 1, January, 2012.
5. Panday, L. N., and Shukla, N., “*Visual Cryptography Scheme using Compressed Random Shares*”, in International Journal of Advanced Research in Computer Science and Management Studies, 2013, IJARCSMS, Vol. 1, Issue 4, Sep. 2013, pp. 62-66.
6. <http://nptel.ac.in/courses/106105031/> accessed on December 05,2014 on Internet.
7. <http://williamstallings.com/Cryptography/>accessed on Dec,05, 2014 on Internet.
8. <http://en.wikipedia.org/wiki/Cryptography> accessed on Dec, 10, 2014 on Internet.
9. <https://technet.microsoft.com/en-us/library/cc962027.aspx> accessed on Dec. 21, 2014 on Internet.
10. <http://freevideolectures.com/Course/3027/Cryptography-and-Network-Security> accessed on January, 02 , 2015 on Internet.
11. <http://people.eecs.ku.edu/~saiedian/teaching/Fa10/710/Readings/An-Overview-Cryptography.pdf> accessed on January, 13, 2015 on Internet.
12. Aameer Nadeem, Dr. M.Younus Javed, “*A performance comparison of data Encryption Algorithm*”, in Global Telecommunication Workshops, 2004 GlobeCom Workshops 2004, IEEE.
13. Elkamchouchi, H.M; Emarah, A.-A.M; Hagraas, E.A.A, “*A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes*”, in the 23rd National Radio Science Conference (NRSC 2006).

# A Scalable Server Architecture for Mobile Presence Services in Social Network Applications

A. Radha Krishna\*

K. Chandra Sekharaiah\*\*

---

## Abstract

The use of Social network is becoming gradually more popular on mobile devices. The important component of a social network application is a mobile presence service because it maintains each mobile user's presence information, such as the current status (online/offline), GPS location and network address, and also updates the user's online friends with the information repeatedly. If presence updates occur frequently, the enormous number of messages distributed by presence servers may lead to a scalability problem in a large-scale mobile presence service. We propose an efficient and scalable server architecture, called PresenceCloud, to address the problem, which enables mobile presence services to support large-scale social network applications. PresenceCloud searches for the presence of his/her friends and notifies them of his/her arrival when a mobile user joins a network. For efficient presence searching presenceCloud categorizes presence servers into a quorum-based server-to-server design. Directed search algorithm and a one-hop caching strategy to achieve small constant search latency is also controls by it. The performance of PresenceCloud we scrutinize in terms of the search cost and search satisfaction level. The search cost is characterized as the total number of messages generated by the presence server when a user arrives; and search approval level is defined as the time it takes to search for the arriving user's friend list. The results of simulations demonstrate that PresenceCloud achieves performance gains in the search cost without compromising search satisfaction.

**Keywords:** Social networks, mobile presence services, distributed presence servers, cloud computing.

---

## Introduction

### *Motivation*

Mainly the enthusiasm for doing this project is an interest in undertaking a challenging project in an interesting area of research (Networking). The prospect to learn about a new area of computing not covered in lectures.

### *Problem Definition*

The reason of the ubiquity of the Internet, mobile devices and cloud computing environments can afford presence-enabled applications, *i.e.*, social network applications/services, worldwide. Facebook [1], Twitter [2], Foursquare [3], Google Latitude [4], Buddy-Cloud [5] and Mobile Instant Messaging (MIM) [6], are examples of presence-enabled

applications that have developed quickly in the last decade. Social –Networks services are altering the way in which participants connects to their friends and develop the information about the status of participants including their appearances and activities to interact with their friends. Social network services enable participants to share live experiences instantly across great distances with the social networks like Facebook, twitter etc by the consumption of wireless mobile network technologies. Mobile devices will become more powerful, sensing and media capture devices in the future and we can expect that the social networks services will be the next generation of mobile Internet applications.

A mobile presence service an important component of social network services in cloud computing environments and to maintain an up-to-date list of presence information of all mobile users is the key function. The presence information consist of details about a mobile user's location, availability, activity, device capability, and preferences. The service must

---

**A. Radha Krishna\***

Vasjrs2004@gmail.com

**K. Chandra Sekharaiah\*\***

chandrasekharaiahk@gamil.com

also connect the user's ID to his/her current presence information, as well as repossess and subscribe to changes in the occurrence information of the user's friends.

Each mobile user has a friend list, typically called a buddy list (contact information of other user) in social network services. The mobile user's status is broadcast automatically to each person on the buddy list whenever he/she transits from one status to the other.

It is expected that the number of mobile presence service users will increase significantly in the near future due to the development of social network applications and mobile network capacity. Thus, a scalable mobile presence service is considered essential for future Internet applications.

Distributed paradigms as well as cloud computing applications have been organized by many Internet services in the last decade, .So we explore the relationship between distributed presence servers and server network topologies on the Internet, and intend an efficient and scalable server-to-server overlay architecture called Presence Cloud to develop the efficiency of mobile presence services for large-scale social network services.

Distributed presence architectures in large-scale geographically data centers first we examine the server architectures of existing presence services, and introduce the buddy-list search problem . The *buddy-list search problem* is a scalability problem that occurs when a distributed presence service is teeming with buddy search messages.

### *Objective of the Paper*

In this project, the main objective is to propose a Presence Cloud is scalable server-to-server architecture , that can be used as a building block for mobile presence services. The validation behind the design of Presence Cloud is to distribute the information of millions of users among thousands of presence servers on the Internet. To avoid single point of failure, no single presence server is supposed to maintain service-wide global information about all users.

Presence Cloud organizes presence servers into a quorum-based server-to-server architecture to make

easy efficient buddy list searching. To accomplish small constant search latency it also influences the server overlay and a directed buddy search algorithm; and employs an active caching strategy that reduces the number of messages generated by each search for a list of buddies. Presence Cloud and two other architectures, a Mesh-based scheme and a Distributed Hash Table (DHT)-based scheme We analyzed the presentation complexity .

Through duplications, we also compare the performance of the three approaches in terms of the number of messages generated and the search response time and the buddy notification time. The results demonstrate that Presence Cloud achieves major performance gains in terms of reducing the number of messages without sacrificing search satisfaction thus can support a large-scale social network service distributed among thousands of servers on the Internet.

The role of this paper is threefold.

- First, the original architecture for mobile presence services is Presence Cloud.
- The second role is that we consider the scalability problems of distributed presence server architectures, and characterize a new problem called the buddy-list search problem.
- Finally we consider the concert complexity of Presence- Cloud and different designs of distributed architectures, and evaluate them empirically to demonstrate the advantages of Presence Cloud.

### **Literature Survey**

#### *A study of internet instant messaging and chat protocols*

Instant messaging (IM) and network chat communication have seen an immense rise in popularity over the last several years. This scrutiny helps bridge this gap by providing an overview of the available features, functions, system architectures, and protocol specifications of the three most popular network IM protocols: AOL Instant Messenger, Yahoo! Messenger, and Microsoft Messenger.

The technical characteristics of commercial Internet IM and chat protocols, due to the closed proprietary

nature of these systems. We have presented a taxonomy of different feature and functions supported by most common systems, namely, AOL Instant Messenger (AIM), Yahoo Messenger (YMSG), and MSN Messenger (MSN). AIM supports the most features and thus is the most complex network IM protocol. This may be a result of the fact that AIM has the largest user base of the three systems.

#### *Perceptive instant messaging traffic characteristics*

Due to its quick response time Instant messaging (IM) has become increasingly popular, its ease of use, and option of multitasking. It is estimated that there are several millions of instant messaging users who use IM for various purposes: simple requests and responses, scheduling face to face meetings, or just to check the availability of colleagues and friends and this leads relatively small traffic volume. All major instant messaging systems route text messages through central servers this facilitating firewall traversal and gives IM companies more control, at the IM servers it creates a potential bottleneck. This is especially so for large instant messaging operators with tens of millions of users and during flash crowd events.

Traces due to privacy concerns is another reason in getting access to instant messaging. AOL Instant Messenger (AIM) and MSN/Windows Live Messenger we analyze the traffic of two popular instant messaging systems. We found that most instant messaging traffic is due to presence, hints, or other extraneous traffic. During the overload the IM server can protect the instantaneous nature of the communication by dropping extraneous traffic. We also found that the social network of IM users does not follow a power law distribution. It can be characterized by a Weibull distribution. Our analysis lean-to light on instant messaging system design and optimization and provides a scientific basis for instant messaging workload generation. In the future, we plan to extend the scope of our study by analyzing traces from other user population.

#### *A token-bucket based notification traffic control mechanism for IMS presence service*

The service to inform about the specified state of another user is called as Presence service. The next

generation applications Instant messaging, push-talk and web2.0 are became the key enable for the Presence service. Heavy signaling load on IP multimedia subsystem (IMS) network are caused by the notification traffic of presence service. A Token-bucket based Notification Traffic Control (TNTC) mechanism, which is an application layer solution deployed at the presence server. The aim of TNTC is Upgrading valid access probability while controlling the notification traffic. Extensive replications established that TNTC can effectively control notification traffic and perform better than the existing schemes in terms of valid access probability and update arrival rate.

TNTC which is a token-bucket based notification traffic control mechanism for IMS presence service. The different notification traffic control policy depending on the user class to improve the QoS of presence service.

Extensible messaging and presence protocol (xmpp): Instant messaging and presence describes instant messaging (im), the most common application of xmpp

First effort in creating an open standard for instant messaging and presence information is the Extensible Messaging and Presence Protocol (XMPP). XMPP was introduced by the Jabber Software Foundation (JSF) and formalized in the IETF. Numerous extensions called Jabber Enhancement Proposals (JEP) have evolved through subsequent work. The XMPP/Jabber technology has achieved big success, especially since the IETF approval of the core protocols. It led to significant implementations, major deployments and renewed activity by open-source projects and commercial software developers.

The XMPP/Jabber still has to face challenge from competing technologies, such as SIMPLE. More effort on the gateway development to interoperate with other IM systems.

#### *Peer-to-peer internet telephony using sip*

P2P systems inherently have high scalability, robustness and fault tolerance because of there is no centralized server and the network self-organizes itself. This is achieved at the cost of higher latency for

locating the resources of interest in the P2P overlay network. Internet telephony can be seen as an application of P2P architecture where the participants form a self-organizing and communicate with other participants. Based on the IP telephony system, a pure P2P architecture for the Session Initiation Protocol (SIP) is proposed. The P2P-SIP architecture supports basic user registration, call set up, offline message delivery, voice/video mail, multi-party conferencing, firewalls, Network Address Translation (NAT) traversal and security.

The pure P2P architecture for SIP telephony provides reliability, scalability and interoperability with existing SIP infrastructure. The cost of increased call setup latency is the advantage. By using Chord as the underlying DHT we can propose various design alternatives.

More simulations may not add any research value to the existing simulation results if the implementation is based on the Chord. Large scale application level multicast conferencing using P2P, distributed reputation system for peers, and PSTN interworking related issues such as authentication and accounting are advanced services need more work. The load on public super-nodes is reduced by allowing an internal node inside a firewall and NAT to become a super-node.

#### *Problem statement for sip/simple*

The number of contributions between domains quickly becomes an issue. This document examines the scaling issue and concludes that additional optimizations are necessary. The traffic up to the 50% can reduce by these calculations show that the current suggested optimizations although effective in some circumstances and there is still a very high volume traffic occur in SIP deployments of presence. In order to make the deployment of SIP presence more effective additional optimizations are needed.

#### *OpenVoIP: An open peer-to-peer VoIP and IM system:*

This demo presents OpenVoIP, a 500 node open peer-to-peer VoIP and IM system running on Planet Lab. The three key aspects of OpenVoIP's design are its ability to use any DHT or unstructured peer-to-peer

protocol for directory service, the use of intermediate peers with unrestricted connectivity to relay signaling and media traffic between peers behind NAT and firewalls, and a diagnostic system integrated with Google maps for graphical monitoring. The demo will show these aspects of OpenVoIP and provide approaching on issues and related problems in building such a system.

#### *A weakly consistent scheme for IMS presence service*

Presence service for Universal Mobile Telecommunications System (UMTS) is offered by IP Multimedia Core Network Subsystem (IMS). In IMS, the updated presence information is done by the presence server responsible for notifying an authorized watcher. If any updates occur the presence server will generate many notifications and it consists of weakly schema to reduce the notification traffic and delayed timer is defined for to control the notification rate.

#### *Failover and load sharing in SIP telephony*

For high service availability and scalability to the relatively new IP telephony context some of the existing web server redundancy techniques are applied.

In this various failover and load sharing methods for registration and call routing server based on the Session Initiation protocols (SIP) are compared.

The SIP server failover techniques based on the clients, DNS (Domain Name Service), database replication and IP address takeover, and the load sharing techniques using DNS, SIP identifiers, network address translators and servers with same IP addresses.

We implemented the failover mechanism by using the SIP proxy and registration server and the open source MySQL database.

Network co-location of the servers does not required for the DNS SRV to do redundancy. DNS itself is replicated and Combining DNS with the identifier-based load sharing can scale to large user base.

More work to do failover and load sharing in the middle of the call without breaking the session is need

Call stateful services such as voicemail, conferencing and PSTN interworking. It is difficult for the individual server failover to detect and recovery of wide area path outage. Instead of statically configuring the redundant servers, it will be useful if the servers can automatically discover and configure other available servers on the Internet.

**Chord: A scalable peer-to-peer lookup service for internet**

- Peer -to-peer applications is to efficiently locate the node is a fundamental problem that deals with that stores a particular data item. Chord, a distributed lookup protocol that addresses this problem.
- Data location can be easily implemented on top of Chord by associating a key with each data item, and storing the key/data item pair at the node to which the key maps.
- Chord can answer queries even if the system is continuously changing and easily adapts the nodes joining and leaving of the system.
- Chord is scalable.
- The Chord protocol solves this challenging problem in decentralized manner.
- Only  $O(\log n)$  messages are needed for updating the routing information for nodes leaving and joining.
- Simplicity, provable correctness, provable performance and parallel node arrivals and departures are the attractive features of Chord.

Experimental results confirm that Chord scales well with the number of nodes, recovers from large numbers of simultaneous node failures and joins, and answers most lookups correctly even during recovery.

Chord will be a valuable component for peer-to-peer, large-scale distributed applications, large-scale distributed computing platforms.

**Algorithm 2.1 PresenceCloud Stabilization algorithm**

- 1: /\* periodically verify PS node n's pslist\*/
- 2: Definition:

- 3: pslist: set of the current PS list of this PS node, n
- 4: pslist[].connection: the current PS node in pslist
- 5: pslist[].id: identifier of the correct connection in pslist
- 6: node.id: identifier of PS node node
- 7: Algorithm:
- 8: r •! Sizeof(pslist)
- 9: for i = 1 to r do
- 10: node •! pslist[i].connection
- 11: if node.id 8= pslist[i].id then
- 12: /\* ask node to refresh n's PS list entries \*/
- 13: findnode •! Find CorrectPSNode(node)
- 14: if findnode= nil then
- 15: pslist[i].connection •! RandomNode(node)
- 16: else
- 17: pslist[i].connection •! findnode
- 18: end if
- 19: else
- 20: /\* send a heartbeat message \*/
- 21: bfailed •! SendHeartbeatmsg(node)
- 22: if bfailed= true then
- 23: pslist[i].connection •! RandomNode(node)
- 24: end if
- 25: end if
- 26: end for

**Algorithm 2.2 Buddy Search Algorithm**

For each buddy list searching operation, the directed buddy search of PresenceCloud retrieves the presence information \_ of the queried buddy list at most onehop.

Proof: This is a direct consequence of Lemma 2 and Lemma 3. Before presenting the directed buddy search algorithm, lets revisit some terminologies which will be used in the algorithm.

B = {b1; b2; : : : ; bk}: set of identifiers of user's buddies  
 B(i): Buddy List Search Message be sent to PS node i  
 b(i): set of buddies that shared the same grid ID i  
 Sj: set of pslist[]:id of PS node j

Directed Buddy Search Algorithm:

- 1) A mobile user logs PresenceCloud and decides the associated PS node, q.
- 2) The user sends a Buddy List Search Message, B to the PS node q.

- 3) When the PS node  $q$  receives a  $B$ , then retrieves each  $b_i$  from  $B$  and searches its user list and one-hop cache to respond to the coming query. And removes the responded buddies from  $B$ .
- 4) If  $B = \text{nil}$ , the buddy list search operation is done.
- 5) Otherwise, if  $B \neq \text{nil}$ , the PS node  $q$  should hash each remaining identifier in  $B$  to obtain a grid ID, respectively.
- 6) Then the PS node  $q$  aggregates these  $b(g)$  to become a new  $B(j)$ , for each  $g = S_j$ . Here PS node  $j$  is the intersection node of  $S_q$ . And sends the new  $B(j)$  to PS node  $j$ .

Following, we describe an example of directed buddy search in PresenceCloud. When a PS node 4 receives a Buddy List Search Message,  $B = \{1; 2; 3; 4; 5; 6; 7; 8; 9\}$ , from a mobile user, PS node 4 first searches its local *user list* and the buddy cache, and then it responds these.

### Existing System

In this we describe previous researches on presence services, and survey the presence service of existing systems. To provide presence services Well known commercial IM systems influence some form of centralized clusters. Jennings III *et al.* presented a taxonomy of different features and functions supported by the three most popular IM systems, AIM, Microsoft MSN and Yahoo! Messenger. The authors also provided an overview of the system architectures and observed that the systems use client-server-based architectures. Skype, a popular voice over IP application, GI is multi-tiered network architecture. Since Skype is not an open protocol, it is difficult to determine how GI technology is used exactly. Moreover, Xiao *et al.* analyzed the traffic of MSN and AIM system. They found that the presence information is one of most messaging traffic in instant messaging systems. In, authors shown that the largest message traffic in existing presence services is buddy NOTIFY messages.

### Proposed System

To remove the centralized server, reduce maintenance costs, and prevent failures in server-based SIP deployment the P2PSIP has been proposed. P2PSIP

clients are organized in a DHT system to maintain presence information. The presence service architectures of Jabber and P2PSIP are distributed, the *buddy-list search problem* we defined later also could affect such distributed systems.

It is noted that few articles in discuss the scalability issues of the distributed presence server architecture. Saint Andre analyzes the traffic generated as a result of presence information between users of inter-domains that support the XMPP. Houriet *et al.* Show that the amount of presence traffic in SIMPLE can be extremely heavy, and they analyze the effect of a large presence system on the memory and CPU loading. Those works in study related problems and developing an initial set of guidelines for optimizing inter-domain presence traffic and present a DHT-based presence server architecture.

Recently, presence services are also incorporated into mobile services. For example, 3GPP has defined the integration of presence service into its specification in UMTS. It is based on SIP protocol, and uses SIMPLE to manage presence information. Recently, some mobile devices also support mobile presence services. For example, the Wireless Village consortium and was united into Open Mobile Alliance (OMA) IMPS in 2005 developed the Instant Messaging and Presence Services (IMPS). In, Chen *et al.* proposed a weakly consistent scheme to reduce the number of updating messages in mobile presence services of IP Multimedia Subsystem (IMS). However, it also suffers scalability problem since it uses a central SIP server to perform presence update of mobile users. In IMS-based presence service, authors presented the server scalability and distributed management issues.

### Conclusion

In this paper, we have presented PresenceCloud, a scalable server architecture that supports mobile presence services in large-scale social network services. We have shown that enhance the performance of mobile presence services by PresenceCloud accomplishes low search latency. In addition, we discussed the scalability problem in server architecture designs, and introduced the buddy-list search problem, which is a scalability problem in the distributed server architecture of mobile presence

services. Through a simple Mathematical model, we show that considerably with the user arrival rate and the number of presence servers by the total number of buddy search messages increases. The result of simulations demonstrate that PresenceCloud

achieves major performance gains in terms of the search cost and search satisfaction. Overall, PresenceCloud is shown to be a scalable mobile presence service in large-scale social network services.

## References

1. Facebook, <http://www.facebook.com>.
2. Twitter, <http://twitter.com>.
3. Foursquare <http://www.foursquare.com>.
4. Google latitude, <http://www.google.com/intl/enus/latitude/intro.html>.
5. Buddycloud, <http://buddycloud.com>.
6. Mobile instant messaging, [http://en.wikipedia.org/wiki/Mobile\\_instant\\_messaging](http://en.wikipedia.org/wiki/Mobile_instant_messaging).
7. R. B. Jennings, E. M. Nahum, D. P. Olshefski, D. Saha, Z.-Y. Shae, and C. Waters, "A study of internet instant messaging and chat protocols," *IEEE Network*, 2006.
8. Gobalindex, <http://www.skype.com/intl/en-us/support/user-guides/p2pexplained/>.
9. Z. Xiao, L. Guo, and J. Tracey, "Understanding instant messaging traffic characteristics," *Proc. of IEEE ICDCS*, 2007.
10. C. Chi, R. Hao, D. Wang, and Z.-Z. Cao, "Ims presence server: Traffic analysis and performance modelling," *Proc. of IEEE ICNP*, 2008.
11. Instant messaging and presence protocol ietf working group <http://www.ietf.org/html.charters/impp-charter.html>.
12. Extensible messaging and presence protocol ietf working group. <http://www.ietf.org/html.charters/xmpp-charter.html>.
13. Sip for instant messaging and presence leveraging extensions ietf working group. <http://www.ietf.org/html.charters/simplecharter.html>.
14. P. Saint-Andre., "Extensible messaging and presence protocol (xmpp): Instant messaging and presence describes instant messaging (im), the most common application of xmpp," *RFC 3921*, 2004.
15. B. Campbell, J. Rosenberg, H. Schulzrinne, C. Huitema, and D. Gurle, "Session initiation protocol (sip) extension for instant messaging," *RFC 3428*, 2002.
16. Jabber, <http://www.jabber.org/>.

# “Aadhar” Management System

Ameer Ulla Siddiqui\*  
Mr. Hare Krishna Singh\*\*

---

## Abstract

The AADHAR Management System provides a 12-digit unique number for every Indian individual, including children and infants. The AADHAR number will be in the form of 12 digit alphanumeric number to provide more security. AADHAR Number which would not just help the government track down individuals, but would make life far easier for citizens as they would not have to submit multiple documents each time they want to avail a new public, private and government service. This system will contain personal details like name, sex, address, marital status, photo, identification mark, fingerprint biometric, iris (uniqueness of human eye patterns) and signature. AADHAR Management System helps to manage persons needs in his/her life span by using a single UID i.e. the number is used as Driving license number, Voter ID card number, registration number in any organization, bank account number, personal or professional details. AADHAR will provide a universal identity infrastructure which can be used by any identity-based application (like ration card, passport, etc.)

**Keywords:** AADHAR, Information security (IS), Unique Identification Numbers, UID, E-Government

---

## Introduction

This system is to provide a unique ID to each and every citizen of India while providing him/her a birth certificate. Citizens after attaining age of 18 must register at the RTO office or Collector office or Tahsildar office and get a password to access the site. ID card will be provided to every user after registration. Later on they can change their password. Once they enter the site they can pay their electricity bill and telephone bill, book railway tickets and airline tickets and pay their taxes. During elections people can poll online. Government officials can verify details about a person from the database for issuing vehicle license, passport, visa, etc.

Unique Identification Authority of India (UIDAI):

The UIDAI is the government project and name for the project is “AADHAAR” means “support”.

---

### Ameer Ulla Siddiqui\*

Computer Assistant, UGC-HRDC,  
Jamia Millia Islamia, New Delhi

### Mr. Hare Krishna Singh\*\*

Software Engineer,  
HCL Infosystem, New Delhi

Unique Identification Management (UIDM):

The UIDM that creates a unique identification number to a particular citizens of state/country.

## Background of the Aadhaar Management System

In India steps in this direction began with, ‘Kargil Review Committee Report’ submitted in January 2000. The committee recommended that ID cards be issued immediately to people in border districts to prevent infiltration and find out illegal immigrants. Based on this a Group of Ministers in a report titled Reforming the National Security System noted “All Citizens should be given a Multipurpose National Identity Card (MNIC) and noncitizens should be issued identity cards of a different color and design”. Acting upon the report Government of India initiated a process for the creation of the National Register of Citizens in 2003.

## UIDAI

UIDAI is expected to provide a link across diverse identities as a citizen, so that once one has it, the Govt. needs nothing more from one, because it can find the links on its own. AADHAAR signifies ‘foundation’ or ‘support’ and communicates the fundamental role of UID initiative and its impact.

### *Applications of UIDAI*

AADHAAR assurance of uniqueness and centralized online identity verification would be the basis of building multiple services and applications -

- It can substitute all other identified issues, including illegal migration, in banking and financial transactions, fraud, health related matters, in the education sector, welfare sector, in the election process, monitoring efficient law and order.
- It is easy to count country's population without any mistakes and take an action to control population which gradually increase in excess amount.
- It will provide support in providing proper identification to the individuals and this UID will be linked with a person's Passport Number, Driving License, PAN card, Bank Accounts, Voter ID etc. and all this information will be checked through a database.

### *Risks in the implementation of UIDAI*

Risks that arise from this centralization include possible errors in the collection of information, recording of inaccurate data, corruption of data from anonymous sources, and unauthorized access to or disclosure of personal information.

The centralized nature of data collection also heightens the risk of misuse of personal information and therefore potentially violates privacy rights. The creation of a centralized database of personal information, it is imperative that such a programme not be established without the proper mechanisms to ensure the security of each individual's privacy rights. As we considered for India, The population of India is more than 5 billion, so Network traffic has to be controlled but is it very tedious task .also we have to increase the bandwidth spectrum and connectivity.

### **UIDM**

The UIDM system is to develop Unique-id management that creates a unique identification number of particular citizen of the country. As well as management of perspective data, information of that citizen. Secondary goal is that we provide his feature

in some project, which are trying to help people to achieve/reduces their stress of normal life. Basically the UIDM system which is handled by a moderator, according to recent work the "Aadhaar" management system which is developed for providing Unique-id. This system not provides different feature. This system can be accessed by the citizen, and different people related to governmental activity, so we try to achieve simple interface, and user friendly system.

### *Design and Architecture*

We describe the Algorithm, which is used to explain how the system is going to work, i.e. the process logic behind it, the flowchart, which represents the pictorial representation of the process logic and finally the Data Flow Diagram (Context Level) of the UIDM system.

### *Algorithm:*

Security mechanism in UID project - if there is no physical Identity card or electronic smart card, then how will UID system validate its citizens. For implementing this, two different processes have to follow, the first one being the recording process and the second one - the authentication process.

### *Recording Process:*

In the first process, the UIDM builds up a centralized database consisting of UID, biometric record and various other details of the person. The UIDM allocates a unique 12 digit alpha numeric number (UID) which is randomly generated by the main computer to every citizen. Then a biometric data record is made by scanning the 10 fingerprints of a person. This biometric data is tagged to the person's unique 12 digit number (UID). The UID tagged to the biometric record of a citizen is later used in the authentication process.

### *Authentication Process*

In the second process, whenever a person has been identified whether he/she is a genuine one, a fresh biometric scan is made and then the scanned image is sent to the centralized server. The server took the fresh scanned biometric image as an input and compares it with all the already stored biometric records in the database. If a relevant match found is found, then the person is designated to be a genuine citizen.

**Advantages**

Manage all the details related to the Bank account, Driving License, Vehicle registration, Voter ID card, Medical records, education and profession, passport, PAN card in one database. A single unique number is used therefore decreasing manual labour and increasing efficiency as every detail is available on the single click and reducing the efforts in maintaining different ID databases. The UID will reduce the duplication, an attempt to make fake documents.

The purpose of this UID system is to provide one unique number to all the citizens to increase the security and verification process by introducing the Biometric authentication technology, and thus identifying illegal immigrants and terrorists.

Along with UID various facilities provided in the system, like paying their electricity bill and telephone bill, book railway tickets and airline tickets and paying their taxes. During elections people can poll online. If a person commits a crime, his/her details will be added to the crime database. This will be useful for embassy, employment exchange and CBI officials.

**Disadvantages**

The disadvantage of this system is that the network has to be very quick and crash free which is not possible. As at a time there will be many citizens who will be working on the system.

Security is the biggest task in this system as each and every possible security measures will have to be taken.

**Biometrics**

Electronic scanning and matching technologies are not 100 percent error-free. Since biometrics is not an exact science, the problem is not only is the underlying data flawed, even the biometric technologies have some error rates. At the time of purchasing biometric scanning equipments, it is important to include a clause mentioning the calibration requirements.

While biometric data in digital format are the norm in the modern day authentication process, choosing the right type of scanning device is more important. While fingerprinting is the most straight forward biometric available in the market. The erosion of fingerprints of people who are involved in heavy

physical labour being affected over a period of time is one such challenge.

**Iris Technology****Overview**

While the benefits of using iris biometrics are important to consider, not much is known about how iris biometric systems function. Here, the paper provides an overview of iris biometrics and the technology that is used.

The iris of the eye is a protected organ, which controls the diameter of the pupils – the center part of the eye - and the amount of light entering the eye.

The front, pigmented layer of the iris, contains random patterns that are visible and highly stable. These patterns are also highly intricate, and unique to every individual. The iris, faces very little wear, and can consequently serve as a secure, always available passport that an individual can present for verification.

The field of iris biometrics has seen significant research and investment over the last decade, and at this point, iris capture has become a mainstream technology with wide acceptance. In India, over 50 million people have been enrolled using iris recognition systems in Andhra Pradesh and Orissa. Feedback on these systems has been positive both from enrolling agencies and state government officials. Mexico is also using iris for its version of Unique ID to deliver public benefits to its entire population.

De-duplication through iris has been carried out on a large scale – one implementation that de-duplicated the entry of immigrants into a country has carried out five trillion iris comparisons since 2001. In Andhra Pradesh, the government has carried out 6.26 quintillion matches in two months for its PDS programs in 2009.

According to one research firm, iris is the fastest growing segment of biometric market and will have the largest market share in next ten years. Responding to the increased demand, the technology has become rapidly cheaper, with a friendlier user experience.

***How do we capture the iris image?***

The capture of the iris image is identical to taking a regular photograph, except that it operates in the infrared region, nearly invisible to our eye. The camera

captures the image of the iris; the image generated is permanently stored in the database, and is used for matching while verifying the identity of the resident, as well as for de-duplication.

### *Devices used for iris capture*

The devices that are used for capturing the iris image depends on the purpose - whether it is for enrolling a resident, or for identity authentication. There are two main types of devices that are commonly used: hand held and wall mounted.

Wall mounted devices, which are an older version of the iris device, are usually used for access control applications. Newer, hand held and mobile device is used for e-governance applications, and iris enrollment. The devices presently being tested by the UIDAI is mobile devices suitable for enrolling people in rural and remote areas.

### **Conclusions**

AADHAR Management System will be beneficiary to the citizens as it is a unique number which contains

basic information of every person. After the ID will be issued there is no need to carry driving license, voter cards, pan card, etc. for any government or private work. For example, for opening a new account one has to show his/her Unique ID only. But to some extent it is harmful to the general public as all the data related to them is stored on computers and can be misused by hackers if the multiple security strategies will not be adopted. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

The role of this system envisions is to issue a unique identification number (UID) that can be verified and authenticated in an online, cost-effective manner, and that is robust enough to eliminate duplicate and fake identities.

### **Acknowledgment**

Our thanks to Mr. Javed Ahmad, who has contributed towards the development of this Research Paper on AADHAR Management System.

### **References**

1. www.uidai.gov.in Background Section as on 14/11/2012.
2. Business Standard (2009, June 25, 2009). Nandan M Nilekani Appointed as Chairperson of UIDAI. Business Standard. Retrieved January 10, 2011
3. Discussion Paper on Aadhaar based Financial Inclusion, UIDAI.
4. <https://aadhaar.uidai.gov.in/>
5. R. Ramkumar, Aadhaar: On a Platform of Myths, The Hindu, 08/07.2011.
6. UIDAI (n.d.). UID and PDS System: Unique Identification Authority of India, Planning Commission, Government of India.
7. UIDAI (2012). Aadhaar Enabled Service Delivery. Planning Commission, Government of India document.
8. Discussion Paper on Aadhaar based Financial Inclusion, UIDAI.

# A Survey on Honeypots Security

Amit Kumar\*

Sonia Kumari\*\*

---

## Abstract

With the increasingly use of computer technology and the Internet, information security becomes more important. The tradition defense mechanism to detect the security risk has been unable to meet the requirement of the people. The honeynet technology as a protection technology to make up for the traditional system. This research paper describes a brief review on network security techniques, Honeynet and Honeypot Technology. A Honeypot is a process of deception trap. It is structured to lure an attacker into intending compromise the information systems in an organization. But it is required a correct deployment, if it is deployed correctly, can serve as an early-warning system and advanced security surveillance tool. It minimize the risks from attack. It is also analyses the ways in which attacker try to compromise an information and networks system, providing valuable insight into potential system loopholes. This paper gives idea how honeypot technology can be used to detect, identify and gather information for a specific threat & how it can be deployed for the purpose to enhance the level of security in organization and enterprise.

**Keywords:** Honeynet, Honeypot, Honeywall, Intrusion Detection

---

## Introduction

Basically, information security is the primarily defensive process. Administrator of the Network use a firewall, intrusion detection system (IDS) and number of information security method to protect their network from data breaches, intruders etc. The firewall control the inbound and outbound traffic according to the policies that has been configured as required for the particular system. The intrusion detection system (IDS) deployed between the local area network and the internet for detecting suspicious packets.

Every technology have some deficiencies of these systems. In case of firewall [1]:-

1. It cannot protect the system against an attacks that bypass it. For example, dial in or dial-out capability.
2. The firewall does not protect against internal threaten the network.

---

## Amit Kumar\*

Scientific Assistant (Adhoc)  
IGIPSS, B-Block, Vikaspuri, Delhi

## Sonia Kumari\*\*

Assistant Professor (Adhoc)  
IGIPSS, B-Block, Vikaspuri, Delhi

3. The firewall does not protect against the transfer of virus files and programs.

In case of Intrusion Detection Systems (IDS) [2]:-

1. High level of false positive and false negative alerts.
2. Must know signature detection patten [3].

The use of honeypots can overcome the deficiencies of intrusion detection system (IDS) and Firewall. The main advantage of honeypots is that they are designed for the interaction with attackers. This is the way honeypots collect smaller set of data with very high value. But there are also some deficiencies like others technologies. If we install honeypots behind the firewall and intrusion detection system (IDS), it can serve as part of defense in-depth system and can be used to detect attackers. It is called a honeynet.

## Honeynet

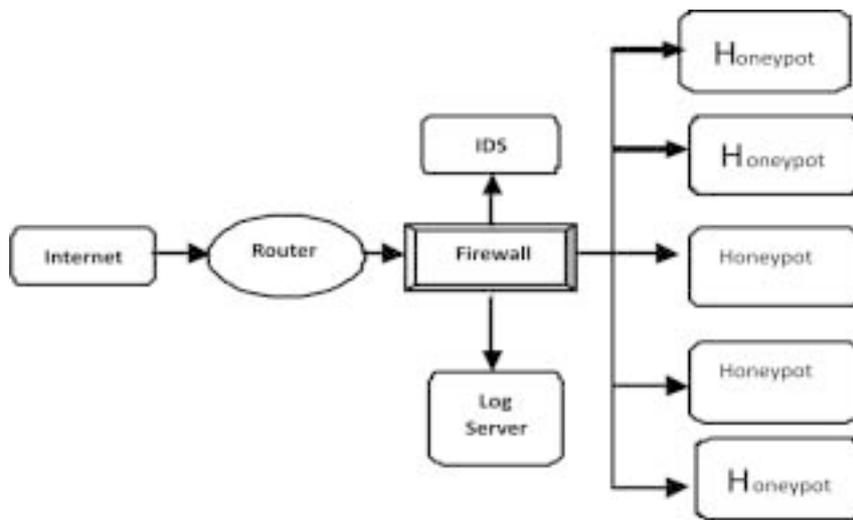
The concept of the honeynet technology was started first in 1999 after the published of paper named "To Build a Honeypot" by Mr. lance Spitzer, founder of the Honeynet technology. In his paper, Mr. Spitzer says that instead of developing technology that emulated systems to be attacked, why we do not install system behind the firewall that waiting to be hacked. Honeynet are neither a product nor a software

solution that it install on the software. Basically honeynet is a architecture that create a highly controlled network in which all activity is controlled and captures in a proposed manner [4][5]. By doing together with firewall, intrusion detection system(IDS), and anti-worm software, honeypots form into a honeynet security defense system that ensure

about the network security as shown in the figure 1.

Basic elements of Honeynet are:

1. A firewall computer
2. Intrusion Detection System (IDS)
3. Log server
4. Honeypots



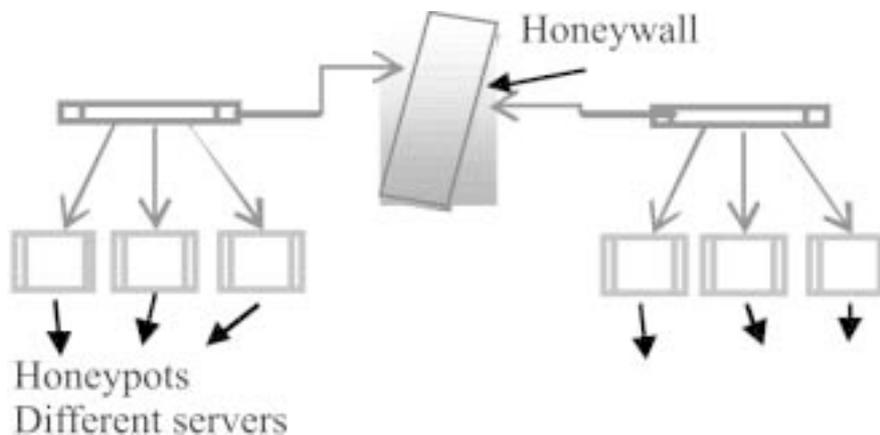
**Figure 1: Network Security**

Honeywall [6] is a key to design of honey net, all the data that access to the honey net must go through the honey wall and it separate the honey network and external network which is control the entire honey net network hub as shown in figure 2. It has three network interfaces.

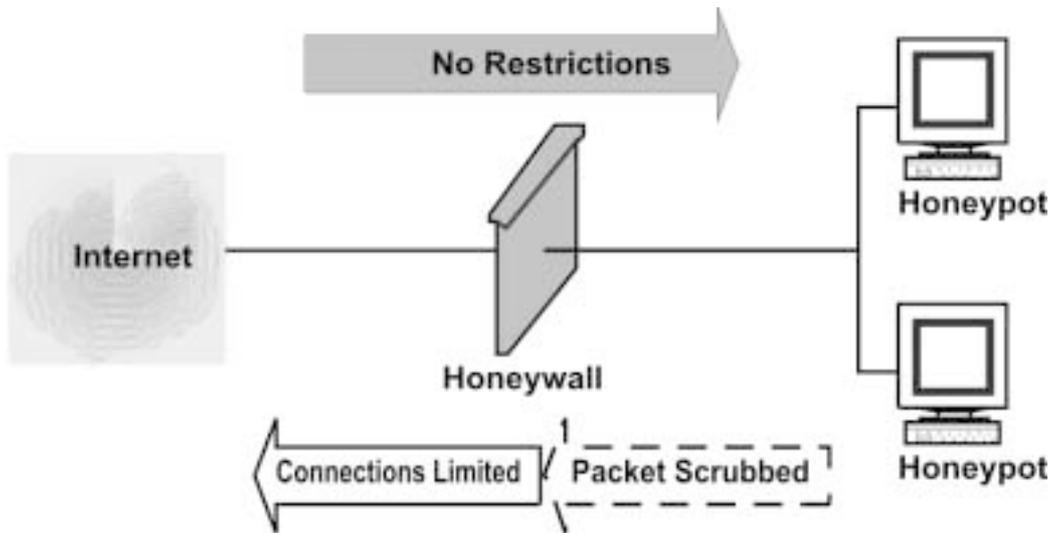
1. External Network interface that connected with service host.

2. Internal Network interface that connected with the honeynet.
3. Network Interface connection logging server that connected with internal network interface.

Honeywall facilitate the remote management and intrusion prevention system detection rules and policies for timely updates.



**Figure 2: Honeywall Network Hub**



**Figure 3: Honeyball**

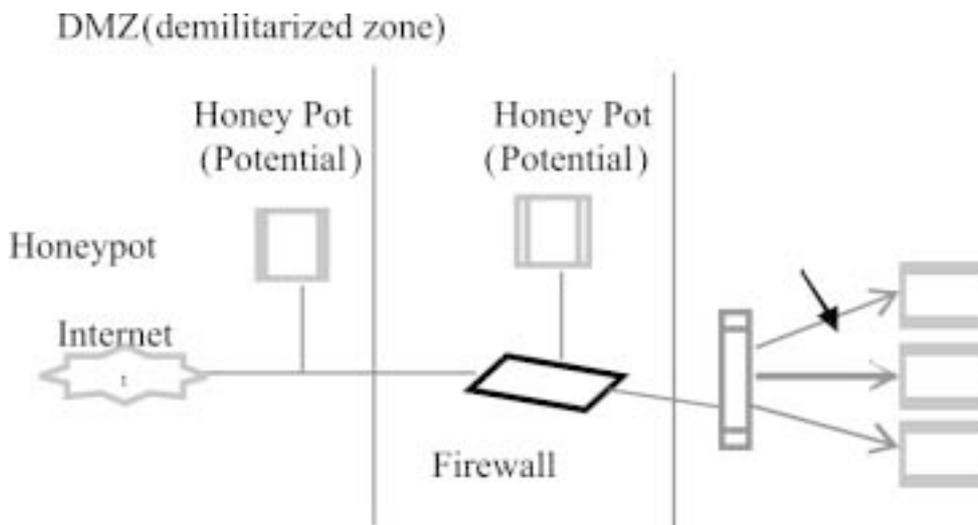
Basic Requirement for the implementation of honeynet:-

1. **Data Control** is the containment of activity that mitigates the risk. We always try to ensure that once an attacker is found within our honeynet accidentally or purposefully harm the other honeynet. This is more challenging scenario as shown in figure 3.
2. **Data Capture** is the process of monitoring and logging of all of the threat's activities within the honeynet or system. The challenge is to capture the data without the threat.

3. **Data Analysis** is another detection of worthless if do not have an ability to convert the data. We must have some ability to analyze the data.
4. **Data Collection** applies to those organizations that have multiple honeynets in distributed environments.

**Honeypot**

Lance Spitzner, founder of the Honeynet Project said that a honeypot is a system structured to learn how “black-hats” enquiring for and utilize weaknesses in an IT System [7]. It can also be defined as “an



**Figure 4: Honeypot**

information system resource whose value lies in unauthorized or illicit use of that resource” [8]. In other words, it is a lure, put out on a network as bait to attract the attackers. Honeypots are a virtually machines that has been designed to imitate real machines.

A Honeypot works by making fool the attackers into believing that it is legitimate system, as they attack the system without knowing that they are being observed covertly. When an intruder try to attempts to compromise a honeypot, attack-related information, like IP address of the intruder, will be captured.

It can be used for the purpose of production or research. A production honeypot is used for risk mitigation.

Research Honeypots are the example of real operating systems and services that intruders can interact with the system. That’s why it involves higher risk. They collect huge information regarding the situation of the types of attacks being execute. It provides the more improved attack prevention and attack detection information captured during the process.

### **Classification of Honeypots**

Honeypots are classified into two categories. These are the following.

1. Low-interaction honeypots: It is used for production purposes.
2. High-interaction Honeypots: It is used for research purposes.

#### *Low-Interaction Honeypots*

It is work by imitating the certain services and operating systems and have a limited interaction.

#### **Advantages**

The advantages of low-interaction honeypots are that they are simple and easy to deploy and maintain. In addition, the limited emulation available or allowed on low-interaction honeypots reduces the potential risks brought about using them in the field. However, with low-interaction honeypots, only limited information can be obtained, and it is possible that experienced attackers will easily recognize a honeypot when they come across one.

#### **Example:**

##### **Facades:**

It is a kind of software emulation of a selected services or application that provides a wrong perception of a selected host. When a façade is attacked, it collects the data about the intruder. Some facades provide partial application-level behavior and some others simulate the target service.

Facades provide easy installation as it requires minimal installation effort and devices. It can emulate a large variety of systems. We know that, it is not a real systems, it does not have any other real vulnerabilities themselves. It is used by small to medium sized organization or by big organization in coordination with other types of security technology because it provides only basic information about a potential threat.

#### *High-Interaction Honeypots*

High-Interaction honeypots are complex as compared with the low-interaction honeypots because it uses a real operating systems, services and applications. For example, a SSH server will be built if the objective is to collect the information about attacks on a particular SSH server or services.

It is a kind of system policies that provides the real system for direct interaction to the attackers. There are not any kind of restriction are imposed on attack behavior. This model allows administrator to gather extensive information about the attacker’s method. Enough protection measures need to be implemented as required in the system.

#### **Example:**

##### **1. Sacrificial Lambs**

It is a system intentionally left vulnerable to attack. The administrator will examine the honeypot to determine if it has been compromised and if so what was done to it.

##### **2. Instrumented Systems**

It is an off-the-shelf system with an installed operating system and kernel level modification to provide information, containment, or control. The OS and kernel have been modified by engineers of security. After the modification in operating system and kernel,

the running system will leave the in the network as a real target. This model combines the strengths of both sacrificial lambs and facades.

### 3. Spam Honeybots

Honeybot technology is used for identifying spam and email harvesting activities. Honeybots have been installed to study how spammers detect open mail relay system. Machine run as simulated mail server proxy server and web server. Spam email is received and analyzed [9].

#### Strategies of honeybot deployment

For minimize the risk and maximize the soundness of the honeybots, it is required the installation should be carefully planned.

1. Honeybots install with the production server. The honeybot need to mirror the original information and services from the production server in order to lure the intruders. In that model, honeynet security loosened slightly that increase the probability of being compromised. The honeynet capture attack related data. When a successful attack takes place on the honeybot within the network, that compromised honeybot machine may be used to scan for other threat target in the network. The main drawback of implementing honeynet within the production system.
2. Paired the servers with a honeybot. It routed the suspicious traffic destined for the server to the honeybot. For example, traffic on port number 80 on TCP can be directed to a web server IP address as normal and other traffic to the web server will be routed towards the honeybot.
3. Build a Honeynet: It is a collection of honeybots that imitate and mirror an original network. This will show to intruders as if different types of application are available on several platforms. A honey net provides an early warning system against the attacks and offers a good way to analyses the intruder's intention. The Honeynet Project [10] is an excellent example of a research honeynet.

#### Building the Network of Honeybot

Building a honeybot network is not difficult. I build it at my college computer lab and it has been successfully intruded number of times.

I used window 8 system with a DVD-ROM drive. It was the best as compared others that is available as it is more secured.

I install a program called Snort. This program is an open source network intrusion prevention and detection system that is utilizing a rule-drive language. It is combines the benefits of signature, protocol and anomaly based inspection methods. Snort is the most popular and widely deployed intrusion detection and prevention technology. In fact, it has the standard for the industry. Snort is a free program that is extremely powerful. This is part of an intrusion detection system.

I also found Windows based Honeybot that is HoneyBot. It works by opening on 1000 UDP and TCP listening sockets on computer and these sockets are designed to mimic vulnerable Services. When an attacker connects to these services they are fooled into thinking they are attacking a real server. The honeybot safely captures all communications with the attacker and logs these results for future analysis.

#### Examples of Honeybot

1. Deception Toolkit [11]: DTK was the first open source honeybot. It is a collection of Perl scripts and c code that emulates a variety of services.
2. LaBrea [12]: It is structures to slow down or stop attacks. It can run on Windows or UNIX.
3. Honeywall CDROM [13]: It is a bootable CD with a collection of open source software. It makes honeynet deployments simple and effective by automating the process of deploying a honeynet gateway known as a honeywall. It is used to capture, control and analyses all inbound and outbound honeynet activities.
4. Honeyd [14]: This very powerful, low-interaction honeybot. It is run on both UNIX and windows platforms. It can monitor the IPs that is unused, simulate thousands of virtual hosts at the same time and monitor all UDP and TCP based ports.
5. Honeytrap [15]: It is a low-interaction honeybot technology that is designed to observe attacks against network services. It helps administrators to collect information regarding known or unknown network-based attacks.

6. HoneyC [16]: It is a client honeypot that initiates connections to a server. The main objective of that technology is to find malicious servers on a network.
7. HoneyMole [17]: It is a tool for the deployment of honeypot farms, or distributed honeypots, and transport network traffic to a central honeypot point where data collection and analyses can be undertaken.
8. Symantec Decoy Server [18]: This is a type of honeypot intrusion detection system that detects and monitors unauthorized access and system misuse in real time.
9. Specter [19]: It is a smart honeypot-based intrusion detection system. It can emulate 14 different operating systems and have acceptability to monitor 14 different network services and trap.

## Result

The result was too good. It was surprising to see how fast the computer was attacked. I let it run for eight hours and found port 162 got quite a bit of scanning while port 67 and 68 were occasionally hit as well. Port 162 is commonly known as SNMP (simple network management protocol) trap. It looks every 3 to 5 seconds, ports were being scanned to see if they were open or closed. This was my first experience using a honeypot on a system.

## References

1. Holostov, V., Neystadt, John, "Automated identification of firewall malware scanner deficiencies, in United State Patent Application Publication, Published date Sep., 18, 2008.
2. <http://cryptome.org/sp800-31.htm> accessed on January 8, 2015 in the Internet
3. Renuka Prasad B et al., "Hybrid Framework for Behavioral prediction of Network Attack using Honeypot and Dynamic Rule Creation with Different context for Dynamic Blacklisting", RV college of Engineering, Bangalore, Karnataka, IEEE, I.S.B.N : 987-14244-5726-7, pp-471-476.
4. Ryan Talabis, "Honeynets: A Honeynet Definition:, A Student IT Security Awareness Initiative by the Philippine Honeynet Project.
5. "Know Your Enemy : Honeynets.", Honeynet Project.
6. Peng Hong et al. "Intrusion Prevention system in the Network of Digital Mine" Chine University of Mining Mechanical and Electrical Engineering Beijing, Chine IEEE, 2010, Vol. 6, pp:296-299.
7. <http://rootprompt.org/article.php3?article=210> accessed on Jan 25, 2015 on the Internet.

## Conclusion

As the growing IT field, there is a requirement to strengthen its security. Preventive and Detective method measures used to improve IT Security. To improve our Security, we must have a knowledge of intruders, attackers, hackers, etc. Hackers can hack our computer. Attackers are constantly scanning our network looking for vulnerable loopholes and open ports. But without the knowledge of the enemy, we cannot defend our network or system. We have to think like a hacker in order to stop a hacker. Honeypots can be used simply to confuse and deflect attacks or to collect evidence. There are many free Windows based and Linux based honeypot programs available to individuals and companies.

Honeypots is a technology. Every technology has its advantages and disadvantages as this is possible in honeypots like other technologies. It is a useful tool for deception and apprehend the intruders that ensnare the information and create alerts when someone is trying to interact with them. This takes of intruders provides the valuable information for analyzing their attacking mode of techniques and methods. Because honeypot capture and collect data.

There are some disadvantages of that technology. It only track and capture activity that directly interacts with them. It cannot detect that attacks against other systems in the network. This is possible to be the most controversial drawback of honeypots.

8. <http://www.spitzner.net/honeypots.html> accesses on the Internet.
9. <http://www.honeyd.org/spam.php> accessed on jan 25,2015 on the Internet.
10. <http://www.honeynet.org> accessed on Jan 26, 2015 on the Internet.
11. <http://www.all.net/dtk/index.html> accessed on Jan 26, 2015, on the Internet.
12. <http://labrea.sourceforge.net/labrea-info.html> accessed on Jan 26, 2015 on the Internet.
13. <http://www.honeynet.org/tools/cdrom/> accessed on Jan 27, 2015 on the Internet.
14. <http://www.honeyd.org> accessed on Jan 27, 2015 on the Internet.
15. <http://honeytrap.mwcollect.org> accessed on Jan 27, 2015 on the Internet.
16. <http://www.client-honeynet.org/honeyc.html> accessed on Jan 28, 2015 on the Internet.
17. <http://www.honeynet.org.pt/index.php> accessed on Jan 28, 2015 on the Interenet
18. <http://www.symantec.com/business/support/documentation.jsp?language=english&view=manuals&pid=51899> accessed on Feb 1, 2015 on the Internet
19. <http://www.specter.com/default50.htm>.

# Security Features of User's for Online Social Networks

A. Radha Krishna\*

K. Chandra Sekharaiah\*\*

---

## Abstract

In recent years Online social networks (OSNs) have practiced fabulous growth and become a genuine portal for hundreds of millions of Internet users. These OSNs provides attractive ways for digital social interactions and information sharing, but also raise a number of security and privacy issues. OSNs allow users to control access to shared data, they currently do not provide any method to enforce privacy concerns over data connected with multiple users. To this end, we suggest an progress to enable the protection of shared data associated with multiple users in OSNs. . We formulate an access control model to capture these sense of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model that allows us to influence the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof-of-concept prototype of our approach as part of an application in Facebook and provide usability study and system evaluation of our method.

**Keywords:** Multiparty Access Control, Multiparty Policy, Online Social Network

---

## Introduction

### *Motivation*

The motivation for writing this paper is primarily an interest in undertaking a challenging task in an interesting area of research (Networking). The opportunity to learn about a new area of computing not covered in lectures.

### *Problem Definition*

The rising of the technology made the communication more easier for the people who are far from us by communicating through the social networks like Facebook, twitter etc., These social networks are mainly used for different activities such as education, business, entertainment etc., But using these social networks there are some troubles like security, privacy etc.

Several benefits of this paper introduces are cut detection capability, suppose if a sensor wants to send data to the source node has been disconnected from the source node. Without the knowledge of the

---

**A. Radha Krishna\***

vasjrs2004@gmail.com

**K. Chandra Sekharaiah\*\***

chandrasekharaiahk@gamil.com

network's disconnected state, it may simply forward the data to the next node in the routing tree, which will do the same to its next node, and so on. However, this message passing merely wastes precious energy of the nodes; the cut prevents the data from reaching the destination.

Therefore, on one hand, if a node were able to detect the occurrence of a cut, it could simply wait for the network to be repaired and eventually reconnected, which saves on board energy of multiple nodes and prolongs their lives. On the other hand, the ability of the source node to detect the occurrence and location of a cut will allow it to undertake network repair.

Thus, the ability to detect cuts by both the disconnected nodes and the source node will lead to the increase in the operational lifetime of the network as a whole.

### *Objective of the Paper*

- Platforms are allowing people to publish their details about themselves and to connect to other members of the network through links so now a days Online Social Networks (OSNs) are becoming more popular eg: Facebook used by hundred million active users.

- The subsistence of OSNs that include person specific information creates both interesting opportunities and challenges.
- On the other hand, simply making a user able to decide which personal information are accessible by other members by marking a given item as public, private, or accessible by their direct contacts by very basic access control systems of current OSNs put into service .
- In order to provide more flexibility, some online social networks implement variants of these settings, but the principle is the same.

### *Objectives*

- a. Safety measure policies.
- b. Unconstitutional access control
- c. To identify their permission provide policy and privacy for multiple user
- d. Discover potential nasty activities using collaborative control
- e. An Online Social Network with User- Defined Privacy.

### **Literature Survey**

- Online Social Networks (OSNs) have seen major growth and are getting much consideration in research in recent years. Social Networks have always been an important part of daily life.
- Because of the public nature of many social networks and the Internet itself, content can easily be disclosed to a wider audience than the user intended. Limited experience and awareness of users, as well as the lack of proper tools and design of the OSNs, do not help the situation. We feel that users are entitled to at least the same level of privacy in OSNs, that they enjoy in real life interactions. Users should be able to trade some information for functionality without that information becoming available beyond the intended scope. For example, a user of a self-help OSN like Patients-Like-Me, who suffers from a given medical condition might not want everyone to know about this, but at the same time the user would like to meet people with the same condition. This is the context of the Kindred

Spirits project, and its aim is to provide users the ability to meet and interact with other (similar) people, while preserving their privacy. This project aims to provide insight into privacy issues and needs faced by users of OSNs and their origins. The insights gained help plot a course for future work. To this end, we look at OSNs as they currently exist, the associated privacy risks, and existing research into solutions. The ultimate goal is to identify open topics in research through reflection on existing proposals.

### *Online Social Networks*

Let the concept begins with the Online Social Networks and why it becoming more popular today. This will help us understand the needs of OSN. Users environments they navigate, and potential threats are discussed in further sections.

### *Definition Of OSNs*

Boyd and Ellison's widely used definition captures the key elements of any OSN: Definitions

1. An OSN is a web-based service that allows individuals to:
  1. Construct a public or semi-public profile within the service,
  2. Articulate a list of other users with whom they share a connection,
  3. View and traverse their list of connections and those made by others within the service.

The list of other users with whom a connection is shared is not limited to connections like friend (Facebook, MySpace) or relative (Genie), but also includes connections like follower (Twitter), professional (Linked In) or subscriber (YouTube).

### *Types of OSNs*

Classification of OSNs based on the openness of the network, we will look at the purpose or functionality that an OSN aims to offer to its user base.

- **Connection OSNs:** : Connection OSNs focus more on the connecting users and by providing a social contact book.
- **Business:** These OSNs aim to provide professionals with useful business contacts,

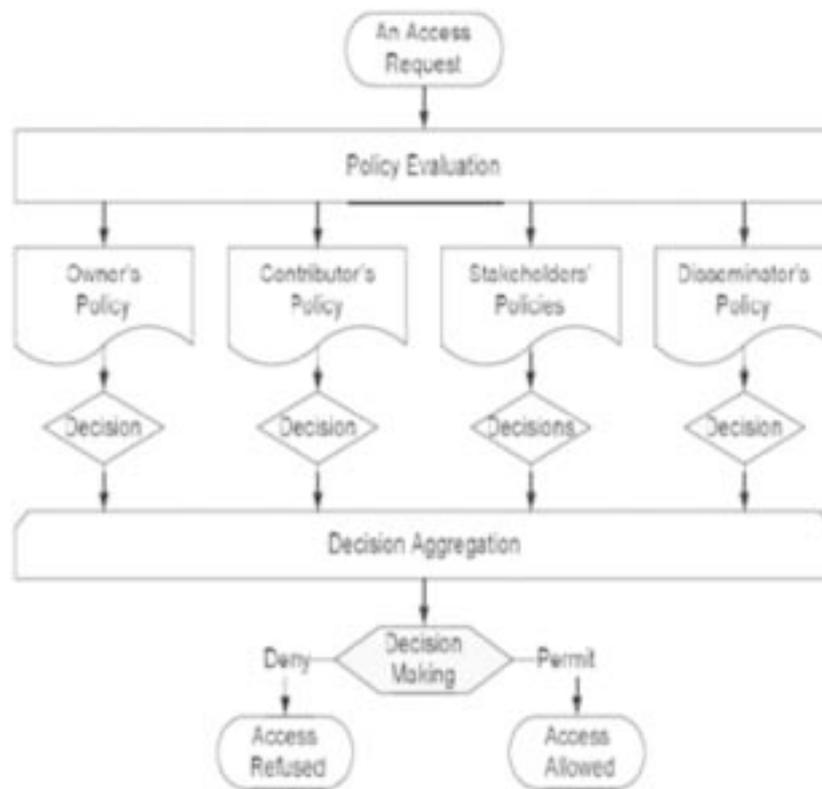
searching for profiles does not always require signing up. Profiles display a users capabilities and work field, this is based on the OSN via messages. This also provide the facility to user to add other user to their network,so that the professional can see whether the user is working or not.

- **Enforcing real-life relationships:** These OSNs are not aimed at finding new friends, but (re)connecting with existing friends or acquaintances that are far.
- **Socializing:** Fitting the more traditional view of social networks. Here users can connect with current friends and find new ones. All types of information found in an OSN are also found in this class; often a lot of this information is public. In order to keep the users this type of OSNs are providing the competitive and social games. Some well known examples of this class are Hypes, Facebook, Orkut and MySpace.
- **Content OSNs:** Content OSNs focus more on the content provided or linked to by users.

- **Content Sharing:** Sharing of user-generated content within a selected group, such as friends or family, or a far wider audience. Content that is shared is usually multimedia. Uploading content most often requires users to sign up and log in; sometimes viewing content also requires logging in, or knowledge of a hard-to-guess obfuscated URL.Examples are Picasa and Photo bucket
- **Content recommendation:** In some cases users do not upload (multimedia) content, but focus more on recommending existing (usually professional) content. Some Book review sites like We Read.com, and URL-tagging communities like Delicious are prime examples where content is discovered and tagged or rated, but not created or uploaded.
- **Entertainment:** These OSNs are tied to a gaming community. Entertainment OSNs might make money by selling games and game add-ons, or through subscriptions. Examples are Xbox.Live and Play fire.

**Table 1: Data Types Typically Found in Different of OSNs**

← OSN types	Data types →	Profiles	Connections	Messages	Multi-media	Tags	Preferences	Groups	Behavioral information	Login credentials
Connection OSNs	Dating	●	●	●	●	-	●	●	●	●
	Business	●	●	●	●	-	●	●	●	●
	Enforcing real-life relationships	●	●	●	●	-	●	●	●	●
	Socializing	●	●	●	●	-	●	●	●	●
Content OSNs	Content sharing	●	●	●	●	●	●	●	●	●
	Content recommendation	●	-	●	●	●	●	●	●	●
	Entertainment	●	●	●	●	●	●	●	●	●
	Advice sharing	●	●	●	●	●	●	●	●	●
	Hobbies	●	●	●	●	●	●	●	●	●
	"News" sharing	●	●	●	●	●	●	●	●	●



**Fig. 1 Multiparty Policy Evaluation**

- **Advice sharing:** place for people to share their experience or expertise in a certain area with others, and advice can be a focus for some OSNs. For example mothers-to-be (Baby Center), medical patients (PatientsLikeMe) or students (Teach Street) can help one another.
- **Hobbies:** Many OSNs focus on audiences that have similar interests and hobbies. This may involve advice sharing elements, but the audience is more homogenous. Examples are Athelings and Care2. "News" sharing. Blog-related OSNs, or ones that focus on world news or gossip. Examples are Buurtlinknl, Twitter, Blogster and GossipReport.com.

### *Multiparty Policy Evaluation*

Two steps are performed to evaluate an access request over MPAC policies.

- The first step checks the access request against the policy specified by each controller and yields a decision for the controller. The accessor element

in a policy decides whether the policy is applicable to a request or not. If the user who sends the request belongs to the user set derived from the accessor of a policy, the policy is applicable and the evaluation process returns a response with the decision (either permit or deny) indicated by the effect element in the policy. Otherwise, the response yields deny decision if the policy is not applicable to the request.

- In the second step, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request. Fig. 1 illustrates the evaluation process of MPAC policies.

Since data controllers may generate different decisions (permit and deny) for an access request, conflicts may occur.

### *A Voting Scheme for Decision Making of Multiparty Control*

Voting scheme to achieve an effective multiparty conflict resolution for OSNs. A notable feature of the

voting mechanism for conflict resolution is that the decision from each controller is able to have an effect on the final decision. Our voting scheme contains two voting mechanisms: decision voting and sensitivity voting. Majority voting is a popular mechanism for decision making, Decision voting.

A decision voting value (DV) derived from the policy evaluation is defined as follows, where Evaluation(p) returns the decision of a policy p:

$$DV = \begin{cases} 0 & \text{if Evaluation(p) deny} \\ 1 & \text{if Evaluation(p) Permit} \end{cases}$$

Assume that all controllers are equally important, an aggregated decision value (DV<sub>ag</sub>) (with a range of 0.00 to 1.00) from multiple controllers including the owner (DV<sub>ow</sub>), the contributor (DV<sub>cb</sub>), and stakeholders (DV<sub>st</sub>) is computed with following equation:

$$DV_{ag} = \left( DV_{ow} + DV_{cb} + \sum_{i \in SS} DV_{st}^i \right) \times \frac{1}{m},$$

where 'SS' is the stakeholder set of the shared data item, and m is the number of controllers of the shared data item.

Sensitivity voting. Each controller assigns an SL to the shared data item to reflect her/his privacy concern. A sensitivity score (Sc) (in the range from 0.00 to 1.00) for the data item can be calculated based on following equation:

$$Sc = \left( SL_{ow} + SL_{cb} + \sum_{i \in SS} SL_{st}^i \right) \times \frac{1}{m}.$$

### Threshold-based Conflict Resolution

A basic idea of our approach for threshold-based conflict resolution is that the Sc can be utilized as a threshold for decision making. Intuitively, if the Sc is higher, the final decision has a high chance to deny access, taking into account the privacy protection of high sensitive data.

Otherwise, the final decision is very likely to allow access, so that the utility of OSN services cannot be affected. The final decision is made automatically by OSN systems with this threshold-based conflict resolution as follows:

$$Decision = \begin{cases} \text{Permit} & \text{if } DV_{ag} > Sc \\ \text{Deny} & \text{if } DV_{ag} \leq Sc. \end{cases}$$

It is worth noticing that our conflict resolution approach has an adaptive feature that reflects the changes of policies and SLs. If any controller changes her/his policy or SL for the shared data item, the DV<sub>ag</sub> and Sc will be recomputed and the final decision may be changed accordingly.

### Strategy-based Conflict Resolution with Privacy Recommendation

In this conflict resolution, the Sc of a data item is considered as a guideline for the owner of shared data item in selecting an appropriate strategy for conflict resolution. We introduce following strategies for the purpose of resolving multiparty privacy conflicts in OSNs:

- **Owner overrides:** The owner's decision has the highest priority. This strategy achieves the owner control mechanism that most OSNs are currently utilizing for data sharing. Based on the weighted decision voting scheme, we set  $\omega_{ow} = 1$ ,  $\omega_{cb} = 0$ , and  $\omega_{st} = 0$ ,<sup>1</sup> and the final decision can be made as follows:

$$Decision = \begin{cases} \text{Permit} & \text{if } DV_{ag} = 1 \\ \text{Deny} & \text{if } DV_{ag} = 0 \end{cases}$$

- **Full consensus permit:** If any controller denies the access, the final decision is deny. This strategy can achieve the naive conflict resolution that we discussed previously. The final decision can be derived as:

$$Decision = \begin{cases} \text{Permit} & \text{if } DV_{ag} = 1 \\ \text{Deny} & \text{otherwise.} \end{cases}$$

- **Majority permit:** This strategy permits (denies, resp.) a request if the number of controllers to permit (deny, resp.) the request is greater than the number of controllers to deny (permit, resp.) the request. The final decision can be made as

$$Decision = \begin{cases} \text{Permit} & \text{if } DV_{ag} \geq 1/2 \\ \text{Deny} & \text{if } DV_{ag} < 1/2. \end{cases}$$

Other majority voting strategies can be easily supported by our voting scheme, such as strong-majority permit (this strategy permits a request if over two-third controllers permit it), super-majority-permit (this strategy permits a request if over three-fourth controllers permit it).

**Logical Definition of Multiple Controllers and Transitive Relationships**

The basic components and relations in our MPAC model can be directly defined with corresponding predicates in ASP. We have defined  $UD_{ct}$  as a set of user-to-data relations with controller type  $ct \in CT$ . Then, the logical definition of multiple controllers is as follows:

The owner of a data item can be represented as:

$$OW(controller, data) \leftarrow UD_{OW}(controller, data) \wedge U(controller) \wedge D(data).$$

The contributor of a data item can be represented as:

$$CB(controller, data) \leftarrow UD_{CB}(controller, data) \wedge U(controller) \wedge D(data).$$

The stakeholder of a data item can be represented as:

$$ST(controller, data) \leftarrow UD_{ST}(controller, data) \wedge U(controller) \wedge D(data).$$

The disseminator of a data item can be represented as:

$$DS(controller, data) \leftarrow UD_{DS}(controller, data) \wedge U(controller) \wedge D(data).$$

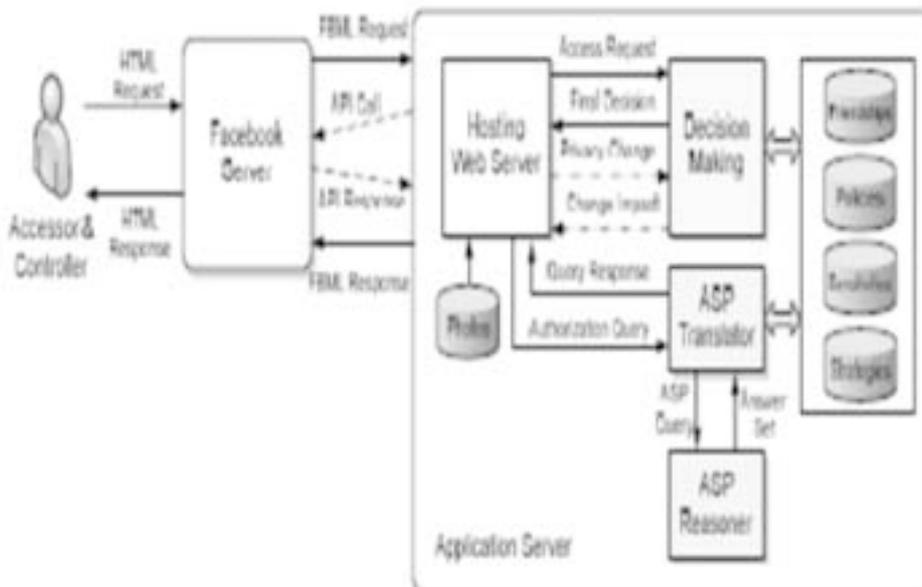
Our MPAC model supports transitive relationships. For example, David is a friend of Alice, and Edward is a friend of David in a social network. Then, we call Edward is a friends of friends of Alice. The friend relation between two users Alice and David is represented in ASP as follows:

$$friendOf(Alice, David).$$

It is known that the transitive closure (e.g., reachability) cannot be expressed in the first order logic [33]; however, it can be easily handled in the stable model semantics. Then, FOF can be represented as a transitive closure of friend relation with ASP as follows:

$$\begin{aligned} friendsOfFriends(U1, U2) &\leftarrow friendOf(U1, U2). \\ friendsOfFriends(U1, U3) &\leftarrow friendsOfFriends(U1, U2), \\ &\quad friendsOfFriends(U2, U3). \end{aligned}$$

Example : (Checking Undersharing). Bob has defined a policy to authorize his friends to see a photo. He wants to check if any friends cannot see this photo in current system. The input query  $\Pi_{query}$  can be specified as follows:

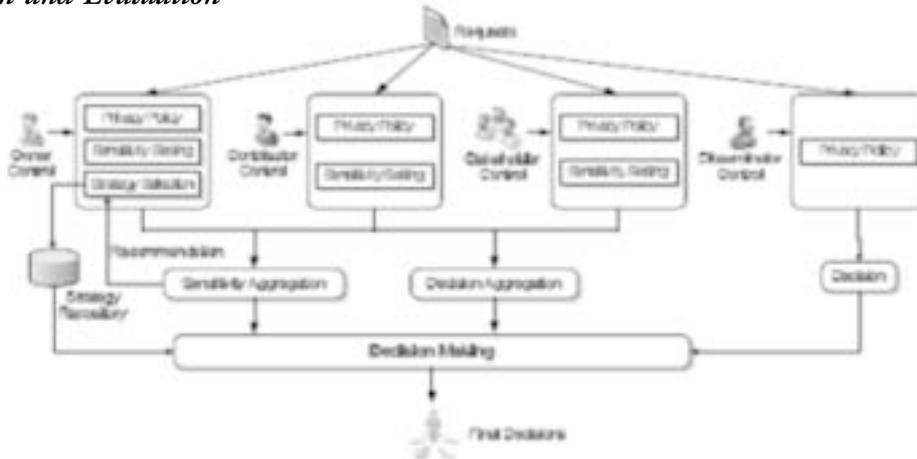


**Fig. 2. Overall Architecture of MController Application**

check:-decision(deny),friendof(bob,x),  
 ow(alice,photoid),user(bob),  
 user(x),photo(photoid).  
 :-notcheck.

If an answer set contains check, this means that there are friends who cannot view the photo. Regarding Bob's authorization requirement, this photo is under shared with his friends.

**Implementation and Evaluation**



**Fig. 3 System Architecture of Decision**

**Making in Mcontroller**

A system architecture of the decision-making module in MController. To evaluate an access request, the policies of each controller of the targeted content are enforced first to generate a decision for the controller. Then, the decisions of all controllers are aggregated to yield a final decision as the response of the request. Multiparty privacy conflicts are resolved based on the configured conflict resolution mechanism when aggregating the decisions of controllers. If the owner of the content chooses automatic conflict resolution, the aggregated sensitivity value is utilized as a threshold for decision making.

Otherwise, multiparty privacy conflicts are resolved by applying the strategy selected by the owner, and the aggregated Sc is considered as a recommendation for strategy selection. Regarding the access requests to disseminated content, the final decision is made by combining the disseminator's decision and original controllers' decision adopting corresponding combination strategy discussed previously.

**System Usability and Performance Evaluation**

*Proposed System*

Our solution is to support the analysis of multiparty access control model and mechanism systems. The use

**Table-2: Usability Study for Facebook and mcontroller privacy Controls**

Metric	Facebook		MController	
	Average	Upper bound on 95% confidence interval	Average	Lower bound on 95% confidence interval
Likability	0.20	0.25	0.83	0.80
Simplicity	0.38	0.44	0.72	0.64
Control	0.20	0.25	0.83	0.80

of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in Online social networks (OSNs), it may reduce the privacy conflicts need to be resolved sophisticatedly.

The following are scenario like content sharing to understand the risks posted by the lack of collaborative control in online social networks (OSNs).

#### *Proposed System Advantages:*

- It checks the access request against the policy specified for every user and yields a decision for the access.
- The use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in online social networks.
- Present any mechanism to enforce privacy concerns over data associated with many users.
- If a user posts a comment in a friend's space, he/she can specify which users can view the comment.

### **Conclusions**

In this paper, in OSNs we have proposed a novel solution for collaborative management of shared data. An MPAC model was formulated, along with a multiparty policy specification scheme and

corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method.

As part we are planning to examine more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs in future work. Also, we would search more criteria to estimate the features of our proposed MPAC model. For example, one of our recent work has evaluated the effectiveness of the MPAC conflict resolution approach based on the tradeoff of privacy risk and sharing loss. In addition, users may be involved in the arrangements of the privacy preferences may become time consuming and tedious tasks and control of a larger number of shared photos. Therefore, we would study inference-based techniques for automatically configure privacy preferences in MPAC. Besides, we plan to thoroughly integrate the notion of trust and reputation into our MPAC model and examine a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in OSNs.

### **References**

1. FacebookDevelopers, <http://developers.facebook.com/>, 2013.
2. FacebookPrivacyPolicy, <http://www.facebook.com/policy.php/>, 2013.
3. FacebookStatistics, <http://www.facebook.com/press/info.php?statistics>, 2013.
4. Google+PrivacyPolicy, <http://http://www.google.com/intl/en+/policy/>, 2013.
5. The Google+ Project, <https://plus.google.com/>, 2013.
6. G. Ahn and H. Hu, "Towards Realizing a Formal RBAC Model in Real Systems," Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 215-224, 2007.
7. G. Ahn, H. Hu, J. Lee, and Y. Meng, "Representing and Reasoning about Web Access Control Policies," Proc. IEEE 34th Ann. Computer Software and Applications Conf. (COMPSAC), pp. 137-146, 2010.
8. A. Besmer and H.R. Lipford, "Moving beyond Untagging: Photo Privacy in a Tagged World," Proc. 28th Int'l Conf. Human Factors in Computing Systems, pp. 1563-1572, 2010.
9. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirida, "All Your Contacts Are Belong to Us: Automated Identity theft Attacks on Social Networks," Proc. 18th Int'l Conf. World Wide Web, pp. 551-560, 2009.
10. B. Carminati and E. Ferrari, "Collaborative Access Control in OnLine Social Networks," Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Worksharing (Collaborate-Com), pp. 231-240, 2011.
11. B. Carminati, E. Ferrari, and A. Perego, "Rule-Based Access Control for Social Networks," Proc. Int'l Conf. On the Move to Meaningful Internet Systems, pp. 1734-1744, 2006.

# Cyber Security in India: Problems and Prospects

Sushma Devi\*

Mohd. Aarif Rather\*\*

---

## Abstract

Cyber security has emerged in the backdrop of information, communication and technological revolution and acts as the corner stone of a connected world. Within the purview of this revolution, the international community across the globe came in confrontation with the new domain of cyber world where opportunities, e.g. communication as well as challenges are becoming paramount. Thus, the world is witnessing different hazards and dangers which have never been experienced in previous periods of history and India is no exception to this. Also, in contemporary times, the current threats faced by the global security environment emerge from the technological progress and were not bound by local origins but extends to include the global networks. Such threats transcend the limits of time and space boundaries and present a continuous and universal challenge. Thus, the inter-state relations drown into securing their economic and security threats without imposing severe restriction on cyber world. In addition, cyber-attacks have the potential to push the states into real acts of aggression and there exists no balance of power in the cyber world. In this context, the paper tries to explore the areas of cyber security out of conventional notions of security and situate India at threshold of analysis with taking different countries responses into consideration. Also, an attempt is made to identify challenges as well as possible diagnosis.

**Keywords:** Cyber security, India, information, technology, threats, global security.

---

## Introduction

The concept of security existed from times immemorial, but has assumed wider dimensions in contemporary times. In common usage, it is connected with a series of different aspects of human existence and with the processes and activities in society and nature. In International relations, the concept came into existence after the end of 2nd World War. But, it was largely assumed to be based on the realistic paradigm i.e., global politics is always a struggle between nations to reach power under a condition of anarchy in which they compete for their respective national interests. Thus, the security was related to the protection of states alone in terms of political stability, territorial integrity and sovereignty. However,

after the end of the cold war, the concept of the security underwent a change from state-centric notion to individual centred. As such, the individuals became the referent objects of security. The nature of threats changed from external aggression to intra-state conflicts[27]. Such threats range from civil wars to environmental degradation, from economic deprivation to human right violation and so on. Apart from these threats, the global politics witnesses the age of information, communication and technology which revolutionised every aspect of human life. It is within the back-drop of this technological revolution that the concept of cyber security came into existence and assumed top priority at global level.

The Network outages, computer viruses, data conceded by hackers and other incidents in one way or the other affect our lives that range from troublesome to life-threatening. The term "Cyber security" refers to securing information technology and focussing on protecting computers, programs, networks and data from unauthorized or unintended access from change or destruction. As most of the government and financial institutions, military groups, corporations, hospitals and other businesses

---

## Sushma Devi\*

Research Scholar,  
Centre for Security Studies, School of International  
Studies, Central University of Gujarat

## Mohd. Aarif Rather\*\*

Research Scholar,  
Centre for Security Studies, School of International  
Studies, Central University of Gujarat

entrepreneurs store and process an abundant deal of confidential information on computers. Such important data is transmitted across networks to other computers. However, with the increasing volume and sophistication of cyber-attacks, the on-going attention is needed to protect personal information and sensitive business as well as to safeguard the national security. On the other hand, Cyber security plays a vital role in the current development of information technology and Internet services [41]. Therefore, it becomes essential for each nation's security and economic well-being to enhance the cyber security and protecting critical information infrastructures. To make the Internet safer has become integral to the development of government policy as well as new services[9].

The concern of cyber security although in the emerging phase has appeared as an important ingredient in the conduct of international relations in contemporary times. It has already started influencing the relations between states. For instance, in recent years, the concern over cyber security has become a contentious issue between U.S - China relations. The U.S has been alleged China of digital espionage against its business and strategic interests as well as targeting proprietary economic data and sensitive national security information. On the other hand, China also claims U.S of being accused of website defacements, network exploitation and service denials attacks. This kind of situation exacerbates mistrust and raises suspicions in both the states regarding the others activities and motives [5].

The cyber-space is evolving as a place where the states are imitating their actions in the real world diplomacy as well as their relations between or among them. It has steadily becoming an arena where states need to protect their territory. Thus, there existed a vital need to apply tools and methods to extract the maximum out of the cyber world in order to serve their national as well as collective interests. Many countries has witnessed several cyber security threats mainly from 2010 onwards and India is no exception to it. For instance, in 2012, some suspected Iranian hackers hacked around 30,000 computers of the Saudi Arabian Oil Company namely "Saudi Aramco" and rendering them useless. The aim of this cyber-attack was to stop the flow of Saudi oil. Similar kind of attack was also

launched against the world's largest liquefied natural gas suppliers "RasGas" a joint-stock company owned by Qatar Petroleum and ExxonMobil which also suffered from the similar damage[7]. In addition, in March 2013, North Korea launched a digital destruction against South Korea by attacking its three TV stations and three banks. Thus, the present decade witnessed numerous cyber security attacks mainly aimed to destruct economic set-up as well as the state's national security.

In the Indian context, the issue of cyber security has received less attention from the policy makers from time to time. The governments have been unable to tackle the growing needs for effective and strong cyber security of India. The reason behind is that India lacks the offensive and defensive cyber security capabilities necessary to tackle the cyber security attacks. Also, India is not boosted with such mechanisms that are vital to confront with sophisticated malware like Stuxnet, Flame, Black shades etc. Thus, the cyber security trends in India seems to be unconvincing at all [19].

### **Historical Background of Cyber Security**

The history of cyber security can be traced back to 1970's when the first computer hackers appeared as they tried to circumvent the system and attempted to make free phone calls. However, it was only after the mid 1980's that the first computer virus called "Brain" was created and as such the Computer Fraud and Abuse Act were established in 1986. Also, in 1990's, several notable threats came into existence affecting the modern information security industry. The Distributed denial of service attacks as well as the bots that made them possible also came into being. Moreover, in early decade of 21st century, this malicious Internet activity assumed the shape of a major criminal enterprise aimed at monetary gain [30]. Such activities entered into mainstream by primarily targeting online banking and then moving onto social networking sites [25]. Now a day, the cyber issues has assumed a much larger dimension and had a greater impact on the national security of states.

With the advent of globalisation process, the world has become more interconnected and the number of Internet hosts and the personal computer industry has

increased. As a result, the large number of people got access to Internet. The everyday life witnessed more people coming online, more things connected to internet, the public sector increasingly leveraging ICTs vis-à-vis the consequences of cyber-attack raised. Under such an open and wide platform, the Internet remained no longer safe [1]. The issues of privacy and security concerns emerged and as such the concept of cyber security came more into picture. Presently, cyber security has become a global concern and includes within its ambit the issues like Cyber warfare, Cyber-crime and Cyber terrorism.

### *Cyber warfare, Cyber terrorism and Cyber-crime*

In contemporary times, computers play an important role in the battlefields in controlling targeting systems, managing logistics as well as in relaying critical intelligence information. Also, at both the strategic as well as tactical levels, the battlefields stand to be fundamentally altered by the information technologies. Therefore, the increasing depth and breadth of this battlefield as well as the improving accuracy and destructiveness of even conventional weaponry have heightened the importance of Control, Command, Communications and Intelligence matters. The dominance in this particular aspect may now yield the advantages of consistent war-winning [2].

### *Cyber warfare*

Cyber warfare is comparatively a new type of weaponry having various effects on the target. It is beyond any limitations of use and can be useful in achieving most of the set goals. The history revealed that military organizations, doctrines and strategies have frequently undergone profound changes due to the technological breakthroughs. Also, the information revolution crosses across borders and thus it generally compels closed systems to open up. This led a direct impact on the future of the military as well as of conflict and warfare more commonly. Thus, cyber warfare revolves around information and communications matters at much deeper levels. The cyber war may be applicable in conventional and non-conventional environments, low as well as high-intensity conflicts and for offensive or defensive purposes. In broader sense, cyber war indicates a transformation in the nature of war [2].

Cyber Warfare has become a more powerful instrument in today's battlefield and had large impact on the development of armies as well as weapon technologies in many countries. In mid-2007, the Israeli cyber warriors hacked the Syrian anti-aircraft installations and reprogrammed their computers. The installation system of Syrian's computers displayed an empty sky. By doing so, the Syrian's allowed Israeli planes to bomb over a suspected nuclear weapons manufacturing industry. The first among known cyber-attacks was launched by the Russia under Deliberate Denial of Service (DDOS) against "Paperless government" of Estonia. After this attack, the DDOS emerged as a common platform of attack for countries like U.S., China, Russia, North Korea, Israel and Pakistan [31]. The analysts around the globe are conscious about the fact that any large-scaled future conflict will comprise cyber warfare as part of a combined arms effort [6].

### *Cybercrime*

Cybercrime refers to any illegal activity by using computers as a primary mode of commission. Cybercriminals use computer technology to access business trade secrets, personal information or using the Internet for malicious or exploitive purposes. The information stolen by the criminal's affects hundreds of millions of people in their day today affairs. It has been estimated that in 2012, 54 million people in Turkey, 40 million in the US, 20 million in Korea, 20 million in China and more than 16 million in Germany have been affected by the cybercrimes. The growth is still alarming and is expected to be more than 800 million in 2013 at global level. The cybercrime is thus a biggest problem affecting both the developed as well as developing world. The consequences of cybercrime had bad implications on the trade, innovation, competitiveness and global economic growth [16]. However, the problem associated with the Cybercrime is that the perpetrators no longer require complex techniques or skills.

On the other hand, the intensity and perceptions of relative risk and threat largely vary between Governments and private sector enterprises. From the perspectives of national security, almost two-thirds of countries view their systems of police statistics insufficient for recording cybercrime. According to the

Police-recorded cybercrime rates, the number of crimes is associated with levels of country's development vis-a-vis specialized police capacity rather than underlying crime rates [36].

In 2000, the first major instance of cybercrime took place when a mass-mailed computer virus affected around 45 million computer users worldwide. However, the cybercrime landscape changed dramatically and began to attain the politically motivated objectives. In the last decade, cyber-attacks have been evolved in utilizing the online weapons affecting several government entities. The cyber experts are of the view that the world has witnessed glimpses of cyber war with unethical cyber hackers stealing important state information. Quoting US Defense Secretary Robert Gates, "cyberspace is the new domain in which war will be fought after land, sea, air and space" [20].

The present age i.e., digital age has witnessed a norm of online communication in which the internet users as well as governments confront with becoming the targets of cyber-attack. With the advancement in the techniques of cyber criminals, their focus shifted from financial information to business espionage as well as accessing government information. To fight fast-spreading cybercrime, governments must collaborate globally to develop an effective model that will control the threat internet-based networking, cybercrime and digital attack incidents have increased around the world [20].

### *Cyber terrorism*

Cyber terrorism is any deliberate attack against information of computer systems, programs and data resulting in violence against non-combatant targets by secret agents or sub-national groups. The attacks are generally politically motivated. The cyber-attacks are designed to cause extreme financial harm or physical violence. The thrust areas of cyber terrorist targets include military installations, banking industry, air traffic control centres, power plants and water systems etc. The term 'Cyber terrorism' is sometimes referred to as information war or electronic terrorism [28].

The present global era has witnessed more than one billion online users and 233 countries connected to

the Internet. In such an inter-connected world, terrorism is flourishing through terrorist's use of information and communication technologies (ICTs). Today, nearly all the terrorist organizations either small or large have their own Web sites. The recent example of terrorist attacks includes Osama Bin Laden, attack on America's army deployment system during Iraq war and the LTTE. The terrorist organisations cooperate with organized crime vis-a-vis use technology to spread propaganda, recruit and train members, raise funds, communicate and launch attacks. The reason in making the internet as an attractive medium is the technological difficulty in dealing with cyber communications. Also, the governments face several difficulties in combating with terrorist's use of ICTs which include the lack of coordinated procedures and laws in investigating cybercrimes, ineffective or inadequate information sharing and complications in tracing and tracking cyber communications [41]. Therefore, a global attention is needed to address these areas of cyber security in order to win the battle against terror.

### **Cyber Security and International Community**

In recent decades, cyber security has emerged as a global phenomenon and the most critical concerns of the IT age. It acts as the corner stone of a connected world. To address this issue, a truly global approach is needed. Because of its universal networks, cyber terrorists and criminals do not need their presence anywhere near the scene of the crime [1]. Therefore, international response and cooperation is needed to address the notion of cyber security properly.

### *Cyber Security under United Nations*

United Nations since its inception has taken the responsibility of maintaining peace, security and cooperation among the member-states. So far as the issue of cyber security is concerned, it had established Information Telecommunication Union (ITU) in 1965 to ensure the safety of all those who venture online. ITU is the leading agency of United Nations for information and communication technologies and a global focal point for the private sectors as well as governments. The purpose of ITU is to focus on the growth and development of information and telecommunication networks as well as to enable global

access to all the people so that they may easily participate and avail the benefits from the global economy and emerging information society [17].

Apart from ITU, the United Nations has expressed itself on cyber security matters and passed five major Resolutions in this regard. The first resolution under A/RES/55/63 was issued on December, 4th 2000 dealing with the criminal misuse of ICT's. It identifies that the unrestricted flow of information can promote social and economic development as well as can be useful in sustaining democratic governance. Another resolution issued on 19th Dec, 2001 by the UN under A/RES/56/121 requested the states to cooperate and coordinate against misuse of ICTs. Basically, the primary purpose of the resolution was to set the national laws and policies to address the crimes related to computer.

On 20th Dec, 2002, the UN passed a resolution under A/RES/57/239 emphasising on the establishment of global culture of cyber security. It urged the need that the law enforcement as well as separate governments cannot address cyber security alone but demands global attention and cooperation. The UN's fourth resolution (A/RES/58/199) issued on 23rd December 2003 also deals on the global culture of cyber security but at the same time focused on the protection of critical information infrastructures like maritime and air transport, financial and banking services, food distribution, water supply and public health [40].

In 2010, the UN appointed three Groups of Governmental Experts (GGE) to examine the prevailing and potential threats from the cyber-sphere as well as to find measures so as to combat them. Also, in 2011, a resolution under A/RES/66/24 was passed by the General Assembly emphasising the need of addressing the assessments and recommendations as contained in the Report of 2010 [35]. In addition, the UN Secretary-General Ban Ki-moon appointed the group of 15 experts on 9th August 2012 to draft a report on the Developments in the Field of Information and Telecommunications from the perspective of International Security. The experts include the five permanent members of the UN Security Council as well as India, Japan, Canada, Belarus, Australia, Egypt, Germany, Argentina, Estonia

and Indonesia. The experts emphasise that there is a need to elaborate confidence-building measures and to set several rules and principles of responsible behaviour of States with respect to cyber security [42].

Again in 2013, the UN General Assembly adopted a resolution under 68/243 in which special attention was to be laid on the outcome of the 2012/2013 GGE. Also, the Secretary-General of UN was requested to establish a new GGE that would report to the General Assembly in 2015 [35]. To sum up, it may be assessed that the issues of cyber security are quickly making its way into the agenda of global public policy issues and thereby demanding proper attention [23].

### *Canada's Cyber Security policy*

The cyber security strategy was issued by the government of Canada in October 2010. The basic purpose of the strategy was to secure the government systems, to protect vital cyber systems outside the federal government so as to strengthen resiliency and facilitating Canadians to be secure online [37]. The Security Intelligence Service of Canada considers the cyber threat as one of its five priority areas including security screening, proliferation of weapons of mass destruction, terrorism and finally espionage and foreign interference [37]. The strategy also focused on the need to have an international engagement between the allied militaries and Department of National Defence on cyber defence for an effective implementation of such practices [12]. The responsibility of handling the computer and communications networks of the armed forces have been entrusted with the Canadian Armed Forces Information Management Group. In addition, the government of Canada established the Directorate of Cybernetics in June 2011 to enhance the cyber warfare capabilities for the armed forces [37]. Thus, the Canada has taken some positive steps in the direction of improving the cyber security dimensions.

### *China's Cyber Security policy*

In early 2011, the government of China's Information Office issued a white paper on national defence by which it directed the military to maintain its security interests in cyber and electromagnetic space. It focuses that the fighting capabilities of the armed forces in circumstances of informationization have been

considerably raised. As such, there is a need to raise a new type of combatting capability so as to win local wars in conditions of informationization [15]. In the same year in May 2011, the Chinese Ministry of National Defence declared that the army had set up an "Online Blue Army" in order to improve the cyber security of the military forces [43].

In 2012, the Republic of China issued a set of new policy guidelines for cyber security. It urged the need for bringing the efforts to better handle and detect information emergencies, protect personal information and to reduce internet crime [44]. The Ministry of Public Security and the Ministry of Industry and Information Technology in China have taken the responsibility for securing the cyber security sector. Apart from the improvements made by china in the sector of cyber security, the country had witnessed several emerging threats in this particular sector. But at the same time, it has evolved as one of the major cyber security nations in the world.

#### *United States (US) Cyber Security policy*

In 2009, the United States formulated a Cyberspace Policy Review and also appointed a mid-level Cyber security Coordinator to the members of the National Security Council [37]. In 2010, it retained some of the provisions of Cyberspace Policy Review in its National Security Strategy [38]. The responsibility of dealing with the cyber security issues is entrusted with the Department of Homeland Security, the Department of Defence and the Bureau of Investigation. However, the major step taken by US in the direction of cyber security was initiated in 2012 under an extensive cyber security programme in the realm of both civilian as well as military aspects. In the same year, in October, President Obama signed a Presidential Decision Directive regarding the activities in cyberspace. The directive makes it clear that the military will have a greater role to play in defending against cyber-attack from foreign invasions[23]. Also, in November, the Defense Advanced Research Projects Agency of UN released a document called Foundational Cyber warfare asking for research into the conduct of cyber war. The document stated that there is a need to investigate into the nature of cyber warfare and to find out the strategies needed to

dominate the cyber battle space [37]. Thus, the US has taken some vital steps towards strengthening its cyber security agenda. The progress made by the US in the cyber security sector becomes clear by the cyber-attack "Stuxnet" against an Iranian nuclear facility in 2010 [29].

#### *United Kingdom's (UK) Cyber Security policy*

In contemporary times, the UK has one of the most advanced national cyber security approaches. In the year 2011, the UK restructured its Cyber Security Strategy in which cyber- attack was considered as a national security threat. The basic objectives of the strategy include addressing cybercrime, enhancing information infrastructure resiliency, ensuring a safe cyberspace for the public and evolving an adequate cyber security workforce. Apart from this, the strategy makes it clear that the UK will work bilaterally as well as through international forums to establish international norms in the realm of cyber security and will also work to develop confidence-building measures in this sector [34]. The UK government has allocated £650 million through 2015 for implementing the National Cyber Security Programme [12].

In 2012, the UK announced the establishment of an academic institute for the purpose of researching cyber security. The objective behind was to increase resiliency against the cyber- attack as well as to better equip the government to defend the country's national interests in cyberspace [21]. Also, the UK government intends to establish a National Crime Agency to investigate and respond to serious national-level cybercrime as well as provide training and support to local police forces to deal with such crimes [34]. In addition, the Defence Cyber Operations Group will be created which would be operational by March 2015. The Group would consist a federation of cyber units across defence to safeguard the comprehensible integration of cyber activities across the spectrum of defence operations [33].

#### *Russian Federation's Cyber Security policy*

The national policy for fighting cybercrime and the establishment of a national system to prevent and detect cyber-attack was released by the Russian Federation's Security Council in July 2012. The

Responsibility for implementing the policy was given to the Federal Security Service. The aim of the policy is to secure the country's networks from foreign sources [4]. Also, the government has drafted a bill to make an advanced military research agency for dealing with cyber security. The bill discusses the principles of information security and different measures to control for interference in information systems. Thus, the Russian federation seems to be determinant to protect national interest's vis-à-vis recognising the greater role of information warfare [37].

To sum up, it may be assumed that various nations particularly the developed ones have taken some serious steps in combatting with the cyber security issues. At the same time, they have initiated various policies and programme to enhance and strengthen their cyber security sectors.

### *Indian perspectives of cyber security*

The IT sector in India has emerged as one of the most significant growth catalysts for its economy. Also, this sector is positively influencing the lives of its people either through direct or indirect contribution to several socio-economic parameters like standard of living, employment, diversity among others etc. In addition, it has played a vital role in transforming India as a global player. Further, the Government sector has facilitated increased adoption of IT sectors in the country that encourage IT acceptance and National programmes like Unique Identification Development Authority of India (UIDAI) and National e-governance Programmes (NeGP). The adoption of such programmes has created large scale IT infrastructure and promoted corporate participation. However, despite the growth in IT sectors of India, there has been a tremendous need to secure computing environment as well as build adequate confidence & trust in this sector. The presence of such environment enables a need for the creation of suitable cyber security eco system in the country [13].

The last couple of decades witnessed India in the niche of IT. Almost, all the financial institutions as well as Indian banking industry have incorporated IT to its full optimization. At the same time, these economic and financial institutions are confronted with cyber-attacks in their daily activities. However, the increasing

dependency of these Indian institutions on IT under cyber threats might lead them to an irreparable collapse of economic structures. Although, the worrying part is that there is absence of alternatives to tackle with these kinds of threats [26].

In India, several organisations within the ambit of Ministry of Defence have taken the responsibility of dealing with the concept of cyber security. In the year 2005, the Indian Army formed the Cyber Security Establishment in order to protect the networks at the division level as well as to conduct safe cyber security audits [24]. Also, in the year 2010, the army established the Cyber Security Laboratory at the Military College of Telecommunications Engineering in Madhya Pradesh with a view to provide specialized training to its officers in security protocols for its signal as well as data transmission networks [10].

In March 2011, the Indian Ministry of Communications and Information Technology released a draft on National Cyber Security Policy. The policy mainly focused on the security and protection of critical infrastructure, development efforts as well as public-private partnerships [13]. In June 2012, a proposal in line with the draft policy under National Security Council intends to create the National Critical Information Infrastructure Protection Centre (under the National Technical Research Organisation). The objective behind this was to ensure the security of the state's critical infrastructure along with national and sector-specific Computer Emergency Response Teams (CERTs) [18]. In the same year in May, the Indian Ministry of Defence Research and Development Organization have established an indigenous system of cyber defence to ensure that network sectors are safe and secure. The project was reportedly about 50 percent to be complete as of May 2012 [45]. In the context of cyber security, the Technical Intelligence Communication Centre and the National Defence Intelligence Agency are creating a joint team to aware the government about potential cyber vulnerabilities [32].

Apart from taking several positive steps, the cyber security projects and initiatives in India are still very less in numbers as compared to other developed nations. Some of the projects proposed by the Indian

government have even remained on papers only. In addition, the Projects like National Critical Information Infrastructure Protection Centre (NCIPC) and National Cyber Coordination Centre (NCCC) of India has eventually failed to materialise so far. Also, the National Cyber Security Policy of India framed in 2013 failed to show fruitful results and even its implementations seems to be weak on numerous aspects. On the other hand, there is a vital need to protect the critical infrastructures such as banks, satellites, automated power grids, thermal power plants etc from the cyber-attacks in India [32]. The Indian government claimed that there has been a huge rise in cyber-attacks against the establishments like the banking and financial services sector. In the year

2013, there was a 136% increase in cyber-threats and attacks against government organizations as well as 126% against financial services organizations in India [3]. Also, the country ranks 7th in the cyber-attacks and 85th in the net connectivity [8]. In addition, the India continues to be an attractive target in recent times for cyber criminals with around 69 percent targeted attacks being focussed on large enterprises. According to the report by security software maker 'Symantec' India nearly witnesses four out of ten attacks which are carried on non-traditional service industries like business, hospitality and personal services [14]. Thus, there exists a vital need for India to frame a cyber-crisis management plan in order to combat with the cyber threats effectively.

## References

1. Andreasson, K., *Cyber Security: Public Sector Threats and Responses*, New York: Auerbach Publications, 2012.
2. Arquilla, J. and Ronfeldt, D., "Cyberwar is coming," *Comparative Strategy*, vol. 12, no. 2, pp. 141-165, 1993.
3. Athavale, D., "Cyberattacks on the rise in India," *The Times of India*, 10 March, 2014.
4. C.news., "Russia rolls out state cyber security policy," *Russia*, 12 July, 2012.
5. IGCC Report, "China and Cybersecurity: China and Cybersecurity: Political, Economic, and Strategic Dimensions," Report from Workshops held at the University of California, San Diego, April 2012, pp. 1-34.
6. Clarke, R. A., and Knake, R., *Cyber War: The Next Threat to National Security and What to Do About It*, USA: Ecco Publications, 2012.
7. Kyrou, D.K., "Critical Energy Infrastructure: Operators, NATO, and Facing Future Challenges," *Connections*, vol. XII, no. 3, pp. 109-117, 2013.
8. Express News Service, "India 7th in Cyber Attacks, 85th in Net Connectivity," *The new Indian express*, 01 July, 2014.
9. Gercke., *Understanding Cybercrime: a Guide for Developing Countries*, Geneva: ITU publication, 2009.
10. Governance Now, "Army sets up cybersecurity lab", 2010, Available: <http://www.governancenow.com/news/regularstory/army-sets-cyber-security-lab>.
11. Government of Canada, "Canada's Cyber Security Strategy", 2010, Available: <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cbr-scrt-strtgty/cbr-scrt-strtgtyeng.pdf>.
12. House of Commons Defence Committee, "Defence and Cyber-Security", London: The Stationery Office Limited, 2013.
13. Indian Ministry of Communications and Information Technology, "National Cyber security Policy", draft v1.0, 26 Mar, 2011.
14. Indo-Asian News Service, "Large firms hit by 69 percent of targeted cyber-attacks in India: Symantec", 26, April, 2014.

15. Information Office of the State Council of the People's Republic of China, "China's National Defense in 2010", Information Office of the State Council, The People's Republic of China, March 2011.
16. Intel Security (2014), Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Center for Strategic and International Studies, USA.
17. International Telecommunication Union, "Agencies of the UN: ITU," 2014, Available: <http://www.un.org/agency-itu.php>.
18. Joseph, J., "India to add muscle to its cyber arsenal," TheTimes of India, 11 June, 2012.
19. Kaushik, R.K., "Cyber Security Needs Urgent Attention of Indian Government,"2014, Available:<http://cybersecurityforindia.blogspot.in/2014/09/cyber-security-needs-urgent-attention.html>.
20. KPMG International,Cybercrime – a growing challenge for governments, Issues Monitor,vol. 8, no. 3, pp. 1-21,2011.
21. Meyer, D., "Spies and professors band together for UK cyber security research institute," ZD Net, 13 September, 2012.
22. Meyer, P,"Cyber Security Takes the Floor at the UN", Canadian International Council," 12 November 2013.
23. Nakashima, E., "Obama signs secret directive to help thwart cyber-attacks", Washington Post, 14 November, 2012.
24. Pandit, R., "Army gearing up for cyber warfare," Times of India, 7 July, 2005.
25. Pillai, P., "History of Internet Security," 2012,Available URL: <http://www.buzzle.com/articles/history-of-internet-security.html>.
26. Raghav, S.S., "Cyber Security in India's Counter Terrorism Strategy", 2009, Available: [http://ids.nic.in/art\\_by\\_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf](http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf).
27. Rather, M.A. and Jose, K., "Human Security: Evolution and Conceptualization,"European Academic Research, vol. II, no. 5,pp. 6766-6797, 2014.
28. Rouse, M., "Cyber terrorism", [Online: web] Accessed on 16 August, 2014, Available: <http://searchsecurity.techtarget.com/definition/cyberterrorism>.
29. Sanger, D.E., "Obama order sped up wave of cyberattacks against Iran," New York Times, 1 June, 2012.
30. SC Magazine, "A brief history of internet security," 2009, Available: <http://www.scmagazine.com/a-brief-history-of-internet-security/article/149611/>.
31. Singh, C.M.,Cyber War and Terrorism, Delhi: Prashant Publishing House, 2009.
32. Singh, H. and Philip J.T., "Spy game: India readies cyber army to hack into hostile nations' computer systems," Economic Times, 6 August, 2010.
33. United Kingdom,"Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review", London: The Stationery Office Limited. (2010),
34. United Kingdom, "The UK Cyber security Strategy: Protecting and Promoting the UK in a Digital World," Cabinet Office 22, Whitehall London, pp. 1-43, 2011.
35. United Nations, "Developments in the field of information and telecommunications in the context of international security,"United Nations Publication: New York, pp. 1-56, 2011.

36. United Nations, "Comprehensive Study on Cybercrime," United Nations Publication: New York, pp. 1-287, 2013.
37. United Nations Institute for Disarmament Research, "The Cyber Index: International Security Trends and Realities," United Nations Publication: New York and Geneva, pp. 1-140, 2013.
38. United States, "National Security Strategy," 2010, Available: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf).
39. UNODA, "Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations, New York, 2011.
40. Wamala, F., "The ITU National Cyber security Strategy Guide," Telecommunication Standardization Sector of ITU (ITU-T), Geneva, Switzerland, 2011.
41. Westby, J.R., "Countering Terrorism with Cyber Security," *Jurimetrics*, vol. 47, no. 3, pp. 297-313, 2007.
42. Wolter, D., "The UN Takes a Big Step Forward on Cyber security," Arms Control Association, 13 September, 2013.
43. Xin, Y, "PLA establishes 'Online Blue Army' to protect network security," People's Daily Online, 26 May, 2011.
44. Xinhua, "China calls for tightened information security measures," China Daily, 18 July, 2012.
45. Xinhua, "India developing cyber defense program," 2012, Available: <http://english.cri.cn/6966/2012/05/04/2941s697329.htm>.

# An Analysis on Improvement of Website Ranking Using Joomla

Kirti Nigam\*

Satyam Saxena\*\*

Nargish Gupta\*\*\*

---

## Abstract

Search engine optimization is a strategically technique to take a web document in top search results of a search engine and is often about making small modifications to parts of your website. When viewed individually, these changes might seem like incremental improvements, but when combined with other optimizations, there could be a noticeable impact on final site's user experience and performance in organic search results. Search engine optimization is about putting your site's best foot forward when it comes to visibility in search engines, but developer ultimate goal is consumers of website are their users (End user uses particular website), and this will not depend on search engines. This present study focuses on impact of a high search engine ranking on the amount of visitors from the search engine and what value comes with their views of the visitors on the various SEO techniques that can be used by webmasters to improve website's visibility in search results and improve traffic to the website.

**Keywords:** Search Engine Optimization, Website SEO(Search Engine Optimization), On Page Optimization, Off Page Optimization, Website Visibility.

---

## Introduction

Now day's web in market website ranking plays an important role. When an user put a query in search bar of search engine then user wish to find his desire output in first three or four results maximum he/ she tries for two or three pages. This psychology of user indicate that particular developer website must come under top 30 results otherwise there is no worthwhile of development. Another issue arises that different user uses different search engine so developer cannot develop a website or application by considering one or two search engine. In other words website and web application must be independent with search engine working [1].

Search engine optimization (SEO) is the practice of altering a website to improve the rankings of

that website, among popular search engines such as Google, Bing, and Yahoo. Many visitors discover new websites and brands on these popular search engines, placement in the search results for common searches has become a critical method of advertising for many businesses.

SEO is a scientific development concept and methodology, which develops along with the development of search engine, and promotes the development of search engines at the same time. SEO is not a suddenly appeared technology, but it synchronously developed with search engines. From the appearance of yahoo, Google and other search engine that become cause of emergence of new SEO theory for search innovations [2]. Search engine technology is in the development and perfection. The excellent search engine should have four characteristics: rapid, accurate, easy to use and storage.

## Seo Using Joomla

Web crawling produces order of the search result. Engines performed and as a means to search the data in search engine result page (SERP), the current

---

**Kirti Nigam\***

SRITS Datia, M.P.

**Satyam Saxena\*\***

Assistant Professor, SRITS Datia, M.P.

**Nargish Gupta\*\*\***

Assistant Professor, IITM, New Delhi

minutes using the search web search engine results web page.

### **Browser Page Title**

Each title in Joomla site is named same as the title user have given to each Menu Item that developer create. User also has ability to create title tag different than the Menu item. These titles are store in the server.

When a query is generated then search engine first search the particular title in server. For example if user pass any query in between inverted comma (“”) then google search engine provide only those link where particular phrase or query is present. Appropriate title for a webpage and application is helpful for improving website ranking on server.

### **Viewing Page Source**

Every page and web application is always store in any server. Search engine fetch the link of particular document and provide it to user. User can view the information of page source if you see how your browser will show the title of the page. This can be done by right-clicking your mouse on the web page and selecting the option of View page source.

### **Meta Descriptions**

In Joomla, for improving your SEO, there is a great strategy of utilizing the Meta keywords and its Description option. Your choices in favor of description used globally Yahoo and Google improve your SEO details. However, it will take sometimes for Joomla site and individually or developer can search for free keywords, articles or menu items and begin work with his own characterized metadata, generally developers use google based application which provide what user interest (regarding with word) for particular issue.

### **Global Metadata Options**

On World Wide Web different geographical user search other words for same query. For developing metadata for your entire site, log into the Administration area (the back end) of your site, and go to the Global Configuration area. Under the Site tab, locate Metadata Settings.

### **Site Meta Description**

These are the key entry site below will be in the Meta”description”text omitted from the past 20 often

connected individuals, around the word show Metadata Meta web entry. A recommended description is of around 20 words. If the metadata entry is blank, then this entry is omitted from web pages. Meta descriptions the SERP page more cuples looking headers, metadata describing the insertion of keywords to describe the page and application on web. Meta descriptions tend to be more important than the keywords.

### **Site Meta Keywords**

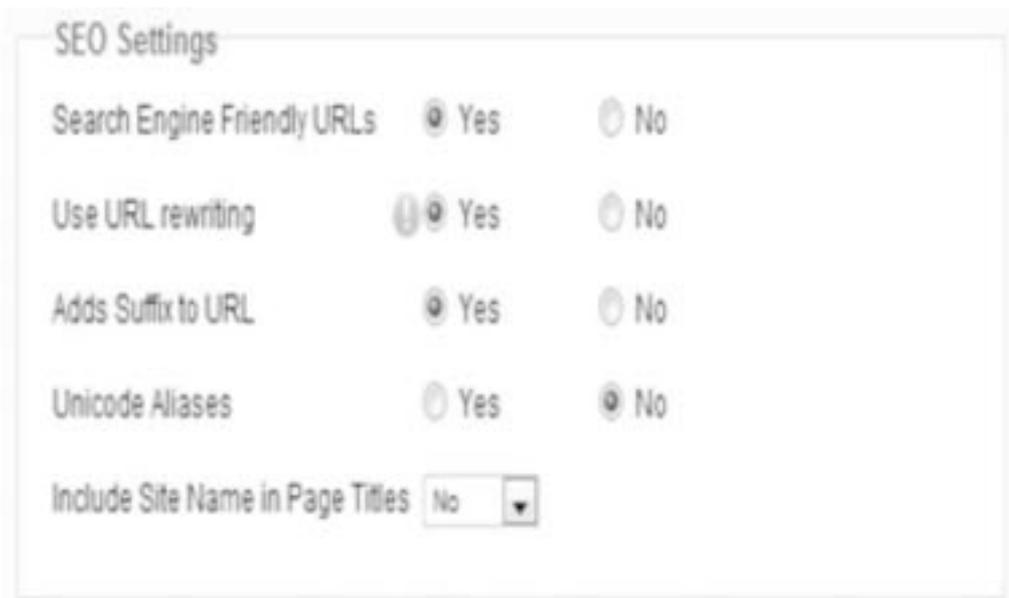
The keywords reflect the content of the web page to move up the search engine rankings. As Search engines may use these words to refine their indexing of the site s web pages. The “keywords” metadata entry are words and phrases (separated by commas) added here appear in web page headers. This metadata entry is omitted from web pages if the metadata entry is blank then this entry is omitted from web pages.

### **Global Seo Settings**

Search URL for the website, configuration easier for the region’s ranking changes. The use and management of the SEO person can format setting pages have a URL settings. The developer offered with significant impact of options within a few pages to global. Once a website is established you do not recommended to alter the SEO Settings [3]. Nearly all of a site s URLs will also change if you changing any of the first three items in this area and result in broken links from other sites and perhaps a temporary drop in search engine rankings.

### **Google Analytics**

In some circumstances developer find that the end user would want more control over the”Google Analytics” code and would prefer to switch it on and off or insert new tracking code at their own will. Id parameter that the engine website plug Google Analytics asynchronously so that sites that we supply or we end analytics tracking the general rankings since loading allow the user to their simple Google search for the term you plug compiled increasing in the new code allow us to build in this code loading performance .Forsite analytic template allow embed prefer to buy enough for a little tracking for Google to accelerate the load is added to that of the analytical



**Fig. 1: Global SEO Settings**

to add some code to plugin. It is well in control of your well circumstances switch itself. Every Google search requires little line code for loading page. Since “Google Now” actively looks at your websites loading performance to calculate its search engine rankings, plug-in play an important role for this, these plugin allows developer to add some enhanced web property. On the other hand these plugins help to create a link between two or more sites, so that if original site is calls in a query then other site which contains the plugins also reflect their links on search results [4].

### **New Advanced Features**

#### *Subdomain and Multiple Top Level Domains*

There is little new support that has been added to the plugin. It now supports multiple sub domains and multiple top level domains,

For example: example.com.au, example.com.

#### *Sample Rate Specifications*

A session timeout is used for computation of visiting users. For the particular needs, if anyone want to change the definition of a ‘session’, then developer can pass new number of milliseconds to define a new value of session. This will impact on visiting reports of every section, where the number of visits are

calculated, these visits are used in computing other values. For example, if you shorten the session timeout, the number of visits will increase and it will decrease when developer increase the session timeout [5].

#### *Site speed sample rate specification*

An analysis shows a fix in value of 1% sampling of site, visitors make up the data pool from which the site speed metrics are derived by default code present on search engine, developer want to adjust the sampling to a larger rate. If a website have relatively small number of daily visitors, such as 100,000 or fewer. It will provide increased granularity for page load time and other Site Speed.

#### *Visitor cookie timeout*

The timeout sets the Google Analytics visitor cookie expire in milliseconds. Using this method, developer prefer to change the expiration date of the visitor cookie. Visitors use cookies for maintain session when user delete the cookie then time out time will change the “expiration time” to 0. If user set browser timeout time then it will increase or decrease expiration time.

#### *Social Media Tracking*

If website contains Facebook and other templates integrated in it. For example functions such as

tracking of Facebook 'like' and 'unlike' as well and follows the site on Twitter. Tracking differentiate between "Frontend" Log-in User and Visitor. Extra code is required to track website member actions compared to website visitors. Google Webmaster tools used for domain verification of websites to distinguish among various geographical servers and their data.

### ***On-page Optimization Tool***

The exact link to our site's key insight glimpse stop the use of the information in this modest site of useful your connection to the meta effect Internet access to view most of the site and equipment to make adjustments in how these elements you can structure your site to reach its maximum potential. Use this tool to evaluate your internal links, Meta information and page content.

### **References**

1. *ComScore Releases June 2012 U.S. Search Engine Rankings*. Retrieved 08 27, 2012, from Comscore:[http://www.comscore.com/Pres\\_Events/Press\\_Releases/2012/6/com](http://www.comscore.com/Pres_Events/Press_Releases/2012/6/com)
2. Ferdig R., & Trammell K., Content Delivery in the "Blogsphere". *The Journal Online - Technological Horizons in Education*. Google *Internet Users*. Retrieved June 14, 2012, from Google Public
3. Jennifer Grappone, Gradiva Couzin, "Search Engine Optimization" Beijing: Tsinghua University Press, pp.100147, July 2007.
4. *Score Releases June 2012 U.S. Search Engine Rankings* Downes, S. (2004). Educational blogging. *Educause*, 39 (5), 14-26. Facebook. (2012, 07 27). *Facebook Key Facts*. Retrieved 08 27, 2012,
5. <http://pbwebdev.com/blog/asynchronous-google-analytics-plugin-for-joomla>

### **Conclusion**

Despite various search engine optimization techniques, the most effective solution to a highly visible website still relies on having good contents. Once a website is submitted to search engine listing, the search engine crawler will categorize and index the website based on keywords in the contents. Therefore, website designers must be smart about choosing the right keywords for website content. There are many useful search engine optimization tools available today. But the challenge lies in knowing which tool to use and how to interpret the data gathered by the tool. SEO can promote web site's ranking in the search engine, also will get more and more attention. Moreover from the perspective of the development of SEO, though there are SEO cheating, but the initiative of industry words basically master in the hands of SEO who uses widely recognizes optimization technique.

# Network Security - Authentication Methods and Firewall

Minal Dhankar\*

---

## Abstract

Nowadays computer security is becoming a major issue because we are moving to a digital world. The security of data is extremely important in ensuring safe transmission of information over the Internet. Authentication and firewalls are one of the most basic and commonly used techniques to ensure security in the network. A firewall is a device that prevents unauthorized access to a network and can be implemented in hardware or software or a combination of both. This paper presents various authentication techniques like Knowledge based, Token based, Biometric based and an analysis of Firewall Technology.

**Keywords:** Firewall Testing, Firewall Technology, Authentication, Biometric, Password, Security Tokens

---

## Introduction

As the world is digitizing people are becoming more active on the Internet, but along with this awareness several security threats like viruses, Denial of service etc. have also increased tremendously. So, the most important issue in today's world is to secure the network. Security network is important because we do not want any sensitive or confidential information to go outside the network. These threats can create serious damage to an individual's personal information and to the resources of a company or an organization. These threats are present mainly due to the ignorance of the user and poor technology and design of the network. These threats are also a result of the network services which are enabled by default into a computer and are used by the hackers for information gathering. The firewalls installed before are not suitable for the present computer threats and cannot prevent data against these threats. A firewall is a hardware or software system that prevents unauthorized access to or from a network and can be implemented in hardware and software or both. Firewall filters incoming and outgoing data packets as they come in and go outside of the network. The following are basic features of a secure network-

- 1) *Access:* Only authorized users are used to communicate to and from a particular network..
- 2) *Authentication:* This ensures that users in the network are who they say they are. Actual flow of information can start only after the user has been authenticated and allowed to communicate to other systems in the network.
- 3) *Confidentiality:* Data in the network remains private. This is done to ensure that the information can be viewed only by authenticated systems and it can be achieved using various encryption techniques.
- 4) *Integrity:* This ensures that the message has not been changed during transmission.

## Data Security And Authentication

During the process of data communication there is always a threat of stealing of data by the hackers. So, to secure sensitive information, authentication is the key in network security. Authentication is the technique of ensuring the identity of user or any other entity involved in the network. Password is the most commonly used scheme for verifying the identity of a person. Attacks which can occur during authentication are given in Table I.

## Authentication Methods

Following are the primary authentication techniques used in the public network these days:

---

**Minal Dhankar\***

Asst. Prof., Maharaja Surajmal Institute  
(Affiliated to GGSIP University)  
New Delhi, India

**Table I: Attacks on Network Data**

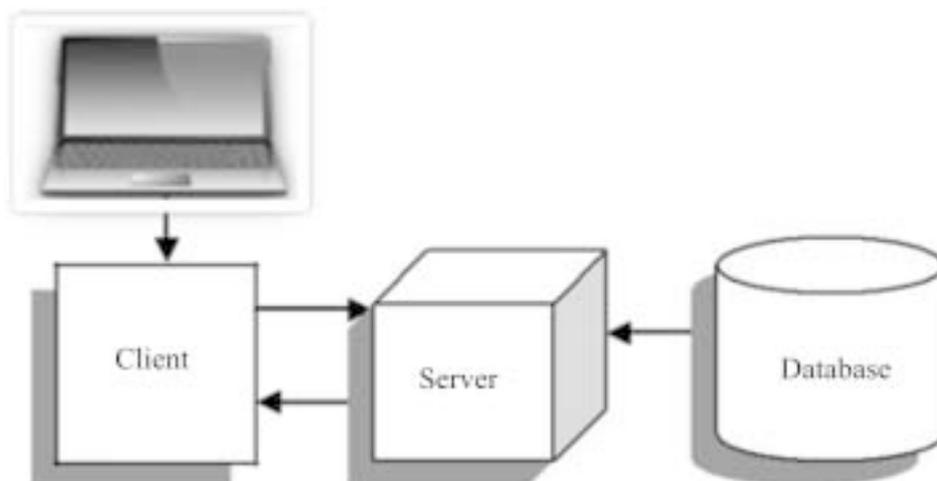
ATTACK	DESCRIPTION
Passive Attack	Monitors unencrypted traffic and looks for sensitive information
Active Attack	The attacker tries to bypass or break into secured systems
Distributed Attack	It introduces code such as Trojan horse to a trusted software
Insider Attack	It involves someone from the inside attacking the network.
Close-in Attack	This involves someone attempting to get physically close to data
Phishing Attack	The hacker creates a fake website that looks like an original website.
Hijack Attack	The hacker takes over a session between you and another person.
Spoof Attack	The hacker modifies the source address of the packets.

#### A. Password and pin based

Passwords and PINs are most commonly used authentication methods. These are known as Knowledge-based methods as users memorize their passwords. Passwords can be single words, numeric, phrases, any combination of these or personal identification number. For stronger protection, password should be longer. Plain passwords must be avoided as far as possible. In an authentication system, a strong password should be a combination of numbers, letters, special characters and mixed cases. In order to protect password during data transmission, the Transport Layer Security (TLS) or Secure Socket Layer (SSL) features, which can generate an encrypted channel for data exchange, should also be enabled for authentication systems. Cases have been reported of

user ID's and passwords being stolen by fraudsters through phishing emails, fake websites, Trojan software and other malicious software. Since such attacks are focused on the end-user side, raising the awareness of user is very important so that they can protect their interests in their daily transactions. Unusual knowledge-based methods can also be adopted based on visual images (graphical password). One example is that a user is presented with a series of five randomly generated life-like faces and the user repeatedly picks out the faces from a series of grids filled with more faces. By picking the correct faces, the user has effectively typed in his password.

Fig.1 shows working of password based authentication technique. The user first enters a name and password. It is required that the Client application binds itself

**Fig.1 Server based authentication**

to the Directory Server with a distinguished Name. The client uses the name entered by user to retrieve domain name. Next the client sends these credentials to the Directory Server. The server then verifies the password sent by the client by comparing it against the password stored in database. If it matches, the server accepts the credentials for authenticating the user identity. Then the server allows client so authorized to access the resources.

### B. Token Based

This is a physical device that performs authentication and hence can be termed as object based. Tokens can be compared with physical keys to houses that are used as a token but in digital tokens many other factors are present to provide information safety. In digital world, security tokens are used. The general concept behind a token based authentication system is simple. Allow users to enter their username and password in order to obtain a token which allows them to fetch a specific resource-without using their username and password. Once their token has been obtained, the user can offer the token-which offers access to a specific resource for a time period-to the remote site. Tokens themselves have password so even if they are lost, the hackers cannot modify the vital information. Bank cards, smart cards are security token storage devices with passwords and pass codes. Pass codes are same as password except that the former are machine generated and stored. There exist one time security tokens and smartcards as. Analysis involves finding out the user expectations or needs regarding new or modified software. It involves frequent communication with the system user for requirement findings and specifying

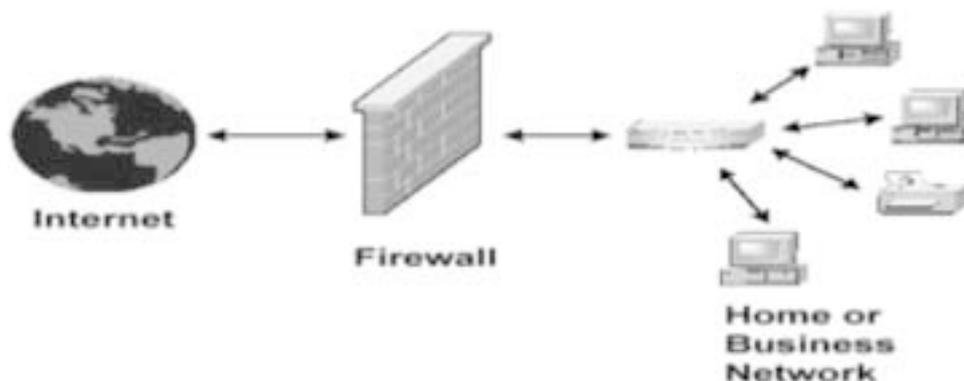
those requirements in the Software Requirement Specification document.

### C. Biometric Based

Biometric authentication is the process of verifying if a user is whom he is claiming to be, using digitized biological signatures of the user. Biometric authentication can be classified into two groups: physiological and behavioral. In physiological authentication, faces, finger prints, hands, iris and retina follow. And in the case of behavioral, voice prints, signatures and keystrokes are used. This technique can term as ID based. This technique is safer as compared to password and token based techniques. Biometric authentication techniques are currently in operation in various enterprises. They are used for passports, visas, personal identification cards, accessing bank machines, doorway access control, and general computer desktop access

### Working of Firewall in PC

There are various different methods firewalls use to filter out data, and some are used in combination. These methods work at dissimilar layers of a network, which determines how specific the filtering options can be used. Firewalls can be used in a number of ways to add protection to your home or business. Large organization or corporations often have very complex firewalls in place to secure their networks. On the other side, firewalls can be configured to avoid employees from sending certain types of mails or transmitting confidence data outside of the network. On the inbound side, firewalls can be programmed to stop access to certain websites like social networking sites.



**Fig. 2 Working of Firewall**

Moreover, firewalls can prevent outside computers from accessing computers inside the network.

A company might choose to select a single computer on the network for file sharing and all other computers could be controlled. There is no limit to the variety of configurations that are possible when using firewalls.

For residence use, firewalls work much more basically. The main goal of a standalone firewall is to protect your personal computer and private network from various threats. Malware, malicious software, is the main threat to your home computer. Viruses are the first type of malware that comes to mind. A virus can be transmitted to your system through email or over the Internet and can quickly cause a lot of injury to your files.

There are two ways a Firewall can prevent this from occurrence. It can allow all interchange to pass through except data that meets a preset set of criteria.

Firewall uses the later way to prevent malware from installing on your computer. This free software firewall, from a global security solutions provider and certification power, uses the patent pending "Clean PC mode" to disallow any application from being installed on your computer unless it meets one of two criteria. Those criteria are as follow a) the user gives authorization for the installation and b) the application is on a widespread list of standard applications provided by this firewall. With this feature, you don't have to worry about unauthorized programs installing on your computer without your awareness.

#### *A. Firewall Technology Overview*

A firewall works like a filter between your computer and the Internet. Firewalls can also do auditing. With firewall you can decide, data which can be accessed on your network and which should not. A firewall can look at a whole packet's contents. There are various different types of firewall used to filter out information. Firewalls can be used in business and at homes too. In business firewalls can prevent employees from sending sensitive data outside the organization and can also be programmed to restrict access to certain websites. For home use the main goal of firewall is to protect your computer from malware or malicious software.

#### *A.1 Packet Filters*

The simplest form of firewall is packet filter. On the Internet, the aim of packet filtering is to allow or block packets based on source and destination addresses, ports, or protocols. A packet is sent from source to destination only if it is certified. A packet filter look at five things like the source and destination IP addresses, the source and destination ports, and the protocol such as UDP, TCP/IP, and so on. As packet filter deals with individual packets a decision is to be made for each and every packet, whether that particular packet can pass or should undergo some other action. Due to its simplicity and speed, a packet filter can be enabled on your routers, eliminating the need of a dedicated firewall. There are some problems with packet filters:

1. They generally do not have any idea about what is being sent in the packets.
2. They are not able to successfully handle protocols that rely on various dynamic conditions.

#### *A.2. Application Gateways*

An application gateway is also known as application proxy or application-level proxy such as an SMTP proxy that understand the SMTP protocol and it is a program that runs on a firewall system between two networks. An application gateway is one step farther than a packet filter as instead of simply checking the IP parameters, it actually looks at the application layer data. When a client program creates a connection to a destination service, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to communicate with the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. This creates two connections: one between the client and the proxy server and one between the proxy server and the destination. Once connected, the proxy makes all packet-forwarding decisions. Since all communication is conducted through the proxy server, computers behind the firewall are protected. An application gateway check the data that is being sent and authenticate that the particular protocol is

being used perfectly. Let's say we were creating an SMTP application gateway. It would need to keep track of the state of the link: Has the client sent a HELO/ELHO request? Has it sent a MAIL FROM before attempting to send a DATA request? As long as the protocol is obeyed, the proxy will shuttle the commands from the client to the server. The application gateway must understand the protocol and process both sides of the conversation. As such, it is a much more CPU exhaustive process than a simple packet filter. However, this also lends it a larger element of security. You will not be able to run the earlier described SSH- over-port-25 trick when an application gateway is in the way because it will realize that SMTP is not in use. Furthermore, because an application gateway understands the protocols in use, it is able to support difficult protocols such as FTP that create casual data channels for each file transfer. As it reads the FTP command channel, it will make out the data channel declaration and allow the specified port to traverse the firewall only until the data transfer is complete. Often there is a protocol that is not directly understood by your application gateway but that must be allowed to traverse the firewall. SSH and HTTPS are two effortless examples. Because they are encrypted end to end, an application gateway cannot read the traffic actually being sent. In these cases, there is usually a way to configure your firewall to allow the appropriate packets to be sent without invasion by the firewall. It can be difficult to put together application gateways into your standard routing hardware due to the processing overhead [10]. Some newer high-end routers are able to function as application gateways, but you'll need plenty of CPU power for satisfactory presentation.

### A.3. Stateful Inspection

In computing, a this firewall is a firewall that keeps track of the state of network associations (such as TCP streams, UDP communication) travelling across it. The firewall is programmed to differentiate legal packets for different types of connections. Only packets matching is an active connection will be allowed by the firewall; others will be rejected it inspection, also referred to as Dynamic Packet Filtering, is a security feature. Check Point Software introduced this inspection in the use of its Firewall 1

in 1994, this firewall assessment takes the basic ethics of packet filtering and adds the concept, so that the Firewall considers the packets in the context of before packets. So for example, it records when it sees a packet in an internal table and in many execution will only allow TCP packets that match an existing conversation to be forwarded to the network. This has a number of advantages over simpler packet filtering: It is possible to build up firewall rules for protocols which cannot be correctly controlled by packet filtering. There is a risk that vulnerabilities in individual protocol decoders could permit an attacker to gain control over the firewall. This worry highlights the need to keep firewall software updated. Some of these firewalls also increase the possibility that personally hosts can be trick into solicit outside connections. This option can only be totally eliminated by auditing the host software. Some firewalls can be conquered in this way by simply screening a web page. More complete control of traffic is possible [6]. Equally, there are some disadvantages to this assessment solution, in that the execution is automatically more complex and therefore more likely to be errors. It also requires a device with more memory and a more influential CPU for a given traffic weight, as data has to be stored about each and every load flow seen over a period of time.

### B. Firewall Testing

Firewalls plays important role in network protection and in many cases build the only line of security against the unidentified rival, systematic Firewall testing has been ignored over years. The reason for this lies in the missing of undependable, helpful and received testing methodologies. Efficiency testing is hard to do without particular tools, and even if you have particular tools, you may not get good results. Efficiency testing should focus on three areas: (1) intrusion prevention (2) antimalware (3) application identification. If you want to block peer-to-peer file sharing, open a few different Torrent clients and see what happens. Performance testing has to be completed by "pass/fail" indicators. For example, when the firewall starts to reject to open new sessions, the test should end as you have gone away from the limits. You should also set other limits, such as greatest latency time, to define when the firewall is not behaving sufficiently well. Do the same for applications such

as webmail or face book, which both are the most important candidates for application identification and control. Don't try an automatic test tool, as the results are never as exact as the real application talking to real servers. This is especially correct of applications that are ambiguous, such as Bit Torrent and Skype, which can never be perfectly virtual in a test tool. Performance testing also usually requires particular tools, but has become so well- liked that there are open source alternative. When testing presentation remember to check your bad test against a null device a router or patch cable would work. This will tell you the maximum speed of your analysis bed. From there, keep in mind noted network tester David Newman's Laws of Testing: It must be repeatable, it must be worrying, and it must be significant. Take the device you're testing to its confines, even if you don't predict going that far. This will tell you where you will hit a wall in the upcoming and where you have sufficient headroom to grow. There are three general approaches to firewall testing:

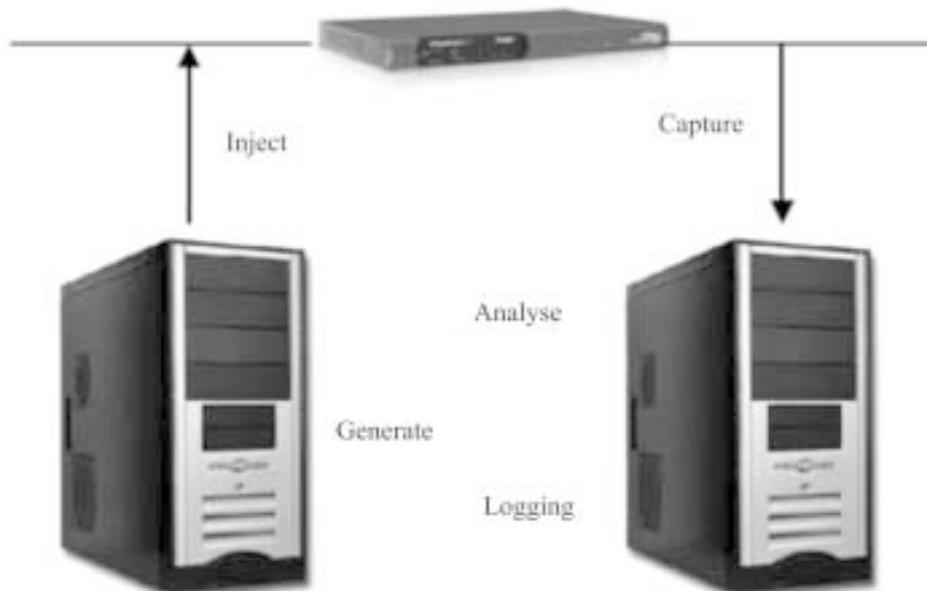
- 1) Penetration testing
- 2) Testing of the firewall implementation
- 3) Testing of the firewall rules

The goal of penetration testing is to expose security flaw of a goal network by running attacks against it.

Penetration testing includes information get-together, searching the network and attacking the target. The attacks are performed by running vulnerability testing tools, Saint that check the firewall for likely breaches of security to be exploited. If vulnerabilities are detected, they have to be permanent. Penetration testing is usually performed by the system administrators themselves or by a third party (e.g. hackers, security experts) that try to break into the computer system. The problem is that we have to be sure that we can trust the external experts. Penetration testing is a way to perform firewall testing but it is not the only one and it is not the way we precede.

Testing of the firewall working focuses on the firewall software. The examiner checks the firewall working for bugs. Different firewall commodities support different firewall

languages. Thus, firewall rules are vendor-exact. Consider a hardware firewall deploying vendor- exact firewall rules. The firewall execution testing approach evaluates if the firewall rules communicate to the action of the firewall. Firewall execution testing is primarily performed by the firewall vendors to increase the consistency of their products. Testing of the firewall rules confirmed whether the security policy is correctly executed by a set of firewall rules. A security plan is a



**Figure 3: Testing of Firewall**

document that sets the basic mandatory rules and morality on information security. Such a document should be plan in every company. The firewall rules are future to implement the directives in the security plan. Considering the test packet driven advance, firewall testing includes two phases: The identification of appropriate test cases that examine the behavior of the firewall and the practical performance of these tests.

## Conclusion

Network security can be maintained by making use of various authentication techniques. User has to use authentication technique depending on requirement. Password based technique is best if you have to

remember a single password. But problems occur when we have to remember many passwords so we use those passwords that are easy to remember. Token based techniques provide added security against denial of service (DoS) attacks. In comparison to above two, techniques biometric cannot be easily stolen so it provides stronger protection. As signals, biometric can be easily copied by attackers so it should not be deployed in single factor mode. Furthermore we can choose a combination of above technique as discussed above. The firewall also has its own limitations All the techniques have their pros and cons. We have to be smart to choose as per our requirement of safety of networks and information by considering cost factor.

## References

1. Lawrence O" Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 à 2003 IEEE.
2. Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", IJVIPNS-IJENS Vol: 10 No. 04.
3. [Online]Available:  
<http://www.authenticationworld.com/Token-Authentication>
4. [Online]Available:  
<http://www.authenticationworld.com/Authentication-Biometrics>.
5. Jae-Jung Kim and Seng-Phil Hong, "A Method of Risk Assessment for Multi-Factor Authentication", Journal of Information Processing Systems, Vol. 7, No.1, March 2011.
6. Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast Authentication in the Smart Grid with One Time Signature", IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011.
7. [Online]Available:<http://www.duosecurity.com>.
8. [Online]Available:[http://ids.nic.in/technical\\_letter\\_TNL\\_JCES\\_JUL\\_2013/Advance%20Authentication%20Technique.pdf](http://ids.nic.in/technical_letter_TNL_JCES_JUL_2013/Advance%20Authentication%20Technique.pdf).
9. Stamati Gkarafli, Anastasios A. Economides, "Comparing the Proof by Knowledge Authentication Techniques", International Journal of Computer Science and Security (IJSS), Volume(4): Issue (2).
10. Roger Meyer, "Secure authentication on the internet" As the part of security reading room, SANS institute 2007.
11. Canghong Zhang, based on network security firew All technology, Information technology, Chinese new Technology new product, 2009.
12. Rui Wang, Haibo Lin, Network security and firewall Technology, Tsinghua university publishing house, In 2000.
13. Kuang chu, network security and firewall technology, Chongqing university publishing house, 2005.
14. S. Smith, E. Palmer, and S. Weingart, "Using a high-Performance, programmable secure coprocessor," in Proc. International Conference on Financial Cryptography, Anguilla, British West Indies, 1998.

# Cyber Security in Biometrics Using Fingerprints

Priyanka Rattan\*

Ritika Kapoor\*\*

---

## Abstract

Nowadays, industries are experiencing technological advancement. With the rise of globalization, it is essential to have an easier and more effective system. Security is a major concern for organizations nowadays as security related risks may affect the organization's information assets badly. One method of ensuring a secure system is the Biometric System. It is a system that uses information about a person that identifies a person. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometrics is an automated method of recognizing a person based on a physiological or behavioral characteristic. Physiological biometrics works by analysing the human body characteristics such as face recognition, fingerprint, face, retina, and iris and behavioral biometrics is based on the person's behavior, e.g. voice recognition. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. This paper covers the use of fingerprints scanning in biometrics. Fingerprint recognition is one of the most well known biometrics, and it is by far the most used biometric solution for authentication on computerized systems. Fingerprints vary from person to person (even identical twins have different prints) and don't change over time. Finger-scan technology is the most widely deployed biometric technology, with a number of different vendors offering a wide range of solutions. Thus biometrics is a means to protect security of data. This paper also covers biometrics recognition, types of biometrics and application of biometrics. One primary conclusion is that identification should be considered as a component of development policy.

**Keywords:** Biometrics, Fingerprint, Security, biometric identification

---

## Introduction

There are two types of systems that help establish the identity of a person: verification systems and identification systems. In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic card, login name, smart card, etc., and the system either rejects or accepts on the basis of identity of a person (Am I who I claim I am?). In an identification system, the system establishes a person's identity (or fails if the person is not enrolled in the system database) without the person having to claim an identity (Who am I?). The topic of this paper is a verification system based on fingerprints, and the terms verification, authentication, and identification are used synonymously.

---

**Priyanka Rattan\***

Trinity Institute of Professional Studies

**Ritika Kapoor\*\***

Trinity Institute of Professional Studies

Among the most remarkable strengths of fingerprint recognition, few are the following:

- Its maturity, providing a high level of recognition accuracy.
- The growing market of low-cost small-size acquisition devices, allowing its use in a broad range of applications, e.g., electronic commerce, physical access, PC logon, etc.
- The use of easy-to-use devices, not requiring complex user-system interaction.

Accurate automatic personal identification is becoming more and more important to the operation of our increasingly electronically interconnected information society. Traditional automatic personal identification technologies to verify the identity of a person, which use "something that you know," such as a personal identification number (PIN), or "something that you have," such as an identification (ID) card, key, etc., are no longer considered reliable enough to satisfy the

security requirements of electronic transactions. All of these techniques suffer from a common problem of inability to differentiate between an authorized person and an unauthorized who fraudulently acquires the access privilege of the authorized person.

## History of Fingerprints

There are records of fingerprints being taken many centuries ago, although they weren't nearly as sophisticated as they are today. In ancient era people pressed the tips of their fingertips into clay to record business transactions. The Chinese used ink-on-paper finger impressions for business and to help identify their children. Until the 19th century fingerprints weren't used as a method for identifying criminals. A few years later, Scottish doctor Henry Faulds was working in Japan when he discovered fingerprints left by artists on ancient pieces of clay. This finding inspired him to begin investigating fingerprints. In 1880, Faulds and Charles Darwin developed fingerprint classification system. Further Galton collected measurements on people around the world to determine how traits were inherited from one generation to the next. He began collecting fingerprints and eventually gathered 8,000 different samples to analyze. In 1892, he published a book called "Fingerprints," in which he outlined a fingerprint classification system — the first in existence. The system was based on patterns of arches, loops and whorls. Sir Edward Henry, commissioner of the Metropolitan Police of London, became interested in using fingerprints to catch criminals. In 1896, he added to Galton's technique, creating his own classification system based on the direction, flow, pattern and other characteristics of the friction ridges in fingerprints.

Examiners would turn these characteristics into equations and classifications that could distinguish one person's print from another's. In 1901, Scotland Yard established its first Fingerprint Bureau. The following year, fingerprints were presented as evidence for the first time in English courts. In 1903, the New York state prisons adopted the use of fingerprints, followed later by the FBI.

## State of the Art in Fingerprint Recognition

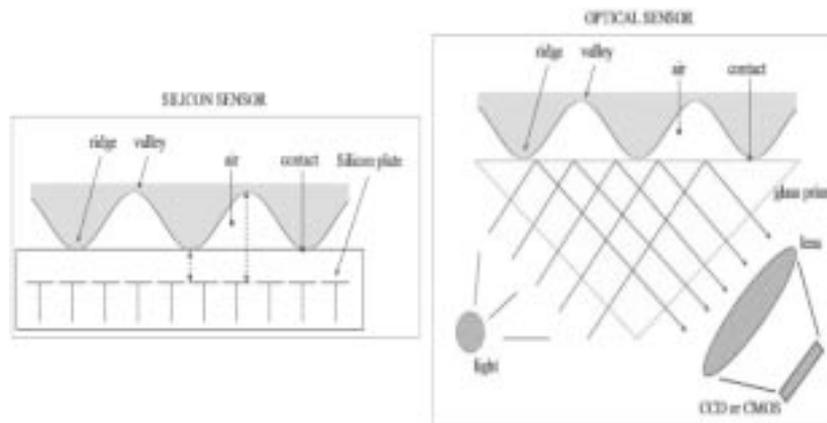
Fingerprint Recognition is the process in which we find out used whether two sets of fingerprint ridge detail come from the same finger. This paper presents a basic introduction to fingerprint recognition systems and their main parts, including a brief description of the process and applications of fingerprints. The main modules of a fingerprint verification system are: a) fingerprint sensing, in which the fingerprint of an individual is taken by a fingerprint scanner to produce a raw digital representation; b) preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction; c) feature *extraction*, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors; and d) matching, in which the feature vector of the input fingerprint is compared against one or more existing records. The records of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints.

### a) Fingerprint Sensing

The processing of fingerprint images is done by spreading the finger with ink and pressing it against a paper card. The paper card is then scanned,



**Fig1. Process of Fingerprint Recognition**



**Fig 2. Acquisition principles of silicon and optical sensors**

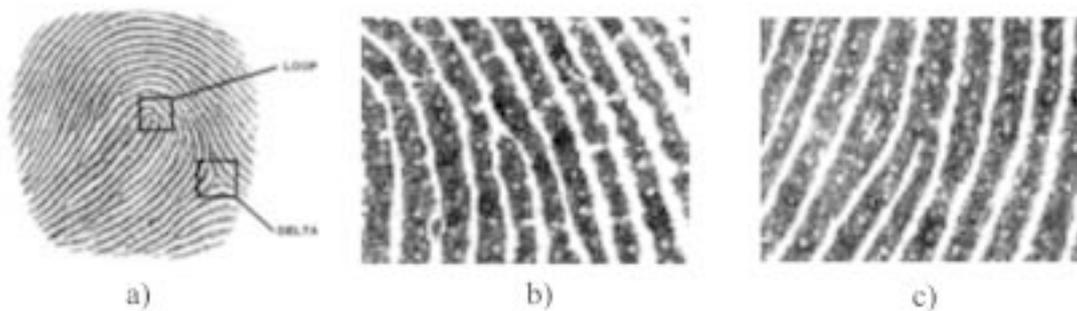
resulting in a digital representation. This process is known as off-line acquisition. Currently, it is possible to acquire fingerprint images by pressing the finger against the flat surface of an electronic fingerprint sensor. This process is known as *online* acquisition. There are three families of electronic fingerprint sensors based on the sensing technology:

- I. *Solid-state* or silicon sensors (left part of Fig 2): These contain an array of pixels where each pixel represents a sensor itself. Users place the finger on the surface of the silicon, and four techniques are typically used to convert the ridge/valley information into an electrical signal: capacitive, thermal, electric field and piezoelectric. Since solid-state sensors do not use optical components, their size is considerably smaller and can be easily embedded. On the other hand, silicon sensors are expensive, so the sensing area of solid-state sensors is typically small.
- II. *Optical* (right part of Fig.2): The finger touches a glass prism and the prism is illuminated with diffused light. The light is reflected at the valleys and absorbed at the ridges. The reflected light is focused onto a CCD or CMOS sensor. Optical fingerprint sensors provide good image quality and large sensing area but they cannot be miniaturized because as the distance between the prism and the image sensor is reduced, more optical distortion is introduced in the acquired image.
- III. *Ultrasound*: Acoustic signals are sent, capturing the echo signals that are reflected at the fingerprint

surface. Acoustic signals are able to cross dirt and oil that may be present in the finger, thus giving good quality images. On the other hand, ultrasound scanners are large and expensive, and take some seconds to acquire an image.

#### b) Preprocessing and Feature Extraction

The process of enhancing the image before the feature extraction is also called pre-processing. A fingerprint is characterized by a pattern of interleaved ridges (dark lines) and valleys (bright lines). Generally, ridges and valleys run in parallel and sometimes they terminate or they bifurcate. At a global level, the fingerprint may present regions with patterns of high curvature, these regions are also called singularity. This pattern sometimes exhibits a number of particular shapes called *singularities*, which can be classified into three types: *loop*, *delta* and *whorl*. At the local level, other important feature called minutia can be found in the fingerprint patterns. Minutia mean small details, and this refers to the behavior of the ridges discontinuities such as termination, bifurcation and trifurcation or other features such as pores (small holes inside the ridges), lake (two closed bifurcations), dot (short ridges), etc. Most system uses only the termination and bifurcations. With the objective of matching the fingerprints we need to extract the fingerprint features such as minutiae and singularity points. From the fingerprint we can also extract other global information such as orientation and frequency of the ridge regions.



**Fig. 3. a) Loop b) Delta c) Whorl**

### c) Fingerprint Matching

In the matching process, features extracted from the input fingerprint are compared against those in the stored database, which represents a single user (retrieved from the system database based on the claimed identity). The result of such a procedure is either a degree of similarity (also called matching score) or an acceptance/rejection decision. There are fingerprint matching techniques that directly compare gray scale images

using correlation-based methods, so that the fingerprint record matches with the gray scale image.

### Comparison of Biometric Technologies

Currently, there are mainly nine different biometric techniques that are either widely used. Including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermograms. A brief comparison of these nine biometric techniques

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Hand Vein	medium	medium	medium	medium	medium	medium	high
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice Print	medium	low	low	medium	low	high	low
F. Thermograms	high	high	low	high	medium	high	high

**Fig. 4: Comparison of Biometric Technologies**

is provided in Fig 4. Although each of these techniques satisfies the above requirements and has been used in practical systems or has the potential to become a valid biometric technique not many of them are acceptable as indisputable evidence of identity. For example, despite the fact that extensive studies have been conducted on automatic face recognition and that a number of face-recognition systems are available it has not yet been proven that face can be used reliably to verify identity and a biometric system that uses only face can achieve an acceptable identification accuracy. So far, the only acceptable, automated, and mature biometric technique is the automatic fingerprint identification technique, which has been used and accepted in forensics since the early 1970's.

### **Applications of biometrics**

Biometrics is a rapidly evolving technology that has been widely used in forensics, such as criminal identification, prison security and broad range of civilian applications. The use of fingerprints as a biometric is the oldest mode of computer-aided and personal identification that is most prevalent today.

Following are the various applications of biometrics:-

- 1) Banking security, such as electronic fund transfers, ATM security, cheque cashing, and credit card transactions
- 2) Physical access control, such as airport access control
- 3) Information system security, such as access to databases via login privileges
- 4) Government benefits distribution, such as welfare disbursement programs
- 5) Customs and immigration, such as the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry
- 6) National ID systems, which provide a unique ID to the citizens and integrate different government services
- 7) Voter and driver registration, providing registration facilities for voters and drivers.

### **Future Scope**

The upcoming techniques of user authentication, which involves the use of passwords and user IDs or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords such as birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric fingerprint authentication technology may solve this problem since a person's biometric data is connected to its owner, is unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card.

### **Conclusion**

Biometrics is a means of verifying personal identity by measuring and analyzing unique physical or behavioral characteristics like fingerprints or voice patterns. The conclusion of this paper is that the manual system should be replaced and there must be easier, reliable, secure, cash free and tension free electronic system, i.e. biometric system in which no one has to take dozens of cards for shopping, traveling, university or bank. So to consider the disadvantages of manual system, the fingerprints system is suggested to be implemented because it is easier, reliable, feasible, secure and authorized to everyone. There is no worry that anyone can stole my finger and anybody can use it. In fingerprint system customer has to place his fingers on the finger scanner and then scanner will recognize the account which belongs to that person and perform the action. Biometric system may be like fingerprints, IRIS, face recognition and blood reading or skin reading and it may be installed at any store, university, library, hostel, bank, office, home door lock, internet online shopping and many kinds where card system is installed. So in this paper we conclude that finger print system is the best biometric for identification of an individual.

## References

1. N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", *Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223-228, 2001.
2. A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "FingerCode: A filterbank for fingerprint representation and matching", *Proc. IEEE Conf. on Computer Vision and Pattern Recognition*, vol. 2, pp. 187-193, 1999.
3. L. O'Gorman, "Overview of fingerprint verification technologies", Elsevier Information Security Technical Report, vol. 3, no. 1, 1998.
4. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021– 2040, Dec. 2003.
5. O' Gorman, L.: Fingerprint Verification, in *Biometrics: Personal Identification in Networked Society*, The Kluwer Academic Publishers, International Series in Engineering and Computer Science, Jain, A. K., Bolle R. and Pankanti, S. eds., Vol. 479, Chapter 2, pp. 43-64 (1999).
6. Uludag, U., Jain, A.: Attacks on biometric systems: a case study in fingerprints. *Proc. SPIEEI2004, Security, Seganography and Watermarking of Multimedia Contents VI* pp. 622–633 (2004)
7. Putte, T., Keuning, J.: Biometrical fingerprint recognition: dont get your fingers burned. *Proc.IFIP TC8/WG8.8, Fourth Working Conf. Smart Card Research and Adv. App.* pp. 289–303 (2000)
8. Jiang, X., Yau, W., Ser, W.: Detecting the fingerprint minutiae by adaptive tracing the gray level ridge. *Pattern Recognition* 34, 999–1013 (2001)

# The Online Murder: Death via Hacked Internet Connected Technologies

Nishtha Girotra\*

Raghunatha Sethupathy\*\*

---

## Abstract

Recently it was specified in the newspaper article that the first online murder is expected to take place in the end of 2014, but fortunately there was no such incident. After this news, everyone in this world really wanted to know about online murder and the events which are associated with it. So this research is an attempt to study about the online murder and its consequence where the researchers have adopted a theoretical review of various documents available in the globe. The authors have made use of the online articles for carrying out this particular research and this is non-quantitative research adopted by reviewing the existing literature. Online murder is one among the gravest cybercrimes and it is predicted by the European police office (Europol) that in near future one such murder will soon occur. So the paper lays its great deal of emphasize on online murder which is classified in this paper as Direct and Indirect murder. The researchers have also focused on the conversion of the society from Internet of Things(IoT) to Internet of Everything (IoE.) The paper focuses on the security aspects of online murder with special emphasize on the Indian Scenario.

**Keywords:** Online Murder, Internet of Everything, Europol Report

---

## Introduction

The time was called as 'age of machines' of late 19th and 20th century and then came the 'age of information' which was when the period of computerization began. Now, it is the era of 'internet of things' and within few decades there will be a time when the internet will be connected to everything and it will said as the era of 'internet of everything'. With the increasing accessibility and connectivity to internet, heinous crimes are also increasing and the biggest crime i.e murder, can now be done by a person sitting far away, by just cracking into the somebody's system and that too, just with a press of a button. He can then stop the functioning of any system or enter some malicious codes and thereby, taking all control in his hands, he can endanger the lives of innocent people. Online murder is one among the gravest cybercrimes

---

### Nishtha Girotra

Student, Campus Law Centre, Delhi University  
E-45, Kamla Nagar, New Delhi

### Raghunatha Sethupathy

Student, Campus Law Centre, Delhi University  
8/61, Vijay Nagar Double Storey, New Delhi

and it is predicted by the European police office (Europol) that in near future one such murder will soon occur [1]. Cybercrimes are increasing at a rapid rate and there is an urgent need to check this. If proper steps are not taken, some easy cheap tools and services will help nefarious people to execute their plans easily. The authors have made use of the online articles for carrying out this particular research and this is non-quantitative research adopted by reviewing the existing literature.

## Internet of Everything

In the virtual world, there is an easy connectivity to physical items around us but the unfortunate part is that the hackers can easily step in the working of these systems and then hack, control, and create and cause issues, due to low cyber-security. With the help of Radio Frequency Identification (RFID) and sensor network technologies everything from automobiles, home appliances to medical devices all will be soon connected. This is easily evident with the increasing use of wifi and wireless internet connectors. Today, around nine billion devices are connected to internet, and the number is increasing at such a fast pace that

probably by 2020 around twenty billion appliances will be connected. From exercise machines, electric toothbrushes, sewing machines, electricity meters, washing machine and thermostats etc. all are connected to networks and rest appliances will also be soon in communication with these.

### **Death by Internet**

Homicide caused through internet can be done in two ways –

- 3.1. Indirect murder
- 3.2. Direct murder

#### **Indirect Murder**

Killing through the use of internet has become a common piece of news since 1990's. All corners of the earth are connected today and this connectivity like any other advancement has also come up with the frightening crimes. Earlier in early 90's the crimes were carried on by publishing advertisements in newspapers and inviting deceitfully naïve people to submit to the cruelty of the criminals. The trend changed with the growth of the use of internet which has become the fertile ground to cheat people. There have been many cases of extortion, blackmailing through internet. Also online dating, chat rooms, online marriage bureau, and advertisements are the tactics used by the notorious criminals to commit murders. This is an easy weapon for them and their enemies are an easy prey of this. The below given few examples will make it clearer:

1. The planned murder of Ofir Rahum, Palestine Liberation Organization, took place after a long conversation of the criminal with the victim through ICQ where the victims came for romantic purposes; he was shot down on coming to Jerusalem. [2]
2. Michael Jhon Anderson, a resident of Savage, Minnesota, who used Craigslist, was convicted for calling a lady for babysitting job and then shooting her [3].
3. In 2009, Christian Goocher, who was believed to be 'first German internet killer', confessed that he had killed women using chat rooms [4].
4. In 2011, a girl student from IIM, Bangalore has put herself to death after her boyfriend who was

an alumnus of IIT, Roorkee posted a hurtful message about their breakup in his facebook wall [5].

According to The Dailymail report, around one Facebook crime occurs in every 40 minutes.

#### **Direct Murder**

New kind of murders is predicted to take place in near future where a person can be killed easily by the use of networks. This is more easily evident in the case of medical devices. It is believed that many devices like the insulin pump, heart pacemakers etc. can be easily hacked and mishandled resulting in an over dosage or an explosion. This particular concept of online murder, is not new but in a report by a medical cyber-security pioneer, Kevin Fu and his partners, this idea was brought forward in 2008, where he mentioned that the medical devices like pacemakers can be hacked [6]. In case of insulin pumps, a security researcher, named Jay Radcliffe, has shown how by the use of strong antenna, the device can easily be hacked. This hacking would have the potential to kill the victim and the criminal can do this even by being half a mile away from the site. The connected insulin pump is used to have controlled frequency and amount of dose for a better treatment. The data entry is given by an external blood glucose device and this advanced continuous glucose monitor uses sensors which can also be hacked and then misused to the extent of causing death [7]. Baranby Michael Douglas Jack, was a New Zealand computer security expert who showed that a laptop which is 50 feet away can easily hack a pacemaker and create a shock of 830 volt by increasing the jolt of electricity in the device. He also brought forward the way how one can onboard firmware can be rewritten and the device can be corrupted. The servers can now be diseased with malicious firmware and that would be capable of infecting pacemakers and ICDs. He said in his blog that "We are potentially looking at a worm with the ability to commit mass murder [8]." A highly controversial issue is the murder of Rolling star and Buzfeed hero, Michael Hastings, who died in high-speed car driving and it was believed that it was a case of cyber-attack. The Former US National Coordinator for Security, Infrastructure Protection, and Counterterrorism Richard Clarke, also said that 'the car accident was consistent with cyber-attack and the

reason is that, the intelligence agencies actually know how to catch hold of the control of the power of the car. Also before the accident, Hastings had informed other journalist through an email that FBI had an eye on his activities.

### **Security**

When the two computers were connected for the first time, the data protection issue arose and security measures were taken. Then with the advancement and use of networking, the security was needed to be strengthened. Today, an era is about to come when internet will be well connected to everything i.e both virtual and physical world and we would need to be little more careful about cyber-attacks which otherwise would become an easy weapon to commit evils. To have a safe environment around proper security should be maintained. Failing to address these issues, things such as nuclear reactor to cars would be hacked by the Cyber-Criminals, thereby leading to Mass-Murders as it appears in Video Games.

### **Crime as a Service**

Europol have mentioned in its meeting about the increasing cybercrimes services but the question arises as to what it is all about? This is actually a service provided by the underground criminals to people who do not even if have much technical knowledge, can commit cyber –crimes by just paying money for the tools and skills. The arrangement of money for a criminal attack is done by all customers together. By this way the service providers can earn a lot of money and the demand of these notorious customers are also fulfilled, with the small investments and without even having any expertise in it. This service now seems to be very attractive, with more and more people entering into it since profit earned out of this business is more than that of an amount, which the hacker gets from hacking and also investments made by the users, is comparatively smaller. So because of these things, a hacking is no more a big deal and these underground service is also a good market, an easier, cheaper and a simple channel to all crimes.

### **Indian Scenario**

Recently, the Government of India has come out with the Digital India and Smart City Initiative Project

which has many proposals and one of the proposals is the constitution of National Cyber Security Coordination Centre where the Government has proposed to spend around 11,000 Crores by 2015. So this proposal of the Government of India is an initiative in combating against large scale cybercrime including online murder. One of the important step taken in the Digital India Program of the Government which focuses at ‘transforming India into digital empowered society and knowledge economy’ is expected to provide a development of the IoT industry ecosystem in the country. Since India is converting itself from Internet of everything (IoT) to Internet of Everything (IoE), the incident of online murder is not so far from the future.

### **Conclusion & Suggestion**

In an article by Joseph Stienbergh, a columnist of cybersecurity, he mentions that the appliances we use today from television, laundry machines, telephone, medical devices, mobiles, and thermostats and even hand guns can be hacked. They can spy on us and collect all our data easily [9].

The following are the suggestions which can be done on an individual level:

1. One should not open unnecessary links which are popping from unknown websites and e-mail attachments received from unknown sources.
2. One should always keep their security software updated as by doing this, the security can be increased and viruses can be removed. New Viruses are discovered every day and based upon which anti-virus system are enhanced and strengthened.
3. One should avoid keeping the same password for all accounts as these in some or in the other way leads to hacking of the accounts.
4. Instead of using public wifi connection, one must invest in virtual private internet connection and securing the wifi connection is also an important task which has to be kept in mind.

On the other hand to control these cyber-attacks, changes must be made to security and legal systems. One of the reasons why these wireless devices are facing problems is that they were not built keeping in mind

the security issues. The systems used in the hospitals are running old windows version which can be easily hit by virus attacks. The real problem is that these systems [10] are not even allowed to update their versions due to regulatory restrictions. By loosening the restrictions on the equipment and bringing a change to legal protection issues, some good changes can be brought. The cyber-criminals are not just limited to a particular or native country but they are present everywhere around the globe. According to a report by the head of European cybercrime Centre,

Paul Gillen has suggested that there should be collaboration among the nations to stop these activities. The report also states that these cyber-attacks can be committed internationally and so the working of all nations and collectively becomes more important thing. The medical devices and all physical appliances connected to the network, should have a tighten security which needs to be constantly updated and access to the information of the data, must be disallowed as these may sometimes leads to Cyber-attacks.

## References

1. The Times of India Correspondent, "first online murder may happen by the end of the year: experts" Times of India retrieved on October 6, 2014 at, <http://www.thehindu.com/sci-tech/technology/internet/first-online-murder-may-happen-by-end-of-year-experts/article6475534.ece>.
2. Hershman Tania, "Israel's 'First Internet Murder'001," New York daily news, 19 January 2011
3. Michael John Anderson, "Craiglist Killer Michael John Anderson", New York Daily News, April 21, 2009
4. London Telegraph, "Internet killer' admits murdering women he met in online chat rooms", January 15, 2009
5. NDTV Correspondent, "IIM student commits suicide amid disturbing Facebook messages", NDTV (2011) retrieved on 12 January, 2015 at <http://www.ndtv.com/article/cities/iim-student-commits-suicide-amid-disturbing-facebook-messages-134966>
6. Kevin Fu and partners, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses", symposium on Security and Privacy.
7. Jerome Radcliff, "Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System", symposium on Security and Privacy, (2008)
8. Darlene storm, "Pacemaker hacker says worm could possibly 'commit mass murder'", Security is Sexy, 17 October, 2012
9. Joseph Stienberg, "these devices may be spying on us (even at our own home)", Forbes, 2013.
10. Website, *Department of Electronic and Information Technology, Ministry of Communications and IT, Government of India* retrieved at <http://deity.gov.in/content/internet-things> on 14, January, 2015

# Future Towards Danger: The Terror of Cyber Attacks

Kanika Sharma\*

Tanvi Bhalla\*\*

---

## Abstract

Cyber terrorism is the use of Internet attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, by the means of tools such as computer viruses [5]. As nation and critical infrastructure become more dependent on computer networks for their operations new vulnerabilities are created.

A hostile group could exploit these vulnerabilities to breach through a poorly secured network and disrupt or even shut down critical functions. All the data is stored on computers in the form of files and is vulnerable to be attacked and thus put ours as well as national security at risk because these files may contain confidential information about our military weapons etc. which if gone into wrong hands may lead to disastrous situations. The terrorists can change or type commands by hacking into a computer which can take over or disrupt the critical infrastructure of entire nation.

This paper covers what is cyber terrorism, what are the cyber attacks held, what the risks are and what preventive measures should be taken to prevent or handle cyber terrorism.

**Keywords:** Terrorism, SCADA, Denial of service (DoS), Cyber attacks.

---

## Introduction

In today's world, a nation and critical infrastructure has become more dependent on computer networks for their operation. This growing dependency has emerged as a new threat for security which can lead to Cyber Terrorism. With the development of cyber technology, the Internet has become an important channel for terrorists to carry out their activities. Cyber terrorism is the intentional use of computers, internet in terrorist activities to cause destruction and harm for personal objectives. A poorly secured network can easily be penetrated by the hostile nation or group which could disrupt or even shut down critical functions. Many terrorist groups make use of the internet for intra group communications, recruiting people, fund-raising, for creating a feeling of terror in people's minds. They can also steal credit card numbers or valuable data to provide financial support for their operations. There can be devastating situations if the national agencies or government policies information could be breached.

---

**Kanika Sharma\***

Management Education & Research Institute

**Tanvi Bhalla\*\***

Management Education & Research Institute

Disruption via cyber attacks could be caused to a variety of communication systems including Internet, mobile phones and cables. However, if the nation's security network could be penetrated so easily so, it means that the private sector infrastructures are also vulnerable. Telecommunications networks, electricity power grids, banks could be attacked by cyber terrorists. Such attacks could cause widespread panic and even damage to the country's economy.

## Terrorist attacks

(1) The Red team attack-

The first such attack was code named 'Eligible Receiver' was carried out by 35NSA computer hackers known as 'The Red Team'. They can only use software and hacking tools that can be easily downloaded from the Internet. They were authorized to break network but was not allowed to break any US laws. Their main target was the Pacific Command in Hawaii and they were easily able to breach into network and make minor changes in e-mails, disrupt telephone services and conduct denial-of-service attack and the best part was they were able to manage everything without being identified.

## (2) Sri Lankan embassy attack-

In 1998, ethnic Tamil guerrillas attempted to disrupt the Sri Lankan embassies by sending large number of e-mail. The Sri Lankan embassy received around 800 e-mails a day for two-week. The messages were “We are the Internet Black Tigers and we’re doing this to disrupt your communications”. It was characterized as the first known attack by the terrorists.

## (3) Attack on U.S. financial institutions-

In March 2013, a pattern of cyber attacks has been reported against U.S. financial institutions by The New York Times. It was believed to be instigated by Iran as well as by incidents affecting South Korean financial institutions.

## (4) Attack on media companies-

In August 2013, many media companies like the New York Times, Twitter and the Huffington Post lost control of some of their websites. The hackers were supporting the Syrian government who breached the Australian Internet company that manages many major site addresses.

## (5) Virus attack-

In September 2003, the ‘Welchia’ virus disabled the State Department’s consular Lookout and Support system. This system contained records from the FBI department, State department and US immigration.[1]

## (6) The attack on Iran nuclear power plant-

In July 2010, “the Stuxnet” computer worm was discovered. It is a windows based worm that spies on and subverts industrial systems. It includes a high specialized malware program that targeted Siemens Supervisory Control and Data Acquisition (SCADA) systems.

It damaged the Iran’s nuclear program Siemens SCADA systems. It specifically targeted the centrifuges which are used in the production of nuclear material, making them spin so fast that they get damaged. This attacked has set back the Iranian nuclear power plant for about two years. [7]

**Case of Estonia**

The Baltic state of Estonia was targeted to a massive denial-of-service attack. The attack consequence was it completely rendered the country offline and the

services dependent and Internet connectivity was shut down for three weeks. The infrastructure of Estonia including everything from online banking, mobile phone networks, government services and access to health care information was disabled for a time. The state was technology dependent and was in severe problem.

As a result, for security reasons Estonia joined NATO in 2004. NATO carefully monitored its member state’s response to the attack and worried both about escalation and the possibility of cascading effects beyond Estonia’s border to other NATO members. In 2008, as a result of the increasing attacks, NATO opened a new center of excellence on cyber defense to conduct research and training on cyber warfare in Tallinn.[5][9]

**Types of Cyber Attacks**

Different types of cyber terrorism attacks-

## 1. Incursion-:

The attacks which are carried out with the purpose of gaining access or penetrating into computer system or network in order to get or modify information. The computer systems and network are very insecure, terrorist take advantage to modify important information which can cause damages to the organization or individual.

## 2. Destruction-:

In this method, the attack is used to intrude into computer system and networks with purpose of inflicting severe damage or destroy them. These attacks are very disastrous to an organization as this costs them very heavy to get their operations up and running again.

## 3. Disinformation-:

This type of attack spreads fake information that can have severe impact to a particular target. These attacks create uncontrollable situation throughout the nation or in the organization.

## 4. Denial of Service-:

The objective of Denial of Service attacks is to disable or disrupt the network by flooding the target server with huge number of packets which ultimately lead the server being unable to handle



**Figure 1. Distribution of cyber hackers**

normal service request from legitimate users. This causes organizations to suffer massive loss.

5. Defacement of websites:-

These attacks focus in defacing the websites of the victims. The website is changed to include cyber terrorist message or to re-direct the users to other websites. [4]

### Preventive measures taken by the world

In May 2011, The Chinese Defense Military confirmed that it has an online defense unit known as “Blue Army”. It has 30 elite Internet specialists who are engaged in cyber defense operations.

On November 2, 2006, the Secretary of the Air Force announced the creation of the ‘Air Force Cyber Command’, whose task is to monitor and defend American interest in cyberspace. But later this plan was replaced by the creation of ‘Twenty-Fourth Air Force’ which became active in August 2009 and is a component of the planned United States Cyber Command.

Another security method is known as ‘sniffing’. It is the process of searching social websites, suspected terrorist web pages and even e-mails to detect terrorist activities or threats. A sniffer is a software program which is programmed to search Internet traffic for specific keywords. A sniffer can be authorized or unauthorized. An unauthorized sniffer can be a threat

because it can be inserted anywhere without permissions.

The US was one of the first countries that considered cyber terrorism to be a big problem in 2006 in terms of economy and national security.

### Cyber Terrorism in India

In March 2013, some Chinese hackers breached the computers of the Defense Research and Development organization, which is India’s top most military organization. It was a classical case of cyber war attack. Hackers from Algeria also carried out an attack on websites run by the DRDO, the Prime Minister’s Office and various other government departments were attacked by them. A group called ‘Pakistan Cyber Army’ had also hacked into several Indian websites.

Experts believe that India’s cyber security is not enough compatible to combat cyber attacks. Experts say that the country spends a small amount of money on cyber security. The budget allocation towards cyber security was Rs.42.2crore (\$7.76 million) for 2012-13. In comparison, the US spends several billion dollars through the National Security Agency, \$658 million through the Department of Homeland Security and \$93 million through US-CERT in 2013.[4]

### Prevention against cyber attacks in India

1. Indian government must collaborate with private sector to create an organization which is developed

mainly to detect and fight against cyber terrorism. Like, in Malaysia they established an International Multilateral Partnership against cyber terrorism (IMPACT), an effort to coax the world's govt.'s into collaboration on cyber security. Some of the major Indian organizations are not a member of IMPACT.

2. Perform required software updates for your operating system and web browser.
3. Install a firewall on your computer.
4. Change your passwords often on a weekly basis. So, that it will be difficult for the hackers to hack the e-mail accounts.
5. Purchase or download any anti-virus software which will detect any virus that can harm your data. It also provides browser security.
6. Install anti-spyware/adware programs onto your system.
7. Delete e-mails from unknown users. [6]

**Our recommendation**

In this paper we will like to propose our ideas for future implementation.

1. During creation of an e-mail account, generally the e-mail websites provide only 1 question for

the recovery of passwords or for authentication. Our idea is that we must provide some 5 uncommon personal questions during account creation. The user must answer to all the 5 questions. Whenever the user login, during sign in, a random question out of the 5 question appears on the screen must be answered by the user. This ensures that the user is the legitimate user. For further security, a message would be send to the user whenever he or she login.

2. To tackle the most common Denial of Service attack we are proposing following methodology-

DoS is the attack which makes a machine or network resource unavailable to its intended users so they are unable to serve them. To tackle this, every organization or a government department must have a "unique secret code" allotted to them. Whenever the sender sends the packet it must attach the secret code with the header of the outgoing packet. The recipient router must check the header of the incoming packet for the "unique secret code". If the code is present in the header, it indicates that the packet is send from the legitimate user then it is accepted otherwise it is discarded. This prevents Denial of Service attack.

**Table 1.**

Unique Secret S.A. Code	D.A.	Data	
-------------------------	------	------	--

Where, S.A. is source address and D.A. is destination address



**Figure 2. Distribution of Targets**

3. The improper and violent data and videos uploaded by the terrorists should not be displayed by sites like you tube etc. The websites should first check the data content that the user is going to upload and if it is violent and can hurt the sentiments of people then that content should be removed. Now-a –days terrorist groups are using social media like face book and twitter to engage and recruit youth into terrorist activities.

### **Conclusion and Future Scope**

Cyber terrorism is increasing day by day. It is very difficult to detect and prevent these attacks. We need to be more attentive and proactive towards cyber

security. Legal Policies against Cyber crime have to be established and implemented for nation's security. More cyber laws firms should be engaged in action towards cyber crime. More funds should be raised in this direction to fight against cyber security.

Government and private sector must collaborate with each other to work together as one hand in this direction. They must recruit ethical hackers and professional programmers to combat cyber security. The idea of "unique secret code" should be applied to reduce denial of service attack. We are still further working on this direction so that we can detect and punish cyber terrorist.

### **References**

1. <http://cyberterrorismpaper.blogspot.in/>
2. <http://www.thehindu.com/scitech/technology/towardscyberdefence/article4974205.ece>
3. <http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274>
4. Shamsuddin Abdul Jalil , Countering Cyber Terrorism Effectively: Are We Ready To Rumble?, June 2003, GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4b Option 1
5. <http://en.wikipedia.org/wiki/Cyberterrorism>
6. <http://www.wikihow.com/Prevent-Hacking>
7. By keith Giacobozzi, Cyber terrorism, 27 feb, 2011, <http://cyber-terrorismpaper.blogspot.in/>
8. <http://hackmageddon.com/tag/cyber-crime/>
9. <http://www.infosecurity magazine.com/magazine-features/cyberterrorism-a-look-into-the-future/>

# Method for Storing User Password Securely

Gunjan Jha\*  
Navneet Popli\*\*

---

## Abstract

Computer users are asked to generate, secret passwords for uses host accounts, email, e-commerce sites, and various online services. In this paper, I'll explain the theory for how to store user passwords securely; we propose technique that uses hashing, salting and Bcrypt to compute secure passwords for many accounts while needed user to memorize only a single short password. The combination of security and convenience will, we believe, entice users to adopt our method, we discuss various methods, compare its strengths and weaknesses to those of related approaches.

**Keywords:** Password Security, website user authentication, hashing, salting, Bcrypt.

---

## Introduction

Logging in with usernames and passwords has become one of the most ubiquitous and most reviled rituals of the Internet age. On the web, passwords are used by publications, blogs, and webmail providers.

We have multiple methods to store password securely in database. In this paper we will discuss about different methods in detail. We have methods like hashing, salting, and Bcrypt. We compare all the methods and analyze that which one is best in which scenario.

## Related Work

### Bad Solution : plain text password

It is not secure to store each users "plain text" password in database:

<b>user account</b>	<b>plain text password</b>
gunjan@hotmail.com	password
jassy@gmail.com	password123
...	...

This is insecure if a hacker gains access to database, they'll be able to use that password to login as that user on your database. This is even worse, if that user uses the same password for all other sites on the internet, the hacker can login there as well. Users will be very unhappy.

---

### Gunjan Jha\*

GGSSIP University (Meri College)

### Navneet Popli\*\*

GGSSIP University (Meri College)

### Bad Solution: sha1(password)

```
def is_password_correct(user, password_attempt):  
    return sha1(password_attempt) == user  
    ["sha1_password"]
```

A better solution is to store a "one-way hash" of the password, typically using a function like md5 () or sha1 ():

<b>user account</b>	<b>sha1(password)</b>
gunjan@hotmail.com	5baa61e4c9b93f3f0682250
mail.com	b6cf8331b7ee68fd8
jassy@gmail.com	cbfdac6008f9cab4083784c
	bd1874f76618d2a97
...	...

The server does not store the plain text password it can still authenticate user:

This solution is secure than storing the plain text , because in theory it should be impossible to "undo" a one-way hash function and find an input string that output the same hash value. Unfortunately, hackers found ways around this.

One problem is that many hash functions (including md5 () and sha1 ()) are not so "one-way" after all, and security expert suggest that these functions not be used anymore for security application. (Instead, you should use better hash functions like sha256 () which do not have any known vulnerabilities so far.)

But there's a bigger problem: hackers don't need to "undo" the hash function at all; they can just keep guessing input passwords until they find a match, It

is similar to trying all the combinations of a combination lock, Here what the code would look like:-

```
database_table = {
"5baa61e4c9b93f3f0682250b6cf83
31b7ee68fd8": "gunjan@hotmail.com",
"cbfdac6008f9cab4083784cbd187
4f76618d2a97": "jassy@gmail.com",
...}
for password
inLIST_OF_COMMONPASSWORDS:
if sha1(password) in databasetable:
print "Yepieeee I win! guessed a password!"
```

You might think that there are too many possible passwords for this technique to be possible. But there are far fewer common passwords than you'd think. People use passwords that are based on dictionary words (possibly with a few extra numbers or letters). And most hash functions like sha1 () can be executed very quickly -- one computer can literally try billions of combinations per second. It means **most passwords can be figured out in less than one cpu-hour.**

Aside: years ago, computers were not this fast, so the hacker community created tables that have pre-computed a large set of these hashes ahead of time, Today nobody uses rainbow tables anymore because computers are fast enough without them.

So the bad news is any user with a simple password like "password" or "password12345" or any of the billion most-likely passwords will have their password guessed, if you have an extremely complicated password (over 16 random numbers & letters) you were probably safe.

Also notice that the code above is effectively **attacking all of the passwords at the same time.** It doesn't matter if there are ten users in your database or ten million, it doesn't take the hacker any longer to guess a matching password, All matters is that how fast the hacker can iterate through potential password, (And in fact, having lots of user actually **help** the hackers. because it is more likely that someone in the system was using the password "password12345".)

sha1(password) which LinkedIn used to store its password, And in 2012 a large set of password hashes

were leaked, Over time hacker were able to figure out the plain text password to **most** of these hashes.

Summary: storing a simple hash (with no salt) is not secure - if a hacker gain access to your database, they will be able to figure out the majority of the passwords of the users.

### **Bad Solution : sha1(FIXED\_SALT + password)**

One attempt to make things more secure is to "salt" the password before hashing it:

<b>user account</b>	<b>sha1("salt123456789" + password)</b>
gunjan@hotmail.com	b467b644150eb350bbc1c8b44b21b08af99268aa
jassy@gmail.com	31aa70fd38fee6f1f8b3142942ba9613920dfea0
...	...

The salt is suppose to be a long random string of bytes, If the hacker gains access to these new password hashes (not the salt), will make it much more difficult for the hacker to guess the passwords because they would also require to know the salt, However if the hacker has broken into server, probably also have access to your source code as well so they'll learn the salt too, That is why security designers just assume the worst, & don't rely on the salt being secret.

But even if the salt is not a secret it still makes it harder to use those old-school **rainbow tables** mentioned before Those rainbow tables are built assuming there is no salt so salted hashes stop them. However since no one uses rainbow tables anymore adding a fixed salt does not help much, The hacker can still execute the same basic for-loop from above:

```
for password
inLIST_OF_COMMONPASSWORDS:
if sha1(SALT + password) in databasetable:
print "Yepieeee I win! guessed a password!",
password
```

Summary: adding a fixed salt still is not secure enough.

### **Bad Solution : sha1(PER\_USER\_SALT + password)**

The next step in security is to create a new column in database and store a different salt for each user, Salt is

randomly created when the user account is first created. (or when user changes their password).

<b>user account</b>	<b>salt</b>	<b>sha1(salt + password)</b>
gunjan@hotmail.com	2dc	1a74404cb136dd600 7fcc 41dbf694e5c2ec0e 7d15b42
jassy@gmail.com	afad	e33ab75f29a9cf3f70d3 b2f fd14a7f47cd752e 9c550
...	...	...

Authenticating the user is not much harder than before:

```
defis_password_correct(user, password_attempt):
return sha1(user["salt"] + password_attempt) ==
user["password_hash"]
```

By having a per-user-salt we get one huge benefit, the hacker cannot attack all of your user's passwords at the same time Instead his attack code has to try each user one by one:

```
for user in users:
PER_USER_SALT = user["salt"]
for password
inLIST_OF_COMMONPASSWORDS:
if sha1(PER_USER_SALT + password) in
databasetable:
```

```
print "yepiee I win! guessed a password!", password
```

So basically if you have 1 million users having a per-user-salt makes it 1 million times harder to figure out the passwords of *all* your users. But still is not impossible for a hacker to do this. Instead of 1 cpu-hour now they need 1 million cpu-hours which can easily be rented from Amazon for about forty thousand dollar.

The real problem with all the systems we have discussed so far is that hash functions like sha1 () (even sha256 ()) can be executed on passwords at a rate of hundred M+/sec (or even faster by using GPU) Even though hash functions were designed with security in mind they were also designed so they would be fast when executed on longer inputs like entire files. These hash functions were not designed to be used for password storage.

### **Good Solution: bcrypt (password)**

Instead there are a set of hash functions that were specifically designed for passwords. In addition to

being secure "one-way" hash functions they were also **designed to be slow**.

One example is Bcrypt, bcrypt() takes about hundred ms to compute which is about 10,000x slower than sha1(). Hundred ms is fast enough that the user won't notice when they login but slow enough that it becomes less feasible to execute against a long list of likely passwords, instance if hackers want to compute bcrypt() against a list of a billion likely passwords it will take about 30,000 cpu-hours about \$1200 and that is for a single password, not impossible but way more work than most hackers are willing to do.

Basically the trick is, it executes an internal encryption or hash function many times in a loop, there are other alternative to Bcrypt such as PBKDF2 uses the same trick.

Also Bcrypt is configurable with log\_rounds parameters that tells it how many times to execute that internal hash function, If all of a sudden Intel comes out with a new computer that is thosand times faster than the state of the art today, you can reconfigure your system to use a log\_rounds that is ten more than before (log\_rounds is logarithmic) which will cancel out the 1000x faster computer.

Because bcrypt() is too slow it makes the idea of rainbow tables attractive again so a per-user-salt is built into the Bcrypt system, In fact libraries like py-bcrypt store the salt in the same string as the password hash so you won't even have to create a separate database column for the salt.

Let us see the code in action, First let's install it:

```
wget "http://py-bcrypt.googlecode.com/files/py-
bcrypt-0.2.tar.gz"
tar -xzf py-bcrypt-0.2.tar.gz
cd py-bcrypt-0.2
python setup.py build
sudo python setup.py install
cd ..
python -c "import bcrypt"# did it work?
```

Now that it is installed, here is the Python code you'd run when creating a new user account (or reset their password):

```
from bcrypt import hashpw, gensalt
hashed = hashpw(plaintext_password, gensalt())
print hashed # save this value to the database for the
user
```

```
'$2a$12$8vxYfAWCXe0Hm4gNX
8nzwuqWNukOkcMJ1a9G2tD71ipotEZ9f80Vu'
```

Let us dissect that output string a little:

```
$2a$12$8vxYfAWCXe0Hm4gNX8nzwuqWNukOkcMJ1a9G2tD71ipotEZ9f80Vu
```

```
$bcrypt_id$log_rounds$128-bit-salt184-bit-hash
```

As you can see it stores both the salt, & the hashed output in the string, It also stores the log\_rounds parameter that was used to generate the password which controls how much work that is how slow it is in computation, If you want the hash to be slower you pass a larger value to gensalt():

```
hashed = hashpw(plaintext_password,
gensalt(log_rounds=14))
print hashed
'$2a$13$ZyprE5MRw2Q3WpNOGZW
GbeG7ADUre1Q8QO.uUUtcblqU0yvzavOm'
```

Notice that there is now a 14 where there was a 13 before, In any case you store this string in to the database, & when that same user attempts to log in you retrieve that same hashed value and do this:

```
if hashpw(password_attempt, hashed) == hashed:
print "matches"
else:
print "does not match"
```

You might be wondering why you pass in hashed as the salt argument to hashpw() The reason this works is that the hashpw() function is smart and can extract the salt from that \$2a\$13\$.... string This is great because it means you never have to store parse or handle any salt values yourself , the only value you need to deal with is that single hashed string which contains everything you need.

## References

1. OpenSSL: The open source toolkit for SSL/TLS.<http://www.openssl.org>.
2. Mart' n Abadi, T. Mark A. Lomas, and Roger Needham. Strengthening passwords. Technical Report 1997 - 033, 1997.
3. Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In EUROCRYPT, pages 139-155, 2000.

## Conclusion

Final Thoughts for choosing a good password If your user has the password "password" then no amount of hashing, salting, bcrypt etc is going to protect that user The hacker will always try simpler passwords first so if your password is toward the top of the list of likely passwords the hacker will probably guess it.

The best way to prevent password from being guessed is to create a password that is as far down the list of likely passwords as possible, Any password based on a dictionary word even if it has simple mutations like a letter/number at the end is going to be on the list of the first few million password guesses.

Unfortunately difficult-to-guess passwords are also difficult-to-remember, If that was not an issue I would suggest picking a password that is a 16 character random sequence of numbers and letters ,people have suggested using passphrases instead, like "shally is a police officer", your system allows long passwords with spaces then this is definitely better than a password like "shally123". (But I actually suspect the entropy of most user's pass phrases will end up being about the same as a password of eight random alphanumeric characters.)

## Acknowledgment

This research paper is made possible through the help and support from everyone, including teachers, family and friends.

4. E. Felten, D. Balfanz, D. Dean, and D. Wallach. Web spoofing: An Internet con game. Proc. 20th National Information Systems Security Conference, 1997.
5. Eran Gabber, Phillip B. Gibbons, Yossi Matias, and Alain J. Mayer. How to make personalized web browsing simple, secure, and anonymous. In Financial Cryptography, pages 17-32, 1997.
6. Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. In EUROCRYPT, pages 524-543, 2003.
7. J. Jeff, Y. Alan, B. Ross, and A. Alasdair. The memorability and security of passwords - some empirical results, 2000.
8. Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. The design and analysis of graphical passwords. 1999.
9. Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient password-authenticated key exchange using human-memorable passwords. In EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, pages 475-494. Springer-Verlag, 2001.
10. J. Kelsey, B. Schneier, C. Hall, and D. Wagner. Secure applications of low-entropy keys. Lecture Notes in Computer Science, 1396:121-134, 1998.
11. David P. Kormann and Aviel D. Rubin. Risks of the Passport single signon protocol. In Proc. 9th international World Wide Web conference on computer networks, pages 51-58. North-Holland Publishing Co., 2000.
12. U. Manber. A simple scheme to make passwords based on one-way functions much harder to crack, 1996.
13. Robert Morris and Ken Thompson. Password security: A case history. CACM, 22(11):594-597, 1979.
14. Blake Ross, Collin Jackson, Nicholas Miyake, Dan Boneh, and John C. Mitchell. A browser plug-in solution to the unique password problem, 2005. Technical report, Stanford-SecLab-TR-2005-1.
15. Bruce Schneier et al. Password Safe application. <http://www.schneier.com/passsafe.html>.
16. Joe Smith. Password Safe cracker utility.

# Security Issues in Bluetooth Technology - A Review

Menal Dr.\*  
Sumeet Gill\*\*

---

## Abstract

Bluetooth is a recently proposed standard for short range, low power wireless communication. Bluetooth Technology has become a popular way of wireless interconnection for exchanging messages, data and other information. Security concern is one of the most important problems behind the mass adoption of this technology. This paper provides a brief overview of security issues and weaknesses faced by the Bluetooth technology.

**Keywords:** Bluetooth technology, Bluetooth security, wireless communication

---

## Introduction

Now a days the use of mobile computing networking increases day by day. People use mobile communication technology more than any other technology. Mobile networking is a pervasive communication platform where users obtain the desired information in seconds and increase the efficiency of work. Smartphones have a number of connectivity features like Bluetooth, wi-fi, RFID etc. Currently Bluetooth is one of the most commonly uses wireless networking technology that quickly share information with each other at a speed of 1Mbps in basic mode within a 50 m range. Bluetooth is a short range, low power wireless communication technology, mostly integrated into mobiles and other devices. This technology combines the features of packet switching and circuit switching thereby supporting both connectionless and connection-oriented links. It was developed by Ericsson in 1994. The Bluetooth standard is managed and maintained by Bluetooth Special Interest Group. [1] IEEE has also adapted as the 802.15.1a standard. Bluetooth uses the unlicensed 2.4 GHz ISM (Industrial Scientific and Medical)

---

### Menal Dr.\*

Department of Computer Science  
Maharaja Surajmal Institute  
Janakpuri, New Delhi

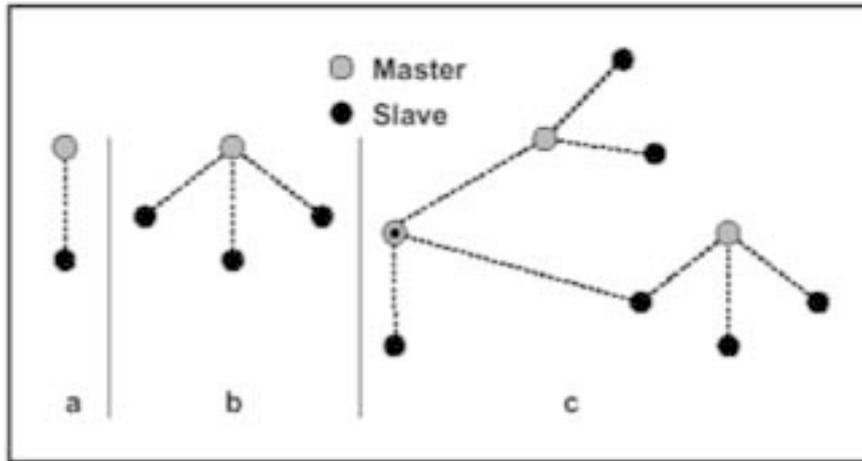
### Sumeet Gill\*\*

Department of Mathematics  
Maharashi Dayanand University  
Rohtak, Haryana

frequency band. Bluetooth operates on 79 channels in the 2.4 GHz band with 1MHz carrier spacing. To make the link robust to interference, it employs a Frequency Hopping technique, in which the carrier frequency is changed at every packet transmission. Like any other wireless technology Bluetooth uses open air medium for transferring data that makes it involved with the security issues. There are several authentication, access control and encryption algorithm that plays major role in the security of wireless technology. Some devices have biometric access control while others have strong password protected systems. But there is no standard access control technique that makes data secure over air.

Bluetooth supports both unicast and multicast connections. Bluetooth protocol uses the concept of master and slave. In a master slave protocol a device cannot talk as when they desire. They need to wait till the time the master allows them to talk. The master and slaves together form a *piconet*. Up to seven "slave" devices can be set to communicate with a "master". Several of these piconets can be linked together to form a larger network in an ad hoc manner. The topology can be thought as a flexible, multiple piconet structure. This network of piconets is called *scatternet*. Figure 1 shows the basic piconet topologies. A scatternet is formed when a device from one piconet also acts as a member of another piconet. In this scheme, a device being master in one piconet can simultaneously be a slave in the other one. [2]

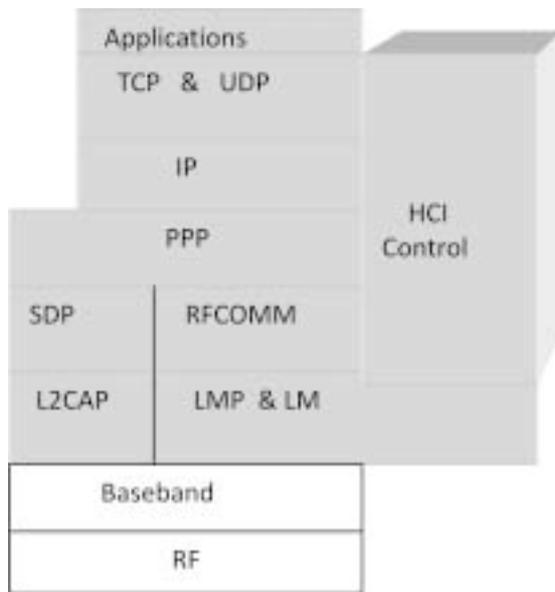
This paper is organized as follows. Section I describes the features of Bluetooth technology. Section



**Fig.1 Piconets with master slave operations**

It explains the Bluetooth architecture and protocols. In Section III, we discuss the security issues and challenges involved in Bluetooth technology. Section IV concludes the paper.

**BLUETOOTH ARCHITECTURE AND PROTOCOLS**



**Fig. 2 Bluetooth Architecture**

**Personal Networking Hardware and the Protocol Stack Layers:**

**The Bluetooth Baseband Layer:** The baseband layer performs functions like Bluetooth packet assembly, forward error correction (FEC), automatic repeat request (ARQ), data whitening, Bluetooth

clock synchronization, and frequency hopping control.

**The Bluetooth Link Manager Layer:** The Link Manager forms the piconet by inquiring what other Bluetooth radios are in the area, establishing connection and maintaining the piconet. The Link Manager also handles security issues like authentication and encryption.

**Radio:** The Radio layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.

**Baseband:** This layer describes the specification of the Bluetooth Link Controller (LC) which carries out the baseband protocols and other low-level link routines. The Link Manager Protocol (LMP) is used by the Link Managers (on either side) for link set-up and control. The Host Controller Interface (HCI) provides a command interface to the Baseband Link Controller and Link Manager, and access to hardware status and control registers.

**Logical Link Control and Adaption Protocol (L2CAP)**

Supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information. L2CAP, which adapts upper layer protocols over the baseband, provides data services to the high layer protocols with group abstractions. The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol.

The protocol is based on the ETSI standard TS 07.10. The Service Discovery Protocol (SDP) provides a means for applications to discover which services are provided by or available through a Bluetooth device. Device information, services and the characteristics of the services can be queried using the SDP [2]. Fig 2 shows Bluetooth architecture

### **Bluetooth Security Issues**

Attack to a wireless network is easier because information is zapping back and forth through the open air. In a wireless environment where every bit is on the air, security concerns are high. Security can be defined by three fundamental elements[4]:

*Authentication:* This service is used for verifying the identity of the communicating devices before being able to connect to the application. Native user authentication does not provided by the Bluetooth.

*Authorization:* This service allows the resources which are connected to Bluetooth for transmitting the data after an authorization procedure. Only the trusted devices allow to do so.

*Confidentiality:* This service ensures that only the authorized devices can share the application and then prevent from all kinds of eavesdropping.

Bluetooth does not address other security services such as audit, integrity, and non-repudiation.

### **Bluetooth Security Modes**

Cumulatively, the BT versions up to 2.1 define four modes of security. Each of these versions supports some of these modes but none of them supports all four.

#### **Security Mode 1**

This mode is non-secure. It has the lowest security level. Mode 1 is only supported in earlier versions.

#### **Security Mode 2 (Service-level Enforced)**

Mode 2 is designed as a *service-level enforced security-mode*. In this mode communication is initiated after the establishment of the channel at L2CAP level. Security Mode 2 is supported by all Bluetooth devices.

#### **Security Mode 3 (Link-level Enforced)**

Mode 3 is designed as a *link-level enforced security-mode*. Here, all security measures take place before the communication link is fully established. Security Mode 3 is only supported in earlier devices.

#### **Security Mode 4 (Service-level Enforced)**

Similar to security Mode 2, this mode is enforced on the service level, after the physical link has been established.

### **Bluetooth Trust and Service Levels**

In addition to the four security modes, two *trust levels* and three *service security levels* are provided in the Bluetooth. Two trust levels are *trusted* and *untrusted*. Devices which falls under trusted level have full permission to access all services provided by the connected devices while untrusted devices restricted for limited access.

For achieving authentication, encryption and authorization the three security levels are allowed to be defined . Available Service Security Levels depend on the security mode being used.

### **Bluetooth Service Security Levels:**

#### **Service Level 1**

Trusted devices are allowed to connect automatically to all services after the completion of authentication and authorization. Untrusted devices need manual authorization for all services.

#### **Service Level 2**

At this level only authentication requires. After the authentication procedure service is accessed by the device.

#### **Service Level 3**

This service is open to all devices i.e. access is granted automatically with no authentication required.

Trust and service levels allow the definition of policies to set trust relationships and may also be used to initiate user-based authentication. Bluetooth core protocols usually only provide device authentication. [3]

### **Analysis of Security Issues**

As technology grows day by day new attacks are also being developed by the attackers. The weakness of the basic Bluetooth protocols involves the pairing process,

**Table-1: Key Issues with Bluetooth Security**

Security Issues	Description
Initialization key is too weak	Generate new initialization key scheme
PIN key is too short and default is all zero	Increase the length of PIN code
The master key used for broadcast encryption is shared among all piconet devices	Change broadcast scheme
Weak $E_0$ stream cipher	Replace the cipher with new advance technique
No user authentication	Application level security and employ user authentication
Encryption key length is negotiable encryption	Program each device to initiate 128 bit Bluetooth immediate after manual authentication
End to end security is not performed	End to end security can be provided by use of additional security controls
Security services are limited	Bluetooth does not address audit, integrity, and non-repudiation; if such services are needed, they should be provided through additional means.
The quality of pseudorandom number generators are not known	Bluetooth should use strong PRNGs based on standards
Unit keys are reusable and static for every pairing	Device uses same unit keys and link leys. This should be avoided using strong cryptographic management
Link keys can be stored improperly	Link keys can be modified if they are not securely stored

device address scheme and its wireless nature. Along with weaknesses, the Bluetooth specifications have several design issues also like how to decide which node become master, slave and bridges in a piconet, how many piconets a node should join and many others.

Table 1 provides an overview of some of the known security issues or vulnerabilities [5].

## Conclusion

This paper was intended as a brief introduction to Bluetooth technology. It is one of the technologies that can be used for ad hoc networking and it uses widely among people due to its key features that includes robustness, low complexity, low power,

and low cost. Since it is a wireless networking communication technology, so security is always a prior issue. This technology is still in research phase due to the security problems.

Bluetooth is by design a peer to peer network technology and typically lacks centralized administration and security enforcement infrastructure. The Bluetooth specification is very complex and includes support for dozens of data services. Because of these complexities and outside interconnection access, high level of security mechanism should be enforced. Various security issues that raises here can be reduced at a certain level using upcoming technologies. The future work would be focused on the improvement in the security schemes.

## References

1. The official Bluetooth technology info site, <http://www.bluetooth.com>.
2. Talukder A, Ahmed H, Yavagal R R, *Mobile Computing*, 2<sup>nd</sup> edition. McGraw-Hill, 2013, pp 84-90.
3. K. Scarfone and J. Padgett. \Guide to bluetooth security,\". Tech. Rep., 2008.
4. T. C. Yeh, J. R. Peng, S. S. Wang, and J. P. Hsu, \Securing bluetooth communications,\" *International Journal of Network Security*, vol. 14, no. 4, pp. 229-235, 2012.
5. Padgett J., Scarfone K., Chen L. \"Guide to Bluetooth security\" NIST Special Publication 800-121, June 2012.
6. Mandal B., Bhattacharyya D., Kim T., \"A Design Approach for Wireless Communication Security in Bluetooth Network\" Vol.8, No.2(2014), pp. 341-352, *\"International Journal of Security and its Application\"*

# Detection of Terrorism Activities Using Face Recognition Technique

Garima Bhatia\*  
Mansi\*\*

---

## Abstract

With the rapid development in the field of pattern recognition and its uses in different areas (e.g. signature recognition, facial recognition), arises the importance of the utilization of this technology in different areas in large organizations. Biometric recognition has the potential to become an irreplaceable part of many identification systems used for evaluating the performance of those people working within the organization. This research attempts to provide a system that recognizes terrorist using face recognition technology to record their presence in over populated areas by matching their faces already stored in a database according to previous criminal records. For face recognition we will be using technique known as PCA.

**Keywords:** Face recognition system, authentication, bio-metric, PCA.

---

## Introduction

Face recognition is an important branch of biometric and has been widely used in many applications, such as human-computer interaction, video monitor system and door control system and network security [4].

For detection, color based technique was implemented, which depends on the detection of the human skin color with all its different variations in the image.

For recognition, PCA technique has been implemented which a statistical approach that deals with pure mathematical matrixes not image processing like the color based technique used for detection. PCA can also be used for detection.

In general Face recognition system can help in many ways:

Checking for criminal records. Enhancement of security by using surveillance cameras.

Searching lost children's by using the images received from the cameras fitted at some public places.

Knowing in advance if some VIP or someone known is entering the hotel. Detection of a criminal at public place. Pattern recognition [18].

---

## Garima Bhatia\*

MCA Student, MERI, GGSIPU

## Mansi\*\*

MCA Student, MERI, GGSIPU

## Biometric Recognition:

There are three different types of authentication: something you know, such as passwords, something you have, such as badges or cards, and finally something you are, which mainly depends on biometrics and physical traits. Each of these three authentication methods has its advantages and disadvantages, and each is considered appropriate for certain types of application [8].

Among these three types, scientists and researchers consider biometric recognition systems as high-level security systems. Biometrics is used in computer science as a form of access control and identification. It is also used to identify individuals in groups that are under surveillance.

**Eye:** Analyzing the eye is generally thought to present the highest levels of accuracy and uniqueness. They can be divided into two different technologies: iris biometrics and retina biometrics [8].

## Iris:

It is the colored tissue representing the ring surrounding the eye pupil. Each person's iris has a unique structure and a complex pattern. In addition, it is believed that artificially duplicating an iris is virtually impossible. It is also known that the iris is from the first body parts decaying after death, therefore



Figure: 1 [18]

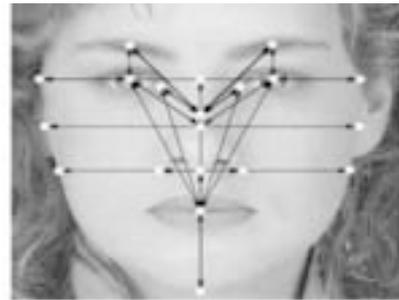


Figure: 2 [18]

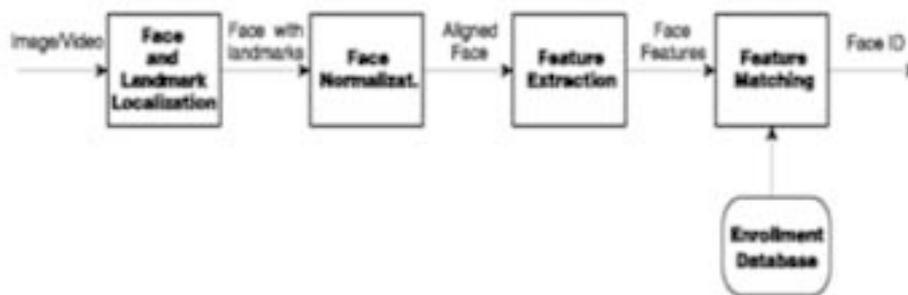


Figure: 3[18]

it is unlikely that a dead iris could be used to by-pass a biometric system.

#### Retina:

Retina is the layer of blood vessels which is situated at the back of eye. Retina used to form a non-identical pattern and decays quickly after death. Retina recognition systems are complex but at the same time regarded as the most secure biometric system.

**Face:** For a computerized system to mimic the human ability in recognizing faces, sophisticated and complex artificial intelligence and machine learning is needed to be able to compare and match human faces with different poses, facial hair, glasses, etc. That is why these systems depend greatly on the extraction and comparison engines. Different tools maybe used in these systems such as standard video, or still imaging.

#### Facial Recognition

Face recognition is considered to be one of the most successful applications of image analysis and processing; that is the main reason behind the great attention it has been given in the past several years [4].

The facial recognition process can be divided into two main stages: processing before detection where face detection and alignment take place (localization and normalization), and afterwards recognition occur

through feature extraction and matching steps as shown in figure above [9].

#### a. Face Detection:

This process separates the facial area from the rest of the background image. In the case of video streams, faces can be tracked using a face tracking component.

#### b. Face Alignment:

This process focus on finding the best localization and normalization of the face; where the detection step roughly estimates the position of the face, this step outlines the facial components, such as face outline, eyes, nose, ears and mouth. Afterwards normalization with respect to geometrical transforms such as size and pose, in addition to photometrical properties such as illumination and grey scale take place.

#### c. Feature Extraction:

After the previous two steps, feature extraction is performed resulting extracting the in effective information and essential information that is useful for distinguishing between faces of different persons.

#### d. Face Matching:

The extracted features are compared to those stored in the database, and decisions are made according to the sufficient confidence in the match score.

**Facial Recognition Techniques:** That is applied to frontal face:

#### A. Eigen faces:

**Eigenfaces** is the name given to a set of eigenvectors which are used in the computer problem for vision of human face recognition.

#### B. Geometrical Feature Matching:

Geometrical feature matching techniques are based on set of geometrical features from the picture of a face. Current automated face feature location algorithms do not provide a high degree of accuracy and require considerable computational time.

#### C. Template Matching:

A simple version of template matching is that a test image represented as a two-dimensional array of intensity values is compared using a suitable metric, such as the Euclidean distance, with a single template representing the whole face. In general, template-based approaches compared to feature matching are a more logical approach.

**Limitations and Challenges of Face Recognition Technologies:** As mentioned earlier, face recognition technology, just as any other biometric technology, has not yet delivered its promise. In spite of all its potentials, it is still quite limited in its applied scope. Many researchers have identified different problems for the biometric system; they can be categorized as follows: [8]

**1. Accuracy:** Two biometric samples collected from the same person are not exactly the same due to the



Figure:4[8]

imperfect imaging conditions. In addition, the face recognition technology is not robust enough to handle uncontrolled and unconstrained environments. In consequence, the results accuracy is not acceptable.

#### Errors in Accuracy

Errors are mainly caused by the complexity and difficulties of the recognition process because of the uncontrollable variables such as lighting, pose, expression, aging, weight gain or loss, hairstyle and accessories [1]. Figures shown below (4,5,6) depicts the errors caused by either pose variation or ageing as a factor or hiding of images [18].

**2. Security:** Facial recognition and other biometric systems are used for many security applications, claiming that biometrics is a secure way of authenticating access. But in fact, security of biometrics (especially face), is very questionable. This is caused by two main reasons:

- a. Biometrics is not a secret: This means that anyone including the attacker knows exactly the biometric features of the targeted user.
- b. Biometrics is not recoverable: This means that one cannot change his face in case it became compromised [18].

#### Implementation

For detection, Color based technique was implemented, which depends on the detection of the human skin color with all its different variations in the image. The skin area of the image is then segmented and passed to the recognition process.



Figure:5[18]



Figure: 6[18]

For recognition, PCA technique has been implemented which is a statistical approach that deals with pure mathematical matrices not image processing like the color based technique used for detection. PCA can also be used for detection [9].

### PCA (Principal Component Analysis)

**Description:** Based on an information theory approach, PCA is used to breakdown face images into a small set of characteristic features images or modules called "Eigenfaces" that can be described as the principal components of the initial training set of images.

In PCA, one can change each original image of the training set into a corresponding eigenface. Therefore, one important feature of PCA is that the reformation of any original image from the training set by combining the eigenfaces is possible. Eigenfaces are the unique features of the faces. Therefore one could say that the original face image can be reconstructed from eigenfaces if one adds up all the features in the right proportion. Each eigenface represents only certain features of the face, which may or may not be present in the original image. If the feature is present in the original image to a higher degree, the share of the corresponding eigenface in the sum of the eigenfaces should be greater. On the other hand if the particular feature is not present in the original image, the corresponding eigenface should contribute a smaller part to the sum of eigenfaces. Indeed, in order to reconstruct the original image from the eigenfaces, one has to build a kind of weighted sum of all the eigenfaces. That is, the reconstructed original image is equal to a sum of all eigenfaces, with each eigenface having a certain weight. This weight specifies, to what degree the specific features (eigenface) is present in the original image. If all the eigenfaces extracted from the original images are used, one can reconstruct the original images from the eigenfaces exactly. But using only a part of the eigenfaces is applicable. Hence, the reconstructed image is an approximation of the original image [7].

However, losses due to omitting some of the eigenfaces can be minimized, which is achieved by selecting only the most important features (eigenfaces).

Moreover, it is possible not only to extract the face from eigenfaces given a set of weights, but to extract the weights from eigenfaces and the face to be recognized. These weights act as the amount by which the face differs from the "typical" face represented by the eigenfaces.

Therefore, using these weights one can determine two important things:

1. Check whether the image is a face. In the case the weights of the image differ too much from the weights of face images, the image probably not a face.
2. Similar faces (images) possess similar features (eigenfaces) to similar degrees (weights). If weights from all images available is extracted, the images could be grouped to clusters. Thus, all images having similar weights are likely to be similar face.

**PCA-based face recognition algorithm:** The approach to PCA-based face recognition involved the following initialization operations: [7]

**Initialization:** Acquire an initial set of face images (the training set). Calculate the eigenfaces from the training set, keeping only the M images that correspond to the highest eigenvalues. These M images define the face space. As new faces are experienced, the eigenvalues can be updated or recalculated. Calculate the corresponding distribution in M-dimensional weight space for each known individual, by projecting their face images onto the face space. Having initialized the system, the following steps are used to recognize new faces: Calculate a set of weights based on the input image and the M eigenfaces by projecting the input image onto each of the eigenfaces. Determine if the image is a face at all (whether known or unknown) by checking to see if the image is sufficiently close to the face space. If it is a face, classify the weight pattern as either a known person or as unknown. The coming sections will elaborate the steps needed to perform the PCA using eigenfaces on a set of images in detail [6, 7].

**Main Algorithm phases:** The previous initialization processes can be summed up into three main phases [6, 7].

Three main functional units are involved in these phases. The characteristics of these phases are described below:

**Face database formation phase:** During this phase, the gathering and the preprocessing of the face images that are going to be added to the face database are performed. Face images are stored in a face library (file system) in the system. Every action such as training set or eigenface formation is performed on this face library. In order to start the face recognition process, the face library has to be filled with face images. Weight vectors of the face library members are empty until a training set is chosen and eigenvectors are formed.

**Training phase:** Images that are going to be in the training set are chosen from the entire face library. After choosing the training set, eigenfaces are formed and stored for later calculations. Eigenfaces are calculated from the training set, keeping only the  $M$  images that correspond to the highest eigenvalues. These  $M$  eigenfaces define the  $M$ -dimensional face space. When the new faces are acknowledged, the eigenfaces can be updated or recalculated. The corresponding weight vector of each face library member has now been updated. **Note:** Once a training set has been chosen, it is not possible to add new members to the face library with the established method that is presented in the “face database formation phase” because the system does not know whether this item already exists in the face library or not. Therefore, a library search must be performed.

### Recognition and learning phase:

After choosing a training set and constructing the weight vectors of face library members, now the system is ready to perform the recognition process. The recognition process is initialized by choosing the input image (the image, one seeks to recognize). The weight vector is constructed with the aid of the eigenfaces that were already stored during the training phase. After obtaining the weight

vector, it is compared with the weight vector of every face library member with a user defined “threshold”. If there exists at least one face library member that is similar to the acquired image within that threshold then, the face image is classified as known”. Otherwise,

a miss has occurred and the face image with its corresponding weight vector for later use. This process is called learning to recognize.

### Eigenvectors and eigenvalues definitions

An eigenvector of a matrix is a vector such that, if multiplied with the matrix, the result is always an integer multiple of that vector. Its direction is not changed by that transformation. This integer value is the corresponding eigenvalue of the eigenvector. The corresponding eigenvalue is the proportion by which an eigenvector’s magnitude is changed. This relationship can be described by the equation  $M * u = \lambda * u$ , where  $u$  is an eigenvector of the matrix  $M$  and  $\lambda$  is the corresponding eigenvalue. This means, an eigenvalue of 2 means that the length of the eigenvector has been doubled. An eigenvalue of 1 means that the length of the eigenvector stays the same. Eigenvectors possess following properties:

- They can be determined only for square matrices.
- There are  $n$  eigenvectors (and corresponding eigenvalues) in an  $n * n$  matrix.

All the eigenvectors are perpendicular, i.e. at right angle with each other [7].

### The Use of Eigenfaces for Recognition:

**Overview of the algorithm using eigenfaces:** The algorithm for the facial recognition system using eigenfaces is basically described in Fig. First, the original images of the training set are transformed into a set of eigenfaces  $E$ . Afterwards; the weights are calculated for each image of the training set and stored in the set  $W$ . When observing an unknown image  $X$ , the weights are calculated for that particular image and stored in the vector  $W_x$ . Afterwards, it is compared with the weights of images, of which one knows for certain that they are faces (the weights of the training set  $W$ ). One way to do it would be to regard each weight vector as a point in space and calculate an average distance  $D$  between the weight vectors from and the weight vector of the unknown image (the Euclidean distance described in the appendix B would be a measure for that). If this average distance exceeds some threshold value, then the weight vector of the unknown image lies too far apart from the weights of

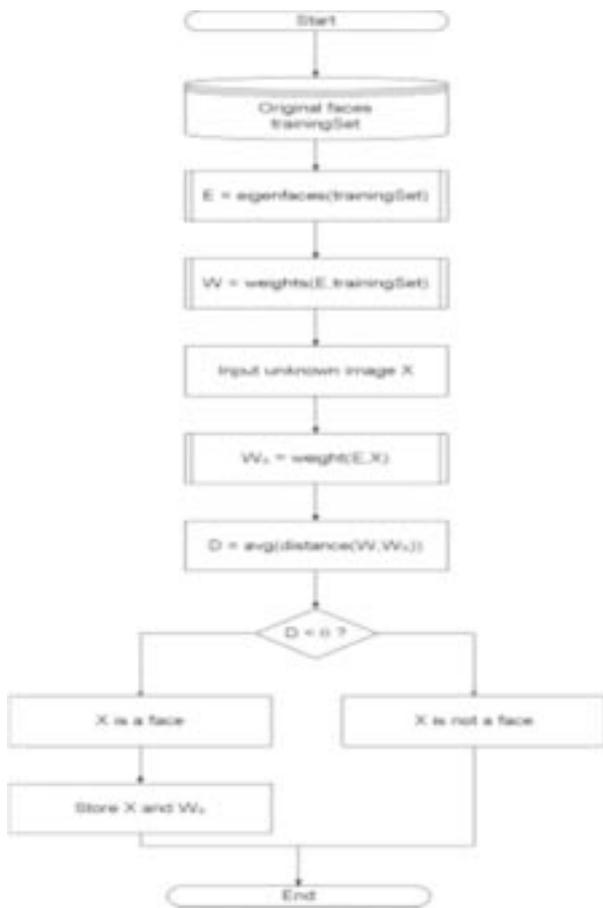


Figure:7[7]

the faces. In this case, the unknown X is considered not a face. Otherwise (if X is actually a face), its weight vector is stored for later classification [7].

**Problems faced:** Calculating the average and weights of the faces takes so much processing and time when run for the first time to run the program.

**Limitations:** Non-uniform backgrounds and lighting conditions affect the recognition process.

**Recommendation:**

- Using black or uniform background used in the image.
- Use sufficient light to illuminate the scene

**Computation step:**

We make use of Eigenvectors and Eigenvalues for face recognition with PCA [7].

**Step 1:** we prepare an initial set of face images [X1, X2, ...,Xn].

**Step 2:** The average face of the whole face distribution is

$$X = (X1 + X2 + \dots + Xn )/n$$

**Step 3:**Then the average face is subtracted from each face,

$$Xi' = Xi - X, i = 1, 2, \dots , n$$

**Step 4:** calculation of eigenvectors

[Y1, Y2, ...,Yn] eigenvectors are calculated from the new image set [X1', X2', ... Xn'].

These eigenvectors are orthonormal to each other.

**Step 5:** Starting with a preprocessed image I(x, y), which is a two dimensional N by N array of intensity values. This may be considered a vector of dimension. A database of M images can therefore map to a collection of points in this high dimensional “face space” as G1, G2, G3.....GM. With the average face of the image set defined as

$$y = \frac{1}{m} \sum_{n=0}^m G_n \tag{1}$$

Each face can be mean normalized and be represented as deviations from the average face by  $i=G_i - y$ . The covariance matrix, defined as the expected value of can be calculated by the equation

$$C = \frac{1}{m} \sum_{i=0}^m i^2 \tag{2}$$

Set of very large vectors is subject to PCA, which seeks a set of M ortho-normal vectors, which best describes the distribution of the data.

The kth vector, is chosen such that

$$= 1/m \text{ pow } 2 \tag{3}$$

Is a maximum, subject to  $= \{ 1 \text{ if } i=j, 0 \text{ if } i \neq j \}$

Given the covariance matrix C, we can now proceed with determining the eigenvectors and eigenvalues of C in order to obtain the optimal set of principal components, a set of eigenfaces that characterize the variations between face images [7].

$$C = 1/m = A$$

Where the matrix  $A = [\emptyset_1, \emptyset_2, \emptyset_3 \dots \emptyset_M]$

Following the matrix analysis, the  $M * M$  matrix  $L=A$  is constructed, where

$=$ , and the M eigenvectors, of L is computed. These vectors

determine linear combinations of the  $M$  training set face images to form the eigenfaces.

$= , I = 1, \dots, m$

The success of this algorithm is based on the evaluation of the eigenvalues and the eigenvectors of the real symmetric matrix  $L$  that is composed from the training set of images. After this step, the "training" phase of the algorithm is accomplished.

### Classifying Images:

#### Classifying an image with eigenfaces

A new face image ( $G$ ) is transformed into its eigenface components (projected onto "face space")

$= (G -)$

For  $k = 1, \dots,$

The weights form a feature vector,

$= []$

The face classes  $W_i$  can be calculated by taking the average of the results of the eigenface representation over a small number of face images (as few as one) of each individual. Classification is performed by comparing the feature vectors of the face library members with the feature vector of the input face image. This comparison is based on the Euclidean distance between the two members to be smaller than a user defined threshold. If the comparison falls within the user defined threshold, then face image is classified as "known", otherwise it is classified as "unknown" and can be added to face library with its feature vector

for later use, thus making the system learning to recognize new face images [7].

### Output

The output of our system will consist of the face ID with the closest match, as well as a value representing how close this match is (a distance value).

### Conclusions and Future work

In order to obtain the presence of terrorist or any unwanted activity in the over populated areas or the targeted areas, this project is imposed to identify the criminals by matching their face with the faces stored in the database. The database comprise of the criminal images that is the images of those having any back record. The database can be updated to add new faces. It can be done at regular intervals or within particular timestamp.

This research aims at providing the system to automatically detect or match the face with the faces stored in the database. In case a match is found, immediate action can be taken and the unwanted attack can be resolved frequently.

In further work, our system can be used in a completely new dimension of face recognition application, automated attendance system using face recognition technique.

The efficiency and the effectiveness of the project can also be improved by using high quality surveillance cameras to achieve more clear vision or images. So as to make the process of identification could be easier and faster.

### References

1. X-Zhang, YGao –Pattern Recognition, 2009- Elsevier
2. M. A. Turk and A. P. Pentland, "Face Recognition Using Eigenfaces," in Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 586–591. 1991.
3. J. Zhu and Y. L. Yu, "Face Recognition with Eigenfaces," IEEE International Conference on Industrial Technology, pp. 434 -438, Dec. 1994
4. Li, S.Z., Jain, A.K. (2004). Handbook of face recognition, New York, USA.
5. Hyconjaan moon, P Jonathan Phillips, "computational and performance aspects of PCA based face recognition algorithms", 2001, volume 30, pp 303-321
6. Ni, Mrin, As, Dwi, "Study of implementing automated attendance system using face Recognition technique", July 2012

7. Seth Jai Prakash, "Face Recognition Using Eigen vectors from PCA "
8. Maytas V, Riha, Z. Biometric Authentication- Security and Usability. Faculty of Informatics, Masaryk University Brno, Czech Republic
9. Y. Cui, J. S. Jin, S. Luo, M. Park, and S. S. L. Au, "Automated Pattern Recognition and Defect Inspection System," in proc. 5<sup>th</sup> International Conference on Computer Vision and Graphical Image, vol. 59, pp. 768 – 773, May 1992
10. M. Turk and A. Pentland, "Eigenfaces for Recognition," Journal of Cognitive Neuroscience, Vol. 3, No. 1, pp. 71-86. Mar. 1991.
11. "Average Face," Boston University Computer Help Desk, Oct. 16, 2001.
12. Algorithm for Efficient Attendance Management: Face Recognition based approach, Vol. 9, Issue 4, No 1, and July 2012www.IJCSI.org
13. Automated Facial Recognition Attendance System Supervised By: Dr.GhassanIssa, January / 2011
14. P. Sinha, B. Balas, Y. Ostrovsky, and R. Russell, "Face Recognition by Humans: Nineteen Results All Computer Vision Researchers Should Know About," in Proceedings of the IEEE, vol. 94, Issue 11, 2006.
15. R. Cendrillon, "Real Time Face Recognition using Eigenfaces", undergraduate thesis, Univ. of Queensland, Dept. of Computer Science and Electrical Engineering,1999.
16. L. H. Xuan and S. Nitsuwat, 2007, "Face Recognition In Video, A Combination Of EigenFace And Adaptive Skin-Color Model", Proc. International Conference on Intelligent and Advanced Systems 2007, pp.742-747, Kuala Lumpur, Malaysia.
17. X. Zhang, J. Jiang, Z. Liang, and C. Liu, 2010, "Skin Color Enhancement Based on Favorite Skin Color in HSV Color Space", IEEE Transactions on Consumer Electronics, Vol. 56.
18. <http://en.wikipedia.org/wiki/Biometrics>

# Cloud Security: A Concerning Issue

Apurva Aggarwal\*  
Shalini Sharma\*\*

---

## Abstract

Cloud computing is defined as an architecture which provides computing services by the use of internet on demand and we pay per use on having the access to a pool of shared resources like storage, servers, applications, services and networks and there is no need to physically possess them. So by this the time of the organizations and the cost for managing can be saved. The organizations and some of the industries like education, healthcare and banking are shifting towards the cloud as the services which are offered by the pay-per-use pattern which are based on the resources such as bandwidth consumed, amount of data transferred, processing power or the amount of storage space occupied etc are more efficient. Cloud services are delivered by data centres which are located all over the world. Cloud computing is a totally internet dependent technology in which the client data is stored and is maintained in the data centres of the cloud provider like Amazon, Google and Microsoft etc.

**Keywords:** quantum cryptography.

---

## Introduction

Cloud refers to a network or Internet. Or we can say in other words as something which is present at remote location is cloud. Cloud computing provide us a way to have access over the applications as utilities, over the Internet. Cloud computing provides the creation, configuration and customization of applications online. Cloud computing ease its consumers by giving them virtual resources by means of internet. The fast growth in field of “cloud computing” also gives rise to severe security concerns. Security issues persist for Open Systems and internet. Cloud computing has not been widely adopted due to lack of security. Cloud computing have security issues like data securing, examining and analysing the usage of cloud by the cloud computing vendors. Both Cloud service provider and the cloud service consumer needs to make sure that the cloud is secure from all the external threats so that the customer does not face any problem like data loss or theft of data. A possibility also exist where a malicious user can access the cloud by impersonating as a legitimate user, and thus infecting the entire cloud

and somehow affecting many customers who are sharing that infected cloud.[1]

## Models

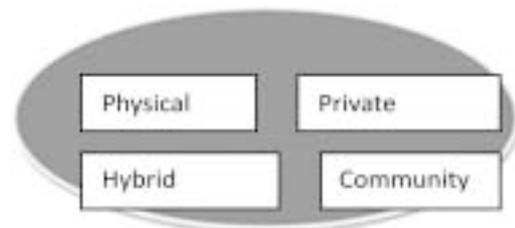
In cloud computing, the working models are deployment model and service model.

The type of access given to the cloud is defined by Deployment model. Different types of accesses that a cloud can have are: Private, Public, Hybrid, and Community.

**Private cloud:** Because of its private nature it offers more security. By the help of private cloud the system and the services are accessible within an organization.

**Community cloud:** The system and services are made to be accessible by the group of organizations.

**Public cloud:** System and services are made accessible to the general public. Its less secure as they are open that is free unrestricted access of the information.



**Figure 1: Different Accesses Given to Cloud**

---

Apurva Aggarwal\*

Management Education & Research Institute

Shalini Sharma\*\*

Management Education & Research Institute

**Hybrid cloud:** It is a mixture of public and private cloud. All the critical activities are carried out by using private cloud and all the non-critical by using public cloud.

**Service model:** The cloud computing is based are called as Service models. It can be categorized into three service models as:

- 1) IaaS- Infrastructure as a Service
- 2) PaaS-Platform as a Service
- 3) SaaS-Software as a Service

**Infrastructure as a Service (IaaS)** is the basic level of service. IaaS gives grant to fundamental resources like physical machines, virtual storage, etc.

**PaaS-**The runtime environment for applications, development and deployment tools are made available by PaaS.

**SaaS-**This model helps to have the Software applications being used as service to end users.

#### **Popular Services for Cloud Computing are:**

- **iCloud.** Apple's iCloud allows you to store music, documents, photos, and other files through Wi-Fi. And is accessible from any of your devices. By signing up for iCloud, you get 5GB of free storage automatically. For add on storage: \$20 per year for 10GB, \$40 per year for 20GB, and \$100 per year for 50GB. All the other Apple apps (calendar, mail, and more) are combined to work effortlessly with iCloud.
- **Google Cloud.** It includes sharing data and editing data of Word, PowerPoint, and Excel. You can have secured copies of each document which is saved. This plan can be terminated at any time, price at \$5 per user account per month, while the annual plan is priced at \$50 per user account per year.
- **IBMSmartCloud:** it provides many services for the companies in IT sector, such as applications developed in the cloud or using the cloud as a backup for the company data. Use the price estimation to estimate the cost for your particular needs – hence you need to therefore select the software, its size, and times that you want to use, and any additional requirements that your company might contain. A 12-month

commitment, for example, is at price \$1,300 per month for each unit. [2]

#### **Security Issues Cloud Computing:**

The security for cloud and non-cloud are almost similar. The Cloud Security Alliance's initial report contains a different sort of log based on different security domains and processes which are needed to be followed in general cloud operations. Some privacy and security-related issues that are believed to have long-term implication for cloud computing are:

##### **A. Governance**

Governance implies management and drop by the organization on procedures, standards and policies for application development and data technology service attainment, also because the style, execution, testing, use, and watching of deployed or engaged services.

##### **B. Compliance**

Compliance refers to an association's responsibility to work in the favor of established laws, provision and standards. One with all the common compliance problems facing a company is information location means storage of data or information [3].

##### **C. Malicious Insiders**

This threat is well known to most of the organizations. Insiders who are malicious they put an impact on the organization which is considerable. The nasty insiders are the threat which has access to the data or information about the organization who are the members. The application made for cloud consumers allows the data to be stored on cloud provided by cloud provider which also has the access to that data too.

##### **D. Account or service Hijacking**

The reason for this threat is due to spoofing, spuriousness and vulnerabilities in the software. In this way the criminal can get access to critical information stored on the cloud from where he can take permission and steal up the data, leading to the compromise on the availability, probity, and confidentiality to the services available.

##### **E. Hypervisor vulnerabilities**

The Hypervisor is the main software component of Virtualization. There known security susceptibility for

hypervisors and solutions are still limited to an extent and often proprietary.

**F. Insecure APIs**

Anonymous access, reusable tokens or password, clear-text attestation or transmission of content, inflexible access controls or improper authorizations, limited auditing, and classification capabilities etc security threats may occur to organizations if the weak set of interfaces and APIs are used.

**Our Recommendation**

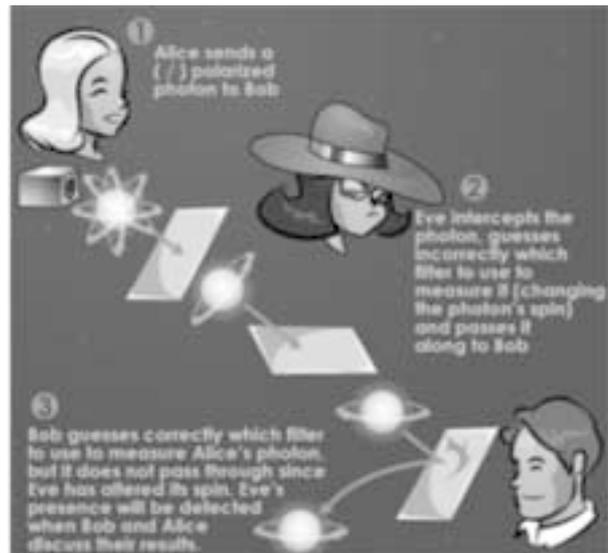
In this paper we will like to propose our ideas for future implementation:

The idea of “Quantum cryptography” should be applied to reduce challenges faced in security of data in cloud computing. Further research in this method’s application is still going on in China. We are still further working on this direction[4].

Some of the goals to provide data securism include three major points. namely: Availability, secrecy, and authenticity. Confidentiality of data in the cloud is obtained through cryptography.

**Quantum cryptography** can be considered for future implementation. But unlike, the traditional **cryptology** methods as encoding and decoding the information, Quantum cryptology depends on physics not on mathematics[5],[6].

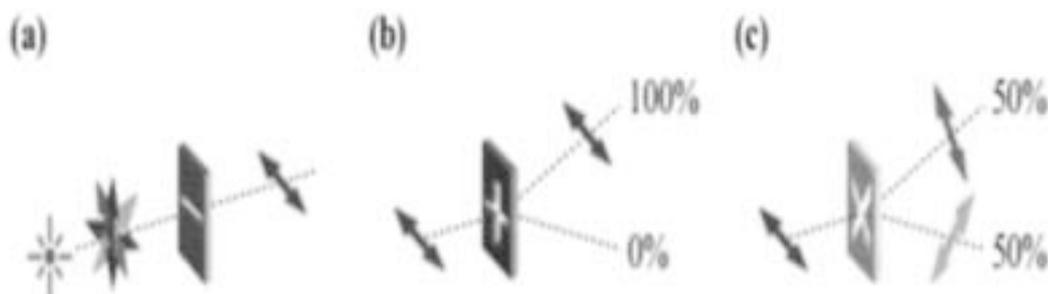
Quantum cryptography, a method used for transmitting a secret key over a distance which is secured and is based on the laws of physics. Quantum Key Distribution uses quantum mechanism to ensure secured communication[7]. It allows two parties to generate a random shared secret key which is known only to them and can be used to encrypt and decrypt



**Figure 2: example for detection**

the information. In quantum computing, a quantum bit is a unit of quantum information. The state of a qubit can be 0 and 1 simultaneously[8]. Explanation, consider a qubit be a single photon and see how it can be manipulated in the diagram below.

- (a) 1<sup>st</sup> a photon emitted from a light source and passes through a linear polarizer, horizontally. This creates a qubit with horizontal polarization.
- (b) When the photon which is polarized horizontally passes through a horizontal/vertical oriented beam splitter which is also polarised, then it always retains its horizontal polarization.
- (c) Suppose that photon which is horizontally polarized passes via diagonally oriented polarized beam splitter:
  - Approximately 50% of the photons could be found at one of the exiting.



**Figure 3: Manipulation of a Qubit**

- The photon can only be detected at one of the existing.
- The polarization of the photon will change as per the corresponding diagonal polarization. Then Polarized photons are able to communicate digital information [9].

### **Conclusion and Future Scope**

Modern cryptography algorithms are based on the fundamental process which includes finding factors of large integers into their primes, which is said to be

ineradicable. But modern cryptography is susceptible to both technological progress of computing power and development in mathematics to quickly reverse one-way functions such as that of factoring large integers. So the idea is to introduce quantum physics into cryptography, which has led to the evaluation of quantum cryptography. Quantum cryptography is one of the emerging topics in the field of IT industry. Hence quantum cryptography and how this technology contributes value to a defense-in-depth strategy related to completely secure key distribution is still in process.

### **References**

1. Swaroop S. Hulawale, Cloud Security Using Third Party Auditing and Encryption Service , 5 june, 2013
2. <http://talkincloud.com/>
3. <https://www.gov.uk/government/publications/implementing-the-cloud-security-principles/implementing-the-cloud-security-principles#audit-information-provision-to-consumers>
4. <http://searchsecurity.techtarget.com/definition/quantum-cryptography>
5. <https://sw.csiac.org/techs/abstract/520602>
6. <http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm>
7. <https://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf>
8. <http://www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986>
9. <http://www.wired.com/2013/06/quantum-cryptography-hack/>

# Hand Recognition System Design

Harleen Kaur\*

Simranjeet Kaur\*\*

---

## Abstract

In the field of Biometrics, attributes, for example, fingerprints, hand and face distinguishment and voice check utilized for personality confirmation are increasing higher worthiness rate. One of the biometric frameworks, hand distinguishment has been viewed as most suitable and adaptable for security application. Geometric estimations of the human hand have been utilized for personality verification as a part of a framework. This paper depicts a method for hand biometric peculiarity extraction utilizing hand form matching. Euclidian separation is gotten from beginning reference point and after that tip and valley purpose of finger is figured. At that point apply some scientific computation to compute the hand geometry gimmicks like finger length, width and border.

**Keywords:** hand geometry, feature extraction, mathematical calculation.

---

## Introduction

In today's reality biometric systems are picking up consideration. Physiological or behavioral attributes of the individual are ruined distinguishment. The physiological qualities infers utilizing human body parts for verification and behavioural attributes suggests activities utilizing body parts like voice, mark and stride and so on. The accompanying are a few gimmicks of biometric frameworks:

- Universality: which implies the trademark ought to be show in all people.
- Uniqueness: every individual have novel qualities.
- Permanence: its imperviousness to maturing.
- Measurability: that it is so natural to gain picture or sign from the single person.
- Performance: how great it is at perceiving and recognizing people.
- Acceptability: the populace must be ready to give the trademark.

In all cases there ought to be a database to store biometric gimmicks. The framework part is to contrast an information and all the entrances in the database

---

**Harleen Kaur\***

Management Education & Research Institute

**Simranjeet Kaur\*\***

Management Education & Research Institute

and check if there is a match, to affirm the personality of the single person. To think about any sort of biometric attributes its important to speak to them in a stable manner.

This is separated into two assignments:

1. Speak to a biometric trademark in reproducible and stable peculiarity such that oppose data variability.
2. Analyze such peculiarities so clients can precisely be recognized.

## Proposed system

The scanner is used to take image. The features are extracted by using image processing techniques and mathematical calculations.

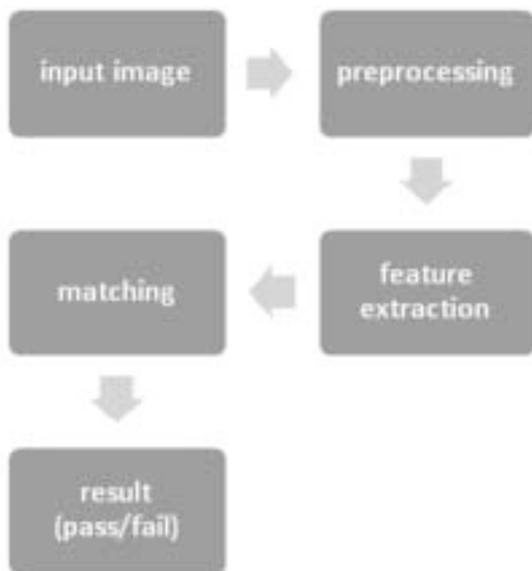
The palm print biometric system include following steps:

## Acquisition

Using scanner image is captured. The image taken is a colour image with no deformity providing easy, less-cost, non contact, effortless and user-friendly acquisition process. The hand's position is not fixed in this process. The image is taken in three different angles (90,180, -180), stored in jpeg format. In case finger is missing the system is unable to process the image.

## Pre-processing

The next step is Palm Print pre-processing. The image is prepared for feature extraction. At this stage colour



**Figure 1. System architecture**

image is transformed to gray level image then the noise pixels from the gray image is reduced.

### Edge detection

After elimination of noise the picture contains locales of highly contrasting pixels. It is obliged just edges are contained in picture to concentrate geometric gimmicks. Subsequently the areas of white space are obliged to change over to a picture containing the limit of the white pixels just. The edge identification calculation is utilized for this reason. The calculation changes over all pixels to dark pixels barring the one at the limit of highly contrasting. The calculation must guarantee that the thickness of this limit is as low as could reasonably be expected.

It is troublesome for edge identification calculation not to miss any edges. It is likewise critical that no non edges are recognized as edges. These two focuses characterize the lapse rate. There are likewise two different qualities that a decent edge discovery calculation ought to groups. The separation between the genuine edge and the edge found by the system ought to be as low as could be expected under the circumstances. Likewise the strategy ought not give various reactions to single edges.

### Algorithm

Step1: gradx and grady to be dead set, the qualities returned by the portions.



**Figure 2. Acquisition of palm print**

Step2: compute plot of the edge  $\theta = \tan^{-1}(\text{gradx}/\text{grady})$ .

Step3: theta approximated to one of these qualities 45, 90, 135 and 0 or 180.

Step4: Traverse along the edge toward the approximated theta and set any pixel to 0 which is not along theta.



**Figure 3. RGB color to gray color**

The estimate in Step 3 is fairly substantial. This is carried out on the grounds that since a pixel has just 8 encompassing pixel and the edge need to continue to one of these plot. An area including 45 degrees is shaped for each of the four plot 0, 45, 90 and 135. The theta quality lies in one of these locales and approximated to the edge in whose district it lies.

### Feature Extraction

This is the most important module in a biometric system which extracts the features of hand geometry. The features of hand print are calculated by using reference point: a) Tip point of all fingers including thumb. b) Starting and ending reference point c) hand centred d) length of major axis e) length of minor axis f) Perimeter

-1	0	+1
-2	0	+2
-1	0	+1

**Figure 4. The kernel to calculate the gradient along X axis**

+1	+2	+1
0	0	0
-1	-2	-1

**Figure 5. The kernel to calculate the gradient along Y axis**

### Matching

This is last step. The features extracted in the previous step are matched with the features of that individual stored previously in the database. The system produces a match score based on this comparison. The match score represents the closeness of the current image with the one in the database. A highest score represents a high closeness of the images. Based on experiments a threshold value is decided which lies in the range of match score. If the match score is less than the threshold value the image is rejected. If the match score is higher than the threshold the image in the database.

### References

1. Saraf Ashish - Design of Hand Geometry Based Recognition System Department of Computer Science & Engineering Indian Institute of Technology Kanpur in Jan 2007.
2. Arun Ross A.K.Jain and S.Pankati. A prototype hand- geometry based veri\_cation system. Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), pages 166{171, March 1999.
3. A. K. Jain and N. Duta. Deformable matching of hand shapes for veri\_cation. International Conference on Image Processing, pages 857{861, October 1999.
4. L. Wong and P. Shi. Peg-free hand geometry recognition using hierarchical geometry and shape matching. IAPR Workshop on Machine Vision Applications, pages 281{284, 2002.
5. Mongkon Sakdanupab and Nongluk Covavisaruch, A Fast and Efficient Palmprint Identification.



**Figure 6. Feature extraction**

### Experiments and results

The 50 clients are included in trials. From every client six picture of hand is taken, three from left and three from right hand. It is utilized for the enrolment procedure to characterize the clients' layouts, or peculiarity vectors. The peculiarities are separated and therefore match the database.

### Conclusion

The Hand geometry has proved to be a reliable biometric. The proposed system shows how features are extract using very simple mathematical formulas. We are attempting to improve the performance of hand geometry based verification system by reducing the amount of features and incorporating new features. Further we can develop a multi model biometric system to improve the efficiency of the system.

6. google references
7. Gnanou Florence Sudha, M. Niveditha, K. Srinandhini, and S. Narmadha Hand Based Biometric Recognition Based on Zernike Moments and Log Gabor Filters, International Journal of Research and Reviews in Information Sciences (IJRRIS).
8. Kostunica B. Ray, Rachita Misra: Palmprint as a Biometric Identifier, on IJECT Vol. 2.
9. A. Kirthika and S. Arumugam: TEXTURE AND COLOR INTENSIVE BIOMETRIC MULTIMODAL SECURITY USING HAND GEOMETRY AND PALM PRINT in International Journal of Advances in Engineering & Technology.
10. Arun Ross on A Prototype Hand Geometry-based Verification System.
11. Sarat C. Dass, Yongfang Zhu, Anil K. Jain: Validating a Biometric Authentication System: Sample Size Requirements in IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE.
12. Anil K. Jain, Arun Ross, and Sharath Pankanti: Biometrics: A Tool for Information Security on IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.
13. Karthik Nandakumar, Anil K. Jain and Arun Ross: Fusion in Multibiometric Identification Systems: What about the Missing Data.

# Infrared Thermal Imaging

Amit Sharma\*

Nidhi Jindal\*\*

---

## Abstract

Infrared Thermography (IRT) is being used in an ever more broad number of application fields and for many different purposes; indeed, any process, which is temperature dependent, may benefit from the use of an infrared device.

All living objects in the world emit infrared energy in the form of heat which is known as its heat signature.

Infrared thermal imaging is a method to improving visibility of objects by detecting the objects infrared radiation and creating a new gray scale image based on that information in a dark environment using the infrared radiations.

**Keywords:** Infrared radiation, thermography camera, medical, armed forces, breast cancer.

---

## Introduction

Infrared thermal imaging technology is one new method using night vision technologies. Thermal imaging works without any ambient light in environments. In general, a hotter object emits more radiation. Infrared thermographic camera can operate as long as 14,000 nm in wavelengths.

A thermal camera is also known as a thermal imager, infrared camera or thermal imaging camera. It is a heat sensor that capable of detecting minor differences in temperature. The Thermal camera can collect the infrared radiation from a sequence of continuous action in the scene and creates a new image based on information about the objects temperature differences. Because objects are rarely precisely the same temperature as other objects, a thermal camera can detect the objects heat i.e., infrared radiation coming from the object and they will appear as distinct in a thermal image that creates a new image using infrared radiation. Those thermal images are also known as **Thermograms**.

Normally, these images are grayscale in nature in which the white objects are hot, black objects are cold and

---

**Amit Sharma\***

Management Education and Research Institute

**Nidhi Jindal\*\***

Management Education and Research Institute

the depth of gray indicates variations between the two objects. Some thermal cameras help users identify an object to add colors to images at different temperatures.

## Advantages

1. It has a capability of finding high temperature components.
2. It is used to observe the areas which cannot be accessed by other methods.
3. It is a non-destructive method. It is very useful to detect the objects in dark places.
4. In real time environment, thermography is capable of catching freely targets.
5. Large area temperature can be differentiated as it helps us to show virtual pictures.
6. It is also used in medical field especially in kinesiotherapy.

## Disadvantages

1. It has a capability of detecting surface temperatures directly.
2. When accurate temperatures are being measured, they are mostly affected by other surface reflections and different emissivity.
3. Thermal Imaging does not perform well in rain falling.



**Figure 1. Thermo Graphic Image of a Ring-Tailed Lemur**

### In Use

1. As in infrared cameras, the cameras are using image sensors which is not able to distinguish between the different wavelengths of infrared radiations because of this cameras have only single color channel. Out of the normal visible spectrum color has less meaning because of the complex construction of the different wavelengths doesn't map the uniform system of color vision used by humans.
2. Monochromatic images sometimes are displayed in pseudo-color, where the changes in color are used rather than changes in intensity to display changes in signal. As humans have much greater dynamic range in intensity detection. And this ability of seeing fine intensity differences in bright areas is limited; this technique is called density slicing.
3. According to the temperature measurements their colors are set. As warmest part of the image are colored white, intensity temperatures are colored red and yellows, and the dimmest part i.e., coolest parts are colored black. A scale should always be shown to relate the colors of temperature. The expensive cameras are of more resolution i.e., of 1280x1024. And thermo graphic cameras are much more expensive than their visible spectrum, though low performances of thermal cameras for smart phones are available in hundreds of dollars in 2014.
4. In un-cooled detectors the temperature differences at the sensor pixel are minute. At the

range of 10 of milliseconds the pixel response time is slow.

5. Thermography has many other uses too. Thermal imaging cameras are installed in various luxurious cars to aid the drivers. It is used by firefighters to see through smoke to find people and hotspot of fires. Power line technicians' uses thermal imaging to find the overheating joints and parts, to eliminate the potential hazards. Cooled infrared cameras can be found at astronomy research telescopes. And in medical field thermo graphic imaging is used to monitor the temperature in human being and warm blooded animals.

### Working of Thermal Imaging

1. First of all it is important to understand the light. Wavelength is related to the amount of energy in the light wave. Higher the energy shorter will be the wavelengths. Of all the visible lights, violet has the most energy and red has the lowest. Infrared spectrum is just next to visible light spectrum.
2. Infrared light can be divided into 3 categories:
  3. **Near-infrared (near-IR)** – It is also known as near-IR and is closest to the visible light. Its wavelength ranges from 700 billionths to 1,300 billionths, or 0.7 to 1.3 microns of a meter.
  4. **Mid-infrared (mid-IR)** – It is also known as mid-IR and its wavelengths range from 1.3 to 3 microns.
  5. In electronic devices both Mid-IR and near-IR are used.
  6. **Thermal-infrared (thermal-IR)** – It is also known as thermal-IR and it has wavelengths ranging from 3 microns to over 30 microns which is covering the highest part of the infrared thermal.

### Case Study

Recently this technology of thermal imaging systems was used in France by French police to arrest 2 brothers suspected in the Charlie Hebdo massacres because of rapidly evolving technology like in airports,

hospitals etc. Like GPS, thermal imaging was once used exclusively by military and law enforcement.

In the early 1990's, National Guard aircraft relied on thermal sensors to look for illegal drug activity at the Davidian Compound Branch in Waco, Tex.

In 2013, the Massachusetts State Police helicopter used thermal imaging to locate the Boston bombing suspect Dzhokhar Tsarnaev, after a homeowner reported that the bloodied fugitive was hiding in a boat in his yard.

In June last year, a military surveillance aircraft equipped with infrared sensors played a key role in the hunt for Justin Bourque, a refugee who had killed three police officers in Moncton, New Brunswick. He found the camera hiding in deep brush late at night.

Thermal imaging cameras are made up of a large array of unusual Micro-electro-mechanical Systems (MEMS) devices, as well as specialized optics. Predictable glass and plastic lenses can't be used because they wedge heat. Instead, these cameras require special lenses manufactured of transparent silicon.

The cameras, which detect changes in human's body temperature as small as one-tenth of a degree Fahrenheit, were originally used in Southeast Asia in response to outbreaks of SARS and bird flu, and more newly to alert officials to individuals who might have contracted Ebola.

### Future Scope

Thermal imaging has been successfully used in several areas. This technology is used by armed forces in various countries. In future we use thermal imaging

to follow the thoughts through infrared radiation detector. The future applications of Infrared Radiation detector systems require:-

- The higher pixel sensitivity and further increase in pixel density.
- The reduction of cost in IR imaging array systems due to less cooling sensor technology combined with integration of detectors and signal processing functions.

Thermal Imaging is now being emerging in smart phones as well and it has been launched by iPhone only. It is the costliest product as it was special product which supports thermal imaging by FLIR. It has several disadvantages to like previously device don't have a battery with a charger. But this advantage has prevailed over. Now a better product has been launched.

### Conclusion

As we discussed that infrared thermal imaging can be widely used in medical, armed forces and many more areas where this technology is used. In army, this technology can be used to find the suspected criminals. In medical, this technology is used to find the good solutions to different number of diseases or viruses. For example, today this technology can be used to measure the fever temperature and it can also be used in detection breast cancer. Infrared thermal imaging is a valuable adjunct to mammography and ultrasound, especially with dense breast parenchyma in women.

### References

1. Ring EF. Quantitative thermal imaging. *Clin Phys Physiol Meas.* 1990;11:87-95.
2. Anbar M, Gratt BM, Hong D. Thermology and facial telethermography, Part I: history and technical review, *Dentomaxillo, Fac Radiol.* 1998;27:61-7.
3. Vainer BG. FPA-based infrared thermography as applied to the study of cutaneous perspiration and stimulated vascular response in humans. *Phys Med Biol.* 2005;50:R63-94.
4. <http://en.wikipedia.org/wiki/Thermography>
5. [http://en.wikipedia.org/wiki/Thermographic\\_camera](http://en.wikipedia.org/wiki/Thermographic_camera)
6. <http://www.nytimes.com/>
7. <http://www.nydailynews.com/>

# Cyber Forensic: Introducing A New Approach to Studying Cyber Forensic and Various Tools to Prevent Cybercrimes

B. Vanlalsiama\*  
Nitesh Jha\*\*

---

## Abstract

With the advancement of technology world today Cyber-crimes, ethical hacking and various internet-based-crimes jeopardizes single or groups of internet users around the world. Even the greatest of the nations suffered being a victim of cyber-crime. However due to lack of digital evidence and methodology of cyber forensic the alarming crime remained unstoppable and will continue to last. The evolution of such crimes increases the need of implementing a proper and structural methodology for the study of cyber forensic to facilitate the inspection of cyber-crime and bring them to court. In this paper we adopted several phases, methodologies, including policies and educational system and combine into one effective procedures along with the powerful tool to work coordinately and to accommodate each phases after the completion of their own task. This paper serves as an enhancement of current tools and technique for the purpose of finding the accurate layers for specialization, certification, and education within the cyber forensics domain. It also highlights the importance and need of Cyber forensics tools to increase its toughness and the ability to combat this persistent threats. This paper focuses on briefing of Cyber forensics, various phases of cyber forensics, handy tools which will helps in the finding and bring the intruders in the court of law for judgment.

**Keywords:** Cyber Crime, Digital Evidence search Kit. Ethical hacking, Resource Centre for Cyber Forensic

---

## Introduction

Cyber forensic play a vital role in solving crimes. the collection of forensic evidence serve an important key role that sometimes it is the only way to establish or exclude any case between suspect and victim or crime scene, eventually to establish a final verdict. As Internet technologies associate with us into everyday life, we come close to realizing new and existing online opportunities. One such opportunity is in Cyber forensics, unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted which helps in investigation process. The American Heritage Dictionary defines

---

### B. Vanlalsiama\*

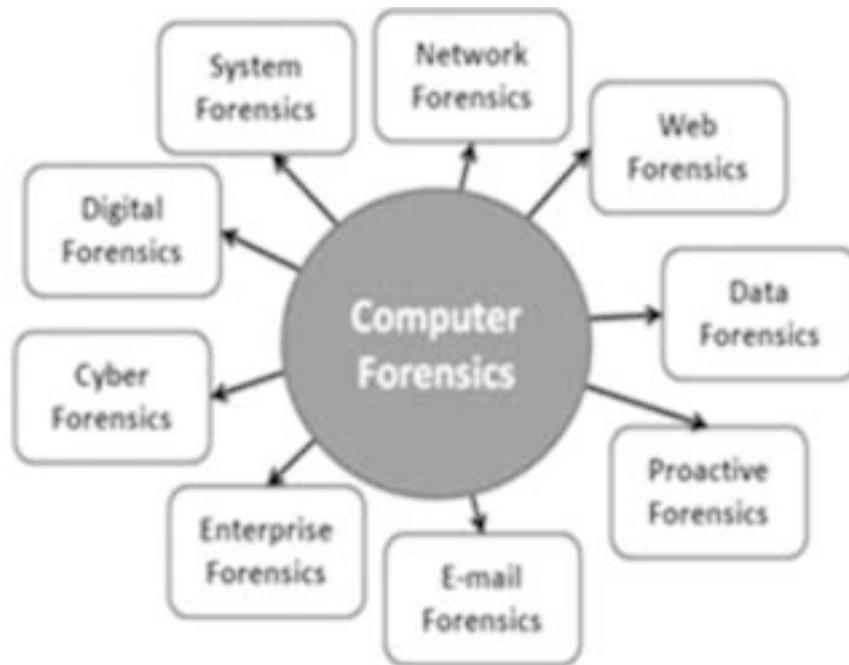
MCA: 4th Semester  
B-46, Chanakya Place, Janakpuri, New Delhi

### Nitesh Jha\*\*

MCA: 4th Semester,  
C-39, Sagar Pur, Jankapuri, New Delhi

forensics as “relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law” [1].

According to the National Crimes Record Bureau, 4,231 cyber-crimes were registered under the IT Act and cyber-crime-related sections of the Indian Penal Code (IPC) during 2009-11. A total of 1,184 people were arrested under the IT Act for cyber-crimes, while 446 people were arrested under IPC sections. At least 157 cases were registered for hacking under the IT Act in 2011, while 65 people were arrested. Although a very large number of cyber-crimes probably go unreported, this statistics give us some idea about prevalence of cyber-crime in the country. This is making cyber forensics increasingly relevant in today's India. The CID's cybercrime cell recorded a massive 202% jump in cybercrime cases in 2014 compared to the year before. While the total number of cybercrime cases recorded in 2014 is 675, the figure stood at 334 in 2013.



**Figure 1. Status of Cyber-crime in India**

Taking the picture of India. Majority of the people in the country are unaware of such crime and keeps to the duty of police or investigator alone. Its initiative work in combating cybercrime remain still ineffective. Due to the unskilled or less knowledge of the investigator these crimes continue to emerge year after year. From the current scenario one can draw a hypothesis as If proper training and awareness regarding the importance of tackling cyber-crime is not recommended possibly India will suffer more than other countries in a coming decade.

Cyber forensics activities commonly include [1]

- The collection and analysis of computer data
- The identification and acknowledgement of suspect data
- The examination and of suspect data to determine details such as origin and content
- The presentation of computer-based information to courts of law
- The application of a country's laws to computer practice.

The existing methodology consists of the 3 A's:

- Acquire the evidence without altering or damaging the original

- Authenticate the image
- Analyze the data without modifying it. [2]

Using the Internet, hacker finds an opportunity to hack or perform illegal action because we all know one person sitting in a room can hack a person bank account living in another country. Since the introduction of inter-networking, hacker or intruder's action against theft, hack, and phishing have increased tremendously. It is essential that high security is maintained. It is however simply cannot be compromised. Hacker also begin to spark a better idea by using anti-forensic tool to commit a crime to hide away his/her identity. Due to this many organization were establish such as Resource Centre for Cyber Forensic (RCCF) in India to combat these kinds of crimes.

#### **Overview of RCCF**

- It offers various Cyber Security auditing services
- Consultancy for ISMS Auditing
- Cyber Forensic Analysis, Training and Laboratory Development
- Malware Analysis
- Vulnerability Assessment and Penetration Testing of Web Applications and Networks [3]

## Overview of tools available

Tools are mainly used for collecting digital evidence pertinent to different areas like disk forensics, network forensics, device forensics, live forensics, enterprise forensics, photo forensics and virtualized environment forensics. Some of the various tools presently used are as under:

Disk Forensics Tool: Suite with Disk imaging (True Imager), Data recovery and analysis (Cyber Check), S/W for tracing sender of e-mail, Forensic Data Carving (F-DaC), Forensic Registry analysis (F-Ran) and Forensic Thumbnail extraction (F-TeX) tools.

Network Forensics Tool: Suite with Network Session Analyzer (NeSA), Forensic Log Analyzer and S/W for tracing sender of e-mail

Mobile Device Forensics Tools: Software solution for acquisition and analysis of mobile phones, smart phones, Personal Digital Assistants (PDA) and other mobile devices (Mobile Check), s/w for analyzing Call Data Records of various service providers (Advik) and forensic solution for imaging and analyzing SIM cards (SIMXtractor)

Live Forensics Tool (Win Lift): Software solution for acquisitions and analysis of volatile data present in running Windows systems

Portable Forensics Toolkit: TrueTraveller is a portable forensics toolkit. [4]

## A New Approach

As with any other crime scene, suspects leave behind trace evidence of their actions when using computers to commit a crime. Gathering evidence from a computer can be challenging, but valuable, because every operation that an each person carries out on a computer leaves behind a record that is usually dated. Finding and preserving that evidence requires careful methods as well as technical skill. Information on a computer system can be changed without a trace, the scale of data that must be analyzed is vast, and the variety of data types is enormous. Just as a traditional forensic investigator must be prepared to analyze any kind of piece of information or fragment, no matter the source, a forensic investigator must be able to make sense of any data that might be found on any device

anywhere on the suspect boundary or areas. However, computer traces can also be misinterpreted and, without the proper approach, files containing valuable evidence can be lost. Therefore the field of cyber forensics, still in its infancy, possesses a strong need to educate with the best training kit to equip the personnel with the latest knowledge and information.

## Policies that enhance cyber forensic

### 1. Accurate data collection

Every policy adopted must fulfill the enterprise or organization requirement. Each enterprise's goal is to collect accurate and precise information to which the investigation could be performed and transform into useful evidence to capture the intruders. Since the misleading of information may have a huge impact on the current status of the investigation. One must keep in mind, presenting accurate data play a key role in the findings.

### 2. Education

Despite the changes, cyber-crime investigation in the state needs improvement. "Majority of the personnel handling cyber-crimes in the state have not studied computer science during their graduation or post-graduation. Though they are still doing their best, we believe that recruitment of B Tech graduates and post graduates with M.Sc., M.Tech or MCA degrees will immensely improve investigation standards and result in effective crime prevention,"

With technology playing a signification role in our day-to-day affairs, electronic data analysis like cellphone data analysis has become a part of even the traditional crime investigation process.

Surveillance and analysis of social media and cellphone data has become an integral part of prevention and investigation of terror and communal cases. It is a high time that cyber forensic education is prioritize with the same level of other line of education or even higher than that.

### 3. Forming forensic team

According to Robert Graham, a response team should include members from upper management, Human Resources, the technical staff, and outside members. The upper management member can ensure that the decisions made by the forensic team are balanced with

the overall goals and best interests of the enterprise and that the decisions of the team have appropriate weight. Because of the personnel issues involved, there should be a member from human resources department. There should also be a member of the Information Technology (IT) staff on the forensics team. Security issues are often handled separately from normal IT activity. In such a case, the forensics team should work hand in hand with the IT department [6546456]

#### **4. Role of investigator**

One of the key factor to investigation is the way of investigating. Approach has been made this paper actually focus on Reactive and Proactive Investigations. Intuitively, reactive investigations attempt to solve crimes that have already occurred; this is the most frequent type .Proactive investigations attempt to deal with crime prior to the victimization, rather than after it has exacted harm on an individual, a corporation, or society.

#### **5. Cyber forensic and law enforcement**

A basic level understanding of computer forensics, at the very least, is an essential knowledge area for all law enforcement officers. Investigators need to know when information on a computer might have a nexus to a crime, how to write an appropriate warrant to seize and search a computer, and how to gather and search cyber evidence. Prosecutors and judges need to better understand the role of digital evidence — and the laborious task of a proper and thorough computer forensics exam. High technology crime task forces have already been formed in the larger metropolitan areas where this is a particularly serious problem, but the problem is actually far more widespread than just the big cities. Even a patrol officer who is not involved in computer crimes needs to know what actions to take when a computer is discovered at a crime or arrest scene. [5]

#### **Overview of Methodology Used**

It has studied that so many methodology for cyber forensic are currently being carried and applied in law enforcement. Even though many tools and various techniques has deployed we came to learnt that so many cyber-crimes cases remain pending and left

unsolved. With the existing methodology and technique in this paper we form a special blended methodology which abbreviate as VIAR and its phases are discussed below:

##### **a. Verification.**

The first phases in this blended-methodology is to verify that an incident has taken place. Determine the breadth and scope of the incident, assess the case. What is the situation, the nature of the case and its specifics? This preliminary step is considered paramount important because will help determining the characteristics of the incident and defining the best approach to identify, preserve and collect evidence.

##### **b. Information acquisition.**

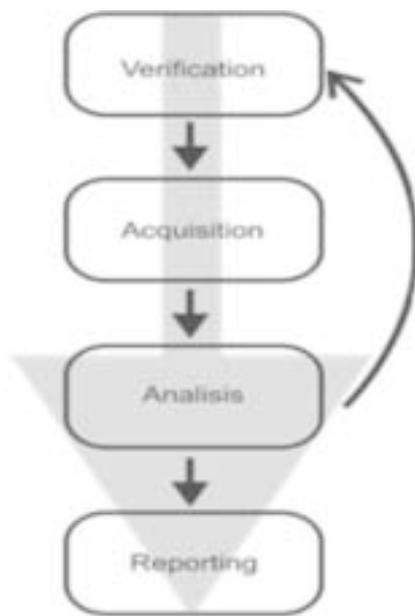
The next step is followed by taking notes (legal document) and describing the system you are going to analyze, where is the system being acquired, Outline the operating system and its general configuration such as disk format, amount of RAM and the location of the evidence. During this step is also important that you prioritize your evidence collection and engage the business owners to determine the execution and business impact of chosen strategies

##### **c. Analysis of information.**

After the evidence acquisition you will start doing your investigation and analysis in your forensics lab. Start by doing a timeline analysis. This is a crucial step and very useful because it includes information such as when files were modified, accessed, changed and created in a human readable format, known as MAC time evidence. The data is gathered using a variety of tools and is extracted from the metadata layer of the file system. Limited examination covers the data areas that are specified by legal documents or based on interviews. This examination process is the least time consuming and most common type. Partial examination deals with prominent areas. Key areas like log files, registry, cookies, e-mail folders and user directories etc., are examined in this case of partial examination. This partial examination is based on general search criteria which are developed by forensic experts.

##### **d. Reporting Results.**

The final phase involves reporting the results of the analysis, which may include describing the actions



**Figure 2. Phases of cyber forensic**

performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process. Reporting the results is a key part of any investigation. Consider writing in a way that reflects the usage of scientific methods and facts that you can prove. Adapt the reporting style depending on the audience and be prepared for the report to be used as evidence for legal or administrative purposes. The scientific method used in this phase is to draw conclusions based on the gathered evidence. This phase is mainly based on the Cyber laws and presents the conclusions for corresponding evidence from the investigation.

The above figure depict phases of cyber forensic. It is arrange in terms of stack resembling a top down approach. The top most phase is the first to be executed followed by acquisition and so on. To enhance cyber forensic phases unlike the existing phases, in this paper we make this phases iterative to ensure all the information gather and document are accurate. This eliminate the need of re-examination.

### **Cyber Forensics Tools**

The main objective of cyber forensics tools is to extract digital evidence which can be admissible in court of law. Electronic evidence (e-evidence, for short) is

playing a vital role in cybercrimes. Computer forensics tools used to find skeletons in digital media. To reduce the effect of anti- forensics tools the Investigator is likely to have the tools and knowledge required to counter the use of anti-forensics techniques [17]. Sometimes collection of digital evidence is straightforward because intruders post information about themselves from Facebook, Orkut, Twitter, Myspace and chat about their illegal activities. A subpoena, rather than special forensics tools, required obtain this information; these e-mails or chats from social networks can be admissible as evidence. [6]

### **Overview of DESK**

To achieve all the phases being introduced we adopted one of the greatest tool called. Digital Evidence Search Kit (DESK). Desk machine is the computer used by a law enforcement agent and the subject machine is the personal computer of the suspect. The two machines communicate with each other using a serial (RS-232)

The main operations of DESK are provide by two software components in the DESK system:

- A text pattern file which contains search keywords, in Chinese and/or English, to be searched for on the subject machine, and
- Hash value databases that contain ‘fingerprints’ of file systems that enable file integrity verification. [7]

### **DESK search methods**

The first important feature of DESK is the search function. It is used to search for files on the subject machine that contain pre-defined search keywords. Pre-defined search keywords are words that are relevant to a particular crime case. For instance, in a bank corruption crime, the pre-defined text patterns may contain names of different banks. The patterns can either be in English or in Chinese, or combinations of both. For Chinese patterns, different encodings of Chinese, such as Big5, GB (2312) and Unicode UTF16, are supported.

There are three main kinds of search operations:

Physical search: Physical search performs a search of the patterns of each physical sector of the subject machine’s storage system. By using a physical search, cybercrime evidence purposely stored in unused sectors in the storage

system can be discovered. Moreover, it provides a way for searching files independent of the specific file system. The disadvantage is that physical search, due to its lack of knowledge about the file system, can only search data within individual physical disk sectors

**Logical search:** Logical search makes use of the information about the file system. Conceptually, a file is a continuous sequence of bytes and the file system takes care of placing portions of the sequence into different sectors (not necessarily contiguous) while maintaining the logical contiguity of the contents of a file. A file can have a size larger than that of a disk sector. Sometimes a search pattern for a file may be split across two sectors. In these cases, the pattern cannot be found by a physical search, but can be found by a logical search.

**Deleted file search:** The third kind of search is the deleted file search. In most file systems, file deletion is typically accomplished by modifying only a few bytes of the file system. The contents of a deleted file are still in the storage system provided that it has not been overwritten. Therefore, patterns in a deleted file can still be found until "deleted" disk sectors are overwritten by other new files. DESK is able to search the sectors of files that have been deleted but not yet overwritten. [8]

## Conclusion

Computer related crime is growing as fast as the Internet itself. Today, enterprises focus on implementing preventative security solutions that reduce vulnerabilities, with little concern for systematic recovery or investigation. We propose six categories of policies that will enable or facilitate after-the- fact

action that can reduce the impact of computer crime and can deter computer crime from occurring. Some of the policies that we propose are simple actions that responsible network managers already engage as a matter of system reliability or as part of a disaster recovery procedures. The focus on computer and network forensics distinguishes these policies from backup and recovery needs. The procedures for cyber forensic require systematic application and detailed documentation, else the information may not be admissible in court. Further, backup and recovery procedures routinely ignore temporary information and other important sources of potential evidence.

Moreover, cyber forensic is much broader than just providing ready sources of potential evidence. As people get more and more comfortable with computers, and technology advances, society becomes more computer dependent. In an era where everything from the stock market to air traffic control is managed by computers, security becomes a survival issue. In today's society, computer crime is a serious problem. Preventive measures are not enough anymore, we must find a way to catch and prosecute computer criminals, and computer and network forensics is the gateway to archive it.

We should not leave everything to computer forensics experts. If we are going to find a solution to the computer crime problem, it will be through a collaborative effort. Everyone from individual users, to company owners have to get involved. This paper proposes policies, methodology and tools to enhance the forensics of computer security by helping experts in the field do their job faster and more efficiently. It is up to the companies and users to adopt these policies according to their needs.

## References

1. Plethora of Cyber Forensics
2. www.ijarcse.com International Journal of Advanced Research in Computer Science and Software Engineering
3. <http://www.cyberforensics.in/Aboutcdac.aspx>
4. [http://cdac.in/index.aspx?id=cs\\_cf\\_cyber\\_forensics](http://cdac.in/index.aspx?id=cs_cf_cyber_forensics)
5. [http://www.computerforensics.com/law\\_enforce.html](http://www.computerforensics.com/law_enforce.html)
6. <http://www.icbse.com/careers/cyber-forensics>
7. [http://www.engpaper.com/a1/computer-forensics\\_research-papers.html](http://www.engpaper.com/a1/computer-forensics_research-papers.html)
8. <http://articles.forensicfocus.com/2014/11/29/investigation-and-intelligence-framework-iif-an-evidence-extraction-model-for-investigation/>
9. <http://articles.forensicfocus.com/>
10. <http://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps/>

# Cyber Crime and Information Warfare- The New Arenas for WAR

Anwasha Pathak\*

Rohit Sharma\*\*

---

## Abstract

With the advent, advancement and development of the Internet and particularly the World-Wide-Web has accelerated the perception in mankind for his dependency on information technology. As a consequence, various problems of national and international law and ethics have emerged which have increasingly been grabbing the attention of cyber experts, public policy makers and national security experts, especially those concerned about the future of warfare. A new form of warfare, "Information warfare", is defined to occur when one nation seeks to obtain strategic leverage over another by subverting, disrupting or damaging information systems. Compared to other forms of warfare, information warfare possesses several distinct features. The distinct features of information warfare and the legal/ethical ramifications of these features are characterized in order to stimulate a deeper consideration of this new context.

The authors here will focus on the measures to prevent cyber crime, effects of these crimes on teenagers and more importantly Legal Issues Concerned with Information warfare & e-Crime.

**Keywords:** Chipping, Espionage, Information warfare, Offensive Software

---

## Introduction

Military affairs which were previously based on wars with hardcore weapons such as long-range missiles, heavy machine guns, tanks, fighter planes etc. which took place at a large piece of land have now changed and have taken a very innovative way. Innovative here means a way through which these wars are now limited to a small room and a desktop with an internet connection which is able to devastate the security of the whole country. In other words, we can say that Information warfare is the latest innovation in the vast history of warfare. Information warfare may be defined as an attack on information systems of military advantage using tactics of destruction, denial, exploitation or deception or all. The spread of information warfare is connected from the rapid dispersion of information technology.

Flowchart-1, below shows us of how information was derived from Fischer (1984). It is to be noted that the

---

**Anwasha Pathak\***

B.A. LL.B. 3rd Yr., New Law College

**Rohit Sharma\*\***

B.A. LL.B. 3rd Yr., New Law College

cycle (flowchart) here has eleven different levels that shows the processing of data gathering to data entry to data reception to data processing and storing and so on. The last 2 stages here are related from data retrieval and thereafter the usage of this data.

Currently cyber experts all around the world are searching for tough protection in each stage of the flowchart, but there is a technical problem often termed as a 'cyber threat problem' that for every solution or for every protection a new kind of threat can be developed, sooner or later. The threat of Information warfare will continue to rise as the costs of beginning are too low and day by day these costs are cutting down due to which many of the foreign governments realized the need of a separate strategic information warfare branch under their military and other security based organizations. Few of the foreign nations have already got within them this facility. The system of information is so critical that one nation attacks other nation's information system, instead of attacking its military. The reason behind this is that the first option is cheap and cost effective as compared to the second option. Also it destroys and devastates the internal security issues of the latter country resulting in huge loss in economical matters.

## Legal and Ethical Challenges of information warfare

The following six sections analyze the most significant legal and ethical questions of information warfare as a new form of warfare. Many of the questions have been raised before in previous contexts but the unique characteristics of information warfare bring urgency to the search for new relevant answers.

It should be noted that this analysis is also pertinent to other military situations generally referred to as Operations Other Than War (OOTW) such as peace-keeping missions, preludes to conflict, alternatives to conflict, sanctions, and blockades. For example, in an information warfare analogy to the U.S. blockade of Cuba during the Cuban missile crisis, there are information warfare techniques (i.e. jamming and denial of service attacks) which could be used to block and thus isolate rogue nations from international communications without circumventing physical sovereignty much in the same way the British decided to sever all transatlantic telegraph cables that linked Germany to international communications at the outset of World War I.

The Sections are as follows:

### 1. What Constitutes an Act of War in the Information Age?

The nation-state combines the intangible idea of a people (nation) with the tangible construct of a political and economic entity (state). A state under international law possesses sovereignty which means that the state is the final arbiter of order within its physical geographical borders. Implicit to this construct is that a state is able to define and defend its physical geography. Internally a state uses dominant force to compel obedience to laws and externally a state interacts with other states, interaction either in friendly cooperation or competition or to deter and defeat threats. At the core view of any nation-state's view of war should be a National Information Policy which clearly delineates national security thresholds over which another nation-state must not cross. This National Information Policy must also include options which consider individuals or other non-state actors who might try to provoke international conflicts.

Increasingly the traditional attributes of the nation-state are blurring as a result of information technology. With INFORMATION WARFARE, the state does not have a monopoly on dominant force nor can even the most powerful state reliably deter and defeat INFORMATION WARFARE attacks. Increasingly non-state actors are attacking across geographic boundaries eroding the concept of sovereignty based on physical geography. With the advent of the information age, the U.S. has lost the sanctuary that it has enjoyed for over 200 years. In the past, U.S. citizens and businesses could be protected by government control of our air, land, and sea geographical borders but now an INFORMATION WARFARE attack may be launched directly through (or around) these traditional geographical physical defenses.

War contemplates armed conflict between nation-states. Historically war has been a legal status that can be specified by declaration and/or occur by way of an attack accompanied by an intention to make war. The modern view of war provides a new look at just war tradition, "jus ad bellum", (when it is right to resort to armed force) and "jus in bello", (what is right to do when using force). The six requirements of "jus ad bellum" were developed by Thomas Aquinas in the 13th century:

- (1) the resort to force must have a just cause
- (2) it must be authorized by a competent authority
- (3) it is expected to produce a preponderance of good over evil
- (4) it must have a reasonable chance of success
- (5) it must be a last resort
- (6) the expected outcome must be peace

There are two requirements for "jus in bello"

- (1) the use of force must be discriminate (it must distinguish the guilty from the innocent)
- (2) the use of force must be proportional (it must distinguish necessary force from gratuitous force)

The application of just war reasoning to future information warfare conflicts is problematic but there is a growing voice that there is a place for the use of force under national authority in response to broader

national security threats to the values and structures that define the international order. Looking at one aspect of the application of just war reasoning to information warfare, the problem of proportionality - It is impossible to respond to every information warfare action, there are too many. At what threshold in lives and money should the U.S. consider an information warfare attack an act of war. How many lives for a certain information warfare attack or what is the threshold in monetary terms or physical destruction.

Article 51 in the United Nations Charter encourages settlement of international disputes by peaceful means. However, nothing in the Charter "impairs the inherent right of individual or collective self-defence if an armed attack occurs..." Note that infringement of sovereign geographical boundaries by itself is not considered an "armed attack". Also note that experts do not equate "use of force" with an "armed attack". Thus certain kinds of data manipulation as a result of information warfare which are consistent with "use of force" would not constitute an "armed attack" under Article 51. Article 41 of the United Nations specifically states measures that are not considered to be an "armed attack": "Complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications..." information warfare might still be considered an Act of War, however, if fatalities are involved. If data manipulation is such that the primary effects are indistinguishable from conventional kinetic weapons then information warfare may be considered an "armed attack". The paradigm shift is that weapons are devices designed to kill, injure, or disable people or to damage and destroy property and have not traditionally included electronic warfare devices.

## 2. What are the Legal and Ethical Implications of the Blurring Distinction between Acts of War from Acts of Espionage from Acts of Terrorism?

It is very important to be precise in what we identify as a crime and what we identify as an act of war. An "armed attack" as stated in Article 51 contemplates a traditional military attack using conventional weapons and does not include propaganda, information gathering, or economic sanctions. Espionage is a violation of domestic and not international law.

The threat analysis section of the 1997 Defence Science Board Report indicates that "a significant threat includes activities engaged on behalf of competitor states." This introduces the new concept of low-intensity conflict in the form of economic espionage between corporations. In the age of multinational corporations that view geographical boundaries and political nation-states as historical inconveniences - should economic warfare between multinational corporations involve the military?

The new information warfare technologies make it difficult to distinguish between espionage and war. If espionage is conducted by computer to probe a nation's databanks and military control systems when is it an act of war versus an act of espionage? Does it depend on whether the intelligence was passively read versus information actively destroyed and/or manipulated? Does it depend on whether the intelligence was used for military advantage or whether the intelligence was used for political or criminal advantage? Does the answer depend on whether a state of war exists or not?

A different scenario is modifying internal computer software (via viruses, trojan horse, or logic bomb) or hardware (chipping) before shipment to cause an enemy's computer to behave in a manner other than they would expect. If during peacetime, gaining entry to a computer's internal operating system could be considered a criminal offense or act of espionage despite the fact that the action in question took place before the enemy had acquired ownership of the computer. Is this prudent preparation for information warfare or is this a hostile action that could precipitate a war? If the computer hardware "chip" is commercially manufactured and altered, what are the legal and ethical ramifications of a company inserting internal hardware hooks in cooperation with a national security "request" from a government? Lastly, is information warfare a potential step which might lead to an escalated conventional military conflict which could have been avoided by other means?

## 3. Can information warfare be Considered Nonlethal?

Nonlethal weapons are defined as weapons whose intent is to nonlethal overwhelming an enemy's lethal force by destroying the aggressive capability of his

weapons and temporarily neutralizing their soldiers. Nonlethal is most often referred to immediate casualty counts and not on later collateral effects. In response to the power of public opinion and instant global media coverage, the U.S. military has begun to develop a new kind of weaponry designed to minimize bloodshed by accomplishing objectives with the minimum use of lethality. This weaponry includes sticky foam cannons, sonic cannons, and electromagnetic weapons which temporarily paralyze an opponent without killing them.

Is it more ethical to use a sophisticated smart bomb precisely targeted to kill 10-20 soldiers immediately or is it more ethical to choose a nonlethal weapon which has the same tactical effect with no immediate casualty count but an indirect collateral effect of 100-200 civilian deaths?

The function of the target against which the weapon is used and the existence or lack of a state of war determines one legal framework for analysis. For instance, disabling the electronics of a fighter plane or air defence radar during wartime is the goal of a large investment in electronic warfare equipment by the U.S. and is considered fair and ethical. However, disabling the electronics of a civilian airliner or air traffic control during either peacetime or wartime violates the principles of discrimination of combatants and proportionality of response and is considered unethical and an illegal act against humanity.

#### 4. Is it Ethical to Set Expectations for a “Bloodless War” Based on information warfare?

As nonlethal weaponry of all types (especially information warfare weapons) advance from novelty to norm, however, many potential pitfalls will need to be faced. The most important of these is the expectation that such weapons will ultimately allow wars to be fought without casualties. Nonlethal military capabilities are not new although information warfare weapons are the newest weapons in the nonlethal arsenal. Military forces have used riot-control chemical agents, defoliants, rubber bullets, and electric stun weapons for decades. As U.S. military forces are involved in missions that require extended direct contact with civilians (e.g. Somalia, Bosnia), force can no longer be viewed as either on or off but rather as a

continuum with nonlethal weapons on one end and nuclear devices on the other end. In more traditional conventional warfare, information warfare attacks to disrupt, deny and destroy C4I capabilities

(Command, Control, Communication, and Computer Intelligence) are a core part of military tactics and strategy.

If information warfare weapons can be used to remotely blind an opponent to incoming aircraft, disrupt logistics support, and destroy or exploit an adversary's communications then many of the problems associated with the use of ground forces for these missions can be avoided. It is important to point out that although nonlethal weapons are not meant to be fatal, they can still kill if used improperly or against people particularly sensitive to their effects. Because these technologies are potentially lethal in these circumstances, the term “nonlethal” has not been universally accepted within the U.S. military. For example, the U.S. Marines Corps uses the term “less lethal” to imply that there is no guarantee of non-lethality.

Asserting that information warfare will ultimately allow future wars to be fought without casualties is a widespread misconception likely to prove counterproductive and even potentially dangerous. First, all nonlethal weapons are not equally applicable to all military missions. Second, overselling of nonlethal capabilities without providing a context can lead to operational failures, deaths, and policy failure. Third, unrealistic expectations about nonlethal weapon capabilities inhibit their adoption by military forces who need to build confidence in these weapons.

There is a large asymmetry in global military power when comparing the U.S. versus other nation-states. In 1994, the U.S. DoD (Dept. of Defense) budget exceeded that of Russia, China, Japan, France and Great Britain combined. This asymmetry makes it unlikely another nation-state would challenge the U.S. in a direct high-technology conventional war except for circumstances which we should not depend upon (e.g. incredible miscalculations and/or ignorant dictators which were both present in the Gulf War). Despite the luxury of a bumbling opponent, the success of the Gulf War has led the U.S. citizenry to

expectations of low casualties in all future conflicts. These expectations go against two cardinal rules of military strategy;

- (1) you do not plan to refight the last war and
- (2) the future battlefields cannot not be dictated by the United States.

The next battlefield for which the U.S. DoD is preparing is a global battlefield with weapons of information warfare “targeting” civilian infrastructure. Even in this scenario, military and civilian casualties will be likely from either primary or secondary effects from information warfare attacks.

5. Is it Legally and Ethically Correct to Respond to information warfare Tactics with the same Tactics?

If the U.S. is attacked by information warfare weapons, how should the U.S. Government respond?

By changing perspectives from defence to offense, what is in the U.S. arsenal to wage information warfare against an adversary:

- A. Offensive Software (viruses, worms, Trojan horses)
- B. Sniffing” Or “Wiretapping” Software (enabling the capture of an adversary’s communications)
- C. “Chipping” (malicious software embedded in systems by the manufacturer)
- D. Directed Energy Weapons (designed to destroy electronics & not humans/buildings)
- E. Psychological Operations (sophisticated and covert propaganda techniques)

A strategy that uses these weapons in various combinations has the potential to replace conventional military force. The questions remains: is it legally and ethically correct for the U.S. to defend its security interests by resorting to the same information warfare tactics that are being used against it? Should information attacks be punished by information counterattacks? The options include maintaining our superpower status at all costs; covertly listening to our adversaries but not actively disrupting operations; or contracting mercenaries in no way officially affiliated with the U.S. government to do our dirty work. Cracking computers to deter and punish computer cracking erodes any moral basis the U.S. has for

declaring the evils of information warfare. It is also harder to predict secondary effects due to the globalization of systems. Retaliation may produce effects ranging from nothing to being counterproductive through destruction of U.S. interests. A nation-state or non-state actor that sponsors an attack on the U.S. might lack an NII (National Information Infrastructure) of their own for the U.S. to attack in punishment and thus not be intimidated by a U.S. information warfare deterrence strategy.

The problem is that there are no characterized rules of engagement for information warfare conflicts which can take forms of isolated operations, acts of retribution, or undeclared wars.

The most serious problem for using information warfare retaliation to counter information warfare attacks is that adversaries could counter and/or copy information warfare capabilities. Every breakthrough in offensive technology eventually inspires a matching advance in defensive technology so forth thus escalating an information warfare weapons race. A last issue related to retaliation is the dilemma faced by the intermingling of the military and civilian sides of society. Given the uncertainty of deterrence and identifying the enemy, which strategy is appropriate for retaliation; (a) a strategy that attempts to separate the military from civilians and in so doing has a diminished impact which potentially prolongs the duration of the conflict; or (b) a strategy that attempts to minimize lethality and duration but deliberately targets civilian systems?

6. Can Protection from information warfare Take Place in the United States Given Our Democratic Rights?

How much government control of the U.S. NII is feasible in a free society?

Most of the information warfare technology is software which is easy to replicate, hard to restrict, and dual-use by nature (uses for both civilian and military). In the 1997 Defence Science Board report, it states that the DoD is “confused” about when a court order is required to monitor domestic communications. This raises basic questions about the constitutional and ethical balance between privacy and national security in a new information warfare context.

A “Big Brother” approach that places all of a nation’s telecommunications under a single government jurisdiction is improbable given the diffusion and complexity of technology and the shrinking size of government. Most systems were built to serve commercial users who will vehemently object to unfunded mandates (i.e. taxes) and new requirements not driven by business demand (e.g. CLIPPER chip encryption and key escrow accounts). Regardless, it is critical to the future security of the U.S. that we find a way to protect our infrastructure from information warfare attack and have contingency plans for potential information warfare crises. If the information warfare attack is detected and the enemy identified but the U.S. is unable to react promptly due to bureaucratic inefficiency or indifference from private industry, it may be too late to react at all.

Current political discussion has floated tax incentives and direct subsidies to promote industry cooperation. In a related matter that may provide a precedent, the government has pledged to provide telephone

companies with at least \$500 million to ensure that FBI officials can access telephone conversations over digital circuits (as opposed to accessing telephone conversations over analogue circuits which is technically much easier).

### **Conclusion**

To be sure, cyberspace is hardly the first or the only policy domain which lies beyond the control of any single nation state. International air traffic, the law of the sea, funds transfers, and such environmental considerations as ozone depletion and global warming, among others, have required concerted international efforts. One would expect that the development of international arrangements in response to telecommunications-related crime will occur in a manner not unlike those which have accompanied other extraterritorial issues, from drug trafficking, to nuclear testing to whaling. Whether the realm of telecommunications will be able to achieve a better record of success than these other enduring global issues remains to be seen

### **References**

1. Department of Homeland Security, A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment. (November 5, 2004) Guttman, M., Swanson, M., National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce.,
2. Generally Accepted Principles and Practices for Securing Information Technology Systems (800-14). (September 1996) National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce.,
3. An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12. Swanson, M., National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., Security Self-Assessment Guide for Information Technology Systems (800-26).
4. The North American Electric Reliability Council (NERC). <http://www.nerc.com>. Retrieved November 12, 2005.
5. [isasecure.org](http://isasecure.org) site
6. ISO webpage
7. NERC Standards (see CIP 002-009)
8. NIST webpage
9. Ssrn.com
10. Westlaw.co.in
11. Google.com

# Legislation Vulnerabilities, Threats and Counter Measures in Wireless Network Security

Kushagra Dhingra\*  
Ankit Verma\*\*

---

## Abstract

Wireless network deliver us numerous advantages, but it also sprinkle up with new security risks and modify overall information security threats profile. Although accomplishment of technological results is the usual reply to wireless security risks and vulnerabilities, wireless security is initially a management outcome. We comes out with a framework to help to conclude and assess different risks running mate with the use of wireless technology. We also comes out with enumerated solutions for combat those threats or risks.

**Keywords:** Wireless Network, Wireless Security, Wireless Threats, Signal-Hiding

---

## Introduction

A **wireless network** is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method through which we can connect Home (Telecommunication Network) and Enterprise (Business) networks. With the help of wireless network installations in these areas, we can avoid the coastally process of introducing cables into a building, or as connections between various equipment locations. Wireless telecommunications networks are generally implemented and administered using "Radio Communication". This implementation takes place at the physical level (layer) of the "OSI model" network structure. Examples of wireless networks include cell phone networks, Wi-Fi local networks and terrestrial microwave networks. Wireless networking presents many advantages to improve productivity because of increased accessibility to information resources, Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile.[3] For example, as

wireless network communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If we not encrypt the message, or message is encrypted with a weak algorithm, the attacker can easily attack and read it, it means we are compromising with our confidentiality. Although wireless networking is not secure but it alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The objective of this paper is to assist in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networking and available countermeasures. To test the performance of wireless network, we consider some bases such as their convenience, cost efficiency, and ease of integration with other networks and network components. In today's world majority of computers sold to consumers with pre-equipped with all necessary wireless Networks technology. The benefits of wireless Networks include: Convenience, Mobility, Productivity, Deployment, Expandability and Cost. Wireless Network technology, is absolutely same with the advantages and conveniences described above has its share of downfalls. For a given networking situation, wireless Networks may not be desirable for a number of reasons. Most of these reasons occur because of the limitations of the technology. The disadvantages of

---

## Kushagra Dhingra\*

Student of BCA  
IITM, Janakpuri, New Delhi

## Ankit Verma\*\*

Assistant Professor  
IITM, Janakpuri, New Delhi



**Figure 1. Wireless networking components.**

using a wireless network are: Security, Range, Reliability, and Speed. A host of issues for network managers presented by wireless network. Unauthorized access points, broadcasted SSIDs (*service set identifier*), unknown stations, and spoofed MAC (media access control) addresses are just a few of the problems addressed in WLAN (*wireless local area network*) troubleshooting. Most network analysis vendors, such as Network Instruments, Network General, and Fluke, offer WLAN troubleshooting tools or functionalities as part of their product line.

### Wireless Vulnerabilities

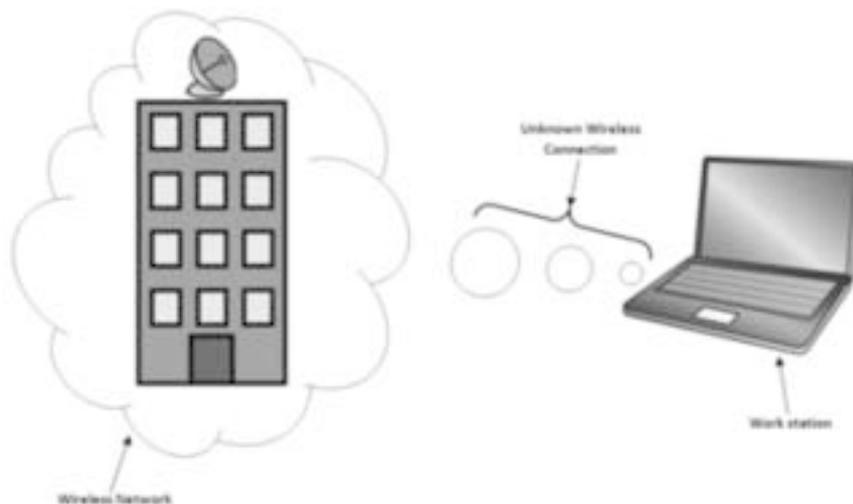
For connecting wireless networks we have to consider of four basic components: The transmission of data using radio frequencies; Access points that provide a connection to the organizational network and/or the Client devices (laptops, PDAs, etc.); and Users. Each of these components provides an avenue for attack that

can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

### Wireless Network Attacks

**Accidental association.** Unauthorized access to company wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company’s overlapping network, the user may not even know that this has occurred.[3] However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

**Malevolent Association.** There are different intents and methods to access any organization’s wireless or



**Figure 2. Malevolent Association**

wired network which is unauthorized. “Malicious association” is the one of these methods. For example:- if a user switch ones his computer and if there is a wireless access point nearby and if it's computer catches with that wireless access point, even he don't know that his system is connected to that wireless network. However, it is a vulnerable situation for the company, as their security is broken and their information is in endangered (one company can make a link to other and can style information). This vulnerability can also with the case if there is a wired network example: if the system is hooked to cables.[2]

**Virulent Association.** It is also known as “Malicious association”. This association are when crackers actively make a connection (through wireless device, a wireless Connection) to a running network through their hardware cracking device (like laptop) instead of that's network's AP (Access Point). Hardware devices which are used here are known as “soft APs”. Cracker develop these network by running some software which help to look lawful Access Point that wireless network which is developed to attack. Once if he/she (cracker) gets access he/she can thief the password, he/she can attack te wired or wireless network. There are some security authentication such as in level 3 and VPNs, and as we know wireless network is at layer 2 level. The wireless 802.1 x authentications is a kind of protection but it is still vulnerable and can be cracked. But attacker's idea is not to break VPNs or any other security measures. Crackers misty take over the client at layer 2 level.

**Computer to Computer Network.** It is also known as (“Ad-hoc network “). It acts as a security hazard this type of networks is defined as peer- to -a peer network which is work within the wireless computers which doesn't have any access point in between. Protection is less with these types of networks, for providing security we can use encryption method.

**Non-Heritage Network.** We can also call it “non-traditional network”. These types of networks such as Private Network Bluetooth devices. These types of networks are not safe and can easily crack by crackers and should be estimated as a security hazard. Some non-heritage networks such as wireless printers, barcode reader, copiers should be secured. These type

of networks can easily be outlook by an IT Personnel who have slender axis on laptops and AP's.

**Injecting Networks.** An attack which is known as Injecting Network (also known as “Man-in-the-middle” attack) , in this AP(Access Point ) is used by an attacker that are endangered with the network traffic which is not fettered, “Spanning Tree” (802.D), RIP,HSRP & OSPF are especial broadcasting network traffic. Attackers injects true networking re-framing the commands that can attack (or affect ) switches , intelligent hubs and routers , rebooting or reprogramming the network is done for the intelligent networking device.[7]

**DOS Attack.** This attack is known as denial-of-service attack. This attack takes place when a cracker (or attacker) ceaselessly assaulting a targeted access point(AP) or network with artificial requests, getting early messages of thriving connections, messages of failure, and many other commands . This scenario can affect legitimate (or true) users not able to get connected with network and even effects network failure or crash of the network. Abuse of protocols like EAP (Extensible Authentication Protocol) is the thing on which attack depends on.

### Wireless Transmission Security

Interception, disruption & alternation are three basic threats which are created by the nature of wireless communication.

### Securing the Confidentiality of Wireless Transmissions

There are couples of countermeasures which exist for decreasing the threats of eavesdropping on wireless transmissions. The first approach involves for materialize it more hellacious to discover and interrupt the wireless signals. The second approach involves the application of encryption to secure the confidentiality even if the wireless signal is interrupted.[8]

**Techniques of Hiding-Signals.** Initially attackers need to identify & discover wireless networks and then intercept the wireless transmissions. So user can follow a number of steps to make it more hellacious to discover their wireless access point. It is totally dependent upon user that which method the user should use. If the user needs signal hiding in easiest & least costly technique he should perform the following

ambulate: Turning off the service set identifier (SSID), provide mystic names to SSIDs, degrade signal strength to the level where only the user is able to use or locating wireless access points in the interior of the building, away from windows & exterior walls. More potent, but also more costly methods for dominating or shielding signals include: Using directional antennas to constrain signal emanations within specific areas of coverage. Sometimes, TEMPEST is referred as using of directional emanation of wireless signals.

**Encryption.** Encrypting all wireless traffic is the best technique for securing the confidentiality of transmits data over wireless networks. This is essentially meaningful for users subject to bylaw.

### **Head off modifications of Interrupted Communications:**

Interruption & modification of wireless transmission shows of form of “man-in-the middle” attack. Strong encryption & strong authentication are the two types of countermeasure can revelatory decreases the threads of such attacks for both devices & users.

### **Risk of DOS Attacks can be reduced with following Countermeasure:**

Denial-of-service also endangers to wireless communication. For reducing the risk of such unintentional DOS attacks organization can take several steps. One of the measure to identify location where signals from other devices exist by regulating careful site surveys; while locating wireless access points the backwash of such surveys should be used. Regular steady scrutiny of wireless networking activity & performance can identify knot areas; appropriate of the outraging devices or measure to signal vigor & scope within the knot areas.

## **Wireless Networks Security**

### **WAP Security**

Unsecured, deficient construction of WAP can leads us to compromise with some importance or confidentiality by permitting accessibility to some unauthorized one to the network.

### **Counteragent for Security WAP**

We can downgrade the threats of unknown/unwanted access to wireless networks by the help of follow three steps:

1. Exclude duplicitous access port
2. Protected architecture of authorized access point.
3. Application 802.1 x to authenticate all devices.

**Exclude Duplicitous Access Point.** The finery way for reducing the risks/threats of duplicitous access point is application 802.1x to authenticating all devices which are connection into a wired network application 802.1x will anticipate any underpowered devices from hooked to the network.[5]

### **Protected Architecture of Authorized Access Point.**

It should be assure that each and every authorized WAP's (wireless access points) are securely configured. Attackers can easily attack to AP (access point) with default setting because they are renowned by attackers so these settings are specifically to be changed.[4]

### **Assuring Wireless Client Devices**

There are couples of major risks to wireless client devices are:

1. Mislays or steal
2. Compromise

Mislays or stealing of some hardware or storing devices like laptops or PD's is a grave matter these hardware or storage devices can stored information which is highly confidential. Evenly mislay or stealing of these hardware devices can lead to reveals the information parties. Second risk to this is that they can compromised. This compromising makes information sensitive to be attacked and access to distinct system resources (which is unauthorized to access).

### **Application Encryption**

Encryption is the most secured way for transferring any information on wireless network. Some of the devices like access points, wireless routes, and base stations have encryption mechanism in-built in them. If you don't have the wireless router it is preferable to get which does have it. Manufacturers make the encrypted feature of wireless routers turned off. It is suggested to turn on it.[1]

### **Application Anti-Spyware and Anti-Virus Software and a Firewall**

As we give protections to the computers which are connected with the internet. This same type of protection system is needed for the computers that are installed and maintained them up to the date.

### Switched Off Identifier Spread

Identifier spread is a mechanism which is used by many wireless routers. This mechanism is used to transmit signals to any device in the proximity enunciate its presence. If any device preliminarily known & connected to network then there is no need to spread or broadcast the information. With the use of identifier spread, attackers can easily attack and expose wireless network. It is suggested that switches off the identifier spread mechanism if wireless router permit is.

### Alter the Default Identifier for Your Router

Your router likely have a standard identifier, manufactures provides default ID to all devices of that model. It doesn't matter that your router not broadcasting its identifier to all, attackers can try to access your network as he know the default ID's. You should change and uniquely identify your identifier and don't forget to provide the same ID to your computer and your wireless router so they can interface among them. It is suggested that your password should be long at least of 10 characters: As longer is your password, is become most difficult to be break by the attackers.

### Permit Only Specific Devices that Access Your Wireless network

Each and every device provides its own unique MAC (Media Access Control) Address for communicating with a network. A mechanism is included with wireless router that permits only devices that have specific MAC address which can access the network. MAC address can be imitate by the attackers, so do not rely on this pad only.

### When you are Not Using Wireless Network Make Turn off It

Turn off wireless router can't be access by the attackers. If you are timely turn off the wireless router ("when

you are not using it"), then you are decreasing the vulnerability to be hacked.[2]

### Public "HOT SPOTS" are not secured

If you are thinking that wireless public Hot Spots are secured, then your thinking is wrong, these are not secured.

### Educate & Train Users

Training & educating will help users to be aware about the securing of wireless networking. To make it effective, the user training & educating process is needed to be repeated periodically. The major part of WLAN policy of security is wireless network inspecting. For decreasing the baddie hardware, network needs to inspect on the daily bases.[6] This method performs scanning & mapping processes for each & every WLAN nodes and access point of network. After it, previously mapped network is compared with this. Wavelan-tool which is usually is use. Airsnort is a specialized tool used for auditing the network for asthenic keys.

### Conclusion

Wireless networking furnishes many opening the accrual of productivity in declivity of costs. Collectively (using wireless network) computer security risk profile is altered. Totally elimination of risks is impossible even with wireless networking, but it is possible to attain a consequent level of collectively securing the network by embracing systematic approach for managing risks. In this paper we discussed about the vulnerabilities & risks hooked up with three wireless networking technical components such as transmission medium, AP (Access points) and client, and describe varied of common methods for decreasing risks. It evenly suggests to educate and give training to users about the safety of wireless networking operations.

### References

1. Graham, E., Steinbart, P.J. (2006) Wireless Security
2. Cisco. (2004). Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.
3. CSI. (2004). CSI/FBI Computer Crime and Security Survey.
4. Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.
5. Kelley, D. (2003). The X factor: 802.1x may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.
6. Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).
7. Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.
8. Paladugu, V., Cherukuru, N., & Pandula, S. (2001). Comparison of security protocols for wireless communications.

# Cyber Ethics in Security Application in the Modern Era of Internet

Megha Sharma\*  
Sanchit Mittal\*\*  
Ankit Verma\*\*\*

---

## Abstract

Societies are becoming more dependent on computer networks and therefore more vulnerable to cyber-crime and internet terrorism. In this paper we have discussed the different ethics of cyber world. In layman terms ethics are the “code of conduct” or the protocols which every responsible citizen should follow while using an internet facility. Here we are mainly concerned with the reasons behind inventing the internet network, and understanding the positive and negative usage of internet, and analyzing the behavior of internet users, and how it affects individual’s life and Indian societies in this modern technical era. Computers raise various problems such as privacy, ownership, theft, illegal use and power. So the main purpose of this article is to provide a glimpse of cyber world including the cyber ethics, cyber-crime and preventive measures to deal with these cyber-crimes.

**Keywords:** Cyber Crime, Cyber Ethics, Cyber Security.

---

## Introduction

In the society where we live, everyone has to accept some kind of rules, values, culture and has to deal with the thinking of people i.e. we need to follow some code of conduct to survive in that particular place. In the same way the ethics in cyber world may referred as the branch of philosophy which deals with values of human behavior, with respect to the rightness and wrongness of certain actions and to the goodness and badness of the motives and ends of such actions. In simple terms Cyber ethics is the philosophical study of a system of moral principles pertaining to computers [1]. In today’s era the internet is growing vastly in terms of its users. Everyone is addicted to the usage of internet, as most Internet users are convinced with its general utility and positive benefits. The internet is

the medium of connecting people through a large worldwide network. Internet has proven tremendously useful in this modern world of technology However, in consequence of the growing internet usage it is leading to some bad or illegal activities such as: cyber stalking, hacking, phishing, cross-site scripting, cyber extortion, fraud and financial crimes. Therefore Measures to protect information systems have received increasing attention as the threat of attacks grows and the nature of that threat is better understood. Among these measures are sophisticated technologies for monitoring computer networks and users, detecting intrusion, identifying and tracing intruders, and preserving and analyzing evidence.

## Internet - A Blessing or A Curse

Internet is a vast computer network linking between computer networks globally. The internet involves educational, governmental, commercial and other networks, all of which use the same communication cycle. The world of Internet today has become a parallel to life and livings. Humans are now able of doing things which were not imaginable few generations ago [2]. The Internet has become a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on the

---

### Megha Sharma\*

Student (BCA) IT  
IINTM, Janakpuri, New Delhi

### Sanchit Mittal\*\*

Student (BCA) IT  
IINTM, Janakpuri, New Delhi

### Ankit Verma\*\*\*

Assistant Professor IT  
IINTM, Janakpuri, New Delhi

machines. Internet has enabled the use of website communication, email, surfing and a lot of anytime anywhere IT solutions for the betterment of human beings. Though, internet offers great advantages to society. It also presents opportunities for crime using new and highly sophisticated technology tools. Regular stories featured in the media on computer crime include topics covering hacking to viruses, web-hackers, to internet paedophiles, sometimes accurately displaying events, sometimes misconceives the role of technology in such activities. Increase in cyber-crime rate has been shown in the news media. The increase in the incidence of criminal activity poses challenges for legal systems, as well as for law enforcement to take active and fast decisions. The internet network has definitely proved a great blessing to the human kind. It should be our responsibility to utilize technology in a positive way to compete with this rapid world. Every coin has two faces. It's up to us to receive well and to leave bad [3].

### Cyber Ethics

Cyber ethics is the study of moral, legal, and social issues including cyber technology. It explores the impact that cyber technology has for our social, legal, and moral systems. It also ascertains the social policies and laws that have been framed in response to issues generated by the development and use of cyber technology. Hence, there is a common relationship [4]. Cyber ethics is a dynamic and complex field of study which considers the interrelationships among facts, observations, experiments, policies and values with regard to constantly changing computer technology. Data processing today is much faster, more flexible, and better arranged and portrayed than ever before in our history. Every technology has introduced not only new opportunity but also new risk. A responsible citizen must follow these cyber ethics to avoid adverse result.

### Cyber Crime

Cyber-crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a technique, or a field of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to comprise traditional crimes in which computers or networks are used to

enable the illicit activity [3]. Internet is certainly the forest of the information and because of its lack of control and restrictions, the Internet aid as a potential threat to society. The various crimes associated with computers are difficult to evaluate in terms of either size or frequency, but it sound safe to say that the number and variety are increasing and the stakes are growing.

### Cyber Crime Variants

There are a large number of cyber-crime variants. A few varieties are discussed for creating the awareness. This article is not intended to expose all the variants hence we have enlightened some of the major issues subjected to the risk in cyber world.

**Hacking.** "Hacking" is a crime. It is the way of gaining unauthorized access to a computer and viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer. In broad terms we can say that hacking is used to describe many complex activities wherein the end goal is typically to obtain access to server, databases or stored files of a computer system [4]. This access may be any combination or desired or undesired, and lawful or illicit.

**Phishing.** Phishing is the attempt to acquire sensitive information such as login id , passwords, credit card information and other personal detail to access someone's account for some reason by masquerading as a trustworthy entity in an electronic communication. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they abide unsuspected that the fraud has occurred [3]. The swindler then has access to the customer's online bank account and to the funds contained in that account.

**Cyber Stalking.** Cyber stalking is the use of the Internet or other electronic means to stalk or harass users. It may include wrong accusations, defamation, slander and libel. It also involves monitoring, identity theft, threats, vandalism, or gathering data that can be used to threaten or harass. Stalking generally involves harassing or threatening behavior that an individual engages in continuously, for example following a

person, appearing at an individual's home or in business organization, making harassing phone calls, or vandalizing a person's property. There are a wide variety of means by which individuals may seek out and harass individuals even though they may not share the same geographic borders, and somewhere it presents a variety of physical, emotional, and psychological results to the victim.

**Cross-site Scripting.** Cross-site scripting, or XSS, is a method of injecting harmful code and links into another safe website's code. It is one of the most commonly used techniques of hacking. As Web browsers have built-in security to prevent a range of XSS attacks, hackers can still exploit flaws or imperfection in the program to convince the browser that planted code is trusted. Examples of such code include client-side scripts and HTML code. The attackers can use an exploited cross-site scripting vulnerability to bypass access controls [5].

**Cyber Extortion.** Cyber extortion is a crime involving an attack or threat of attack against a venture, coupled with a demand for money to stop the attack. Cyber extortion can be of many forms. Originally, denial of service attacks was the most common method. As the number of enterprises that rely on the Internet for their business has expanded, therefore opportunities for cyber extortionists have exploded.

### **Cyber Security – Protect Yourself**

The Internet operates and functions largely on a collaborative basis. Its smooth functioning depends heavily on the proper conduct of users. In this technological era our protection is only in our hands, we should act as an aware and responsible user of this technology [5]. Below we list a set of good practices that make the Internet a better place for all users.

#### **Using webmail wisely**

- Usually the default setting of social networking website is to allow anyone to see your profile. You can change your settings to restrict access to only authorized people.
- Select only trusted and well-known webmail service providers.
- If you use a public computer to check your email. Read the tips that what security points should one

kept in my mind while using a public computer, If an individual access his/her webmail account using a shared computer, remember to remove the data in cache memory, cookies, and other temporary buffer space that might hold your email attachments before you leave the machine.

#### **Be a Responsible Internet User**

As a responsible Internet user, you should protect your system and data with adequate security techniques [4]. An Individual must maintain a Good habit in handling of emails, password management, usage of software, web surfing and downloading files, will help in securing your computer from attack.

#### **Be a Law-abiding Internet User**

- Do not perform any activity which is illicit, fraudulent or prohibited under any applicable legislation.
- Do not publish post, distribute, or disseminate libelous, infringing, obscene, or other illegal material.
- Do not transmit, download or upload data, information, or software in violation of any applicable legislation. It involves, but is not limited to, data protected by privacy and copyright laws.

#### **Self-Awareness for Information Security**

- One should take it as his/her responsibility in keeping own information secure from external misuse.
- An individual should keep equipped with the latest knowledge and must be alert to the news regarding security threats.
- If any person is in doubt, then they must consult advisers or experts.

#### **Handling user accounts carefully**

- Use a password of at least six mixed-case alphabetic characters, numerals and special characters.
- Change your password frequently
- Change your password immediately if you believe that it has been steal by some other person. Once done with making change in the password, notify the system or security administrator for follow up action.

- Always do remember to Log out from your account when finished using public pc, such as in a library.

### **Handling your personal information**

- Make your account and password secure with the available security mechanisms.
- Encrypt/secure the sensitive data when transferring personal information over public networks such as the Internet.
- Always be wary when giving out sensitive personal or account information over the Internet. Banks and financial institutions rarely ask for your personal or account information via email or over the web.

### **Be a Good Neighbor in Internet Community**

- Do not perform any activities which may interfere with other users or restrict or hinder any person from accessing, using or enjoying the benefits of Internet.
- Do not access, use or monitor any data, networks or system, including an individual's private information, without any authority or his/her permission.
- Do not attempt to conduct any network/port scanning or hacking activities on other computers.

### **References**

1. ACM, 1992, ACM Code of Ethics and Professional Conduct, Association of Computing Machinery, USA, October 1992.
2. Chan, Serena and L. Jean Camp, 2002, Law Enforcement Surveillance in the Network Society.
3. Berinato, Scott; "Debunking the Threat to Water Utilities", CIO Magazine, CXO Media Inc., March 15, 2002.
4. Stephanou, Tony; "Assessing and Exploiting the Internal Security of an Organization", The SANS Institute, March 13, 2001.
5. FX, "Attacking Networked Embedded Systems" CanSecWest Conference, Vancouver, May 2003.

- Do not send or distribute links or source of any computer virus, malicious codes or harmful programs.

### **Conclusion**

Internet has been invented for the betterment of humans. Internet has its own boon and bane. However it's our choice to use this invention for betterment of society or to produce harm to others. The ill activities taking place through internet are grouped under cyber-crimes and are also taken care by some cyber authorities by stating some policies, protocols, preventive measures etc. An individual must be aware of cyber ethics i.e, the protocols followed while using an internet network; cyber-crimes, crimes taking place in the cyber world and what are the risks while working on internet; and what are the possible ways to protect ourselves from being attacked by these cyber criminals. Strict penalties must be taken by the law if someone tries to mishandle the use of internet and to harm others for own benefits over internet. Cyber authorities should also aware the people about the threats and what protective measures could be taken. Government should also take remarkable steps towards the criminals indulging in such offences. At a point our protection is in our hands first so must follow the preventive measures and take care of some points discussed in this article to protect yourself from cyber-crimes.

# Comparison of AES and DES Algorithm

Shruti Kumari\*

Gautam Kumar\*\*

---

## Abstract

Cryptography is used for protection of information security. There are various algorithms like DES, RSA, HASH, MD5, AES, SHA-1 and HMAC. DES algorithm is developed by IBM. This algorithm used a 56 bit key to encipher/decipher a 64 bit block of data. In this paper we will compare between DES and RSA algorithm. In ATM DES algorithm is used in live at some place but AES algorithm should be used everywhere, we will also show how AES is better in ATM.

**Keywords:** Cryptosystem, Encipher, Decipher.

---

## Introduction

Encryption is the process of encoding the plaintext into cipher text and Decryption is the process of decoding cipher text to plaintext. There are two types of encryption and decryption technique symmetric key cryptography and asymmetric key cryptography. In symmetric key cryptography sender and receiver both use same key, But in asymmetric key cryptography sender and receiver both uses different key. Symmetric key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithm etc. ,and asymmetric key cryptography includes RSA algorithms[1].

## AES ALGORITHM

AES is created by the National Institute of Standards and Technology (NIST). The algorithm has been developed to replace the Data Encryption Standard (DES). AES is more secure than DES. AES is six times faster Than DES [2]. The algorithm uses three rounds -10,12 or 14. The size are 128,192 or 256 bits according to the number of rounds. Several rounds made of several stages. This algorithm is used to encrypt electronic data. AES is adopted by US but now it is used by whole world. It is a symmetric key algorithm; same key is used for encryption and decryption.

On May 26, 2002 AES became effective as a federal government standard after approved by the Secretary

---

**Shruti Kumari\***

MCA (4th) M.E.R.I. (GGSIPU)

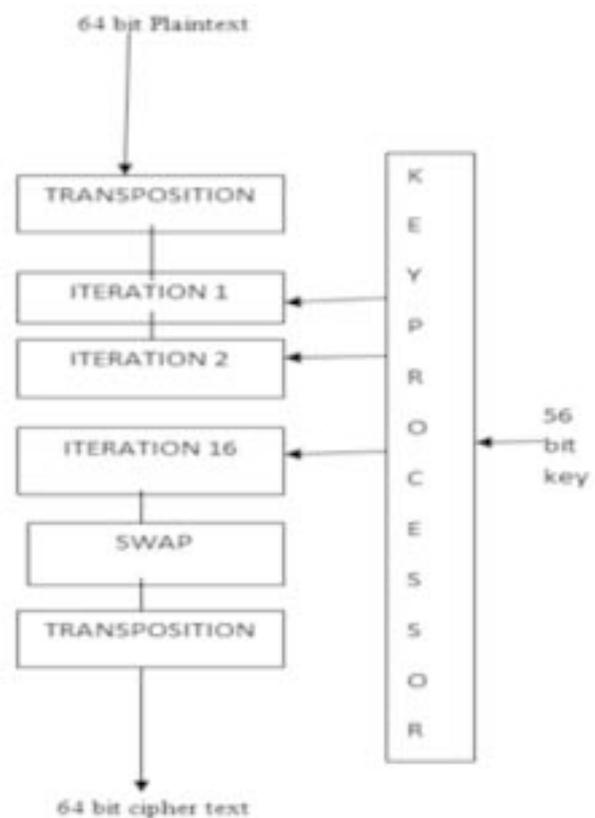
**Gautam Kumar\*\***

MCA (4th) M.E.R.I. (GGSIPU)

of Commerce. AES is found in some other encryption package. [3]

## DES ALGORITHM

Data Encryption Standard (DES) is a symmetric key, developed by IBM This algorithm uses a 56-bit key to encrypt/decrypt 64-bit data. The algorithm is best for



**Figure-1. Encryption/Decryption Technique in DES**

hardware. Key length is too short[4].The key is put through 19 different and complete procedures to create a 64-bit ciphertext.DES has two transposition block and 16 complex blocks called iteration blocks[5].

#### COMPARISON OF DES AND AES

DES is developed in 1977 and AES is developed in 2000.Key size of DES is 56-bit but key size of AE is 128,192,256 bits. Block size of data in DES is 64-bit but in AES is 128-bits.Both are symmetric key algorithm. Speed of encryption/decryption is moderate in DES but faster in AES.Power consumption is low in both. DES is not secure enough and AES excellent secured. Same key is used for encryption and decryption in both. Simulated speed is faster in both[6].

#### *How DES Works in ATM*

ATM uses secret key ,called the PIN key ,to derive the PIN from the account number in terms of algorithm known as DES.The result is natural PIN ,an offset can be added to it and then final PIN which the customer enter. The offset has no cryptographic function, it just used for customer to choose their own PIN [7].

#### EXAMPLE:

Account number: 6693082465987012  
 PIN key:FEFEFEFEFEFEFEFEFE  
 Result of DES:B6AE897C54ECD43A  
 Result decimalized:0665148956702468  
 Natural PIN:0664  
 Offset:4646  
 Customer PIN:5678

Usually DES is use to encrypt the ATM transaction but most of time need more secure triple DES.There are many illegal withdrawals take place from ATM.RossAnderson,a researcher investigated various cases of illegal withdrawals and exposing errors in bank security. There have many cases in which criminals used fake machines, attached keypads or card readers to real machines, and record customer's PIN and bank account details to access the accounts illegally. The algorithm selected as an Official Information Processing Standard (FIPS) for the United States. There are four different mode of operation, these four modes

are Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode and the Output Feedback (OFB) mode.ECB is used for direct application in DES to encrypt/decrypt.CBC is modified form of ECB.CFB uses previous cipher text as an input to theDES to produce output which combined with plaintext ,OFB is same as CFB but in OFB previous output of DES is used as input.

#### *Program for encrypting and decrypting with DES*

```
#include"msp 430xxxx.h"
#include"TI_DES.h"
Intmain(void)
{
  Des_ctx dc1;
  Unsigned char *cp;
  Unsigned char
  data[]={0x24,0xc2,0xa0,0xe7,0x5b,0x6a,0xa3,0x50};
  Unsigned char key
  [8]={0x01,0x15,0x24,0x07,0x17,0x15,0x26,0x18};
  Cp=data;
  De_key(&dc1,key,ENDE);
  DE_En(&dc,cp,1);
  DE_De(&dc,cp,1);
  Return 0;
}
```

#### *How AES is used in ATM*

ATM using DES has been breached 24 hours. Advanced encryption standard (AES)is recent and new encryption algorithm.AES support AES with CBC (cipher block chaining) mode to IP security .[9]

#### Program of Encrypting with AES

```
#include "msp 430xxxx.h"
#include "TI_aes.h"
Intmain(void)
{
  Unsignedcharstate[]={0x64,0x72,0x90,0xb2,0x22,
  0x72,0xa1,0xb6,0xc5,0x5a,0x49,0x28,0x44,0xa0,
  0xc2,0x01};
```

```

UnsignedcharKey[]={0x12,0x06,0x01,0x43,0x72,
0x15,0x15,0x91,0x52,0x21,0x31,0x71,0x26,0x38,
0x45,0x81};
Ae_en_de(state,key,0);
Return 0;
}

```

### *Program of Decrypting with AES*

```

#include "msp_430xxxx.h"
#include "TI_aes.h"
Int main (void)
Unsignedcharstate[]={0x69,0x45,0x87,0x61,0x56,
0x87,0x23,0x54,0x34,0x21,0x41,0x73,0x91,0x61,
0x95,0x14};
Unsignedcharkey[]={0x00,0x11,0x12,0x13,0x14,
0x15,0x16,0x17,0x18,0x19,0x22,0x21,0x24,0x41,

```

```

0x32,0x64};
Ae_en_de(state,key,1);
Return0;

```

### **Conclusions**

Encryption algorithm is very important in communication because it provides security. This paper based on AES and DES cryptographic algorithm technique, how DES at some place used in ATM and AES is more secure than DES so at everywhere in ATM AES algorithm should be used.

### **Acknowledgement**

I would like to thank my faculty, college staff for their abundance guidance and support. Without their cooperation & motivation this research paper won't be possible.

### **References**

1. [www.scholar.google.co.in/21-01-2015/7:00pm](http://www.scholar.google.co.in/21-01-2015/7:00pm)
2. [www.scholar.google.co.in/21-01-2015/9:00pm](http://www.scholar.google.co.in/21-01-2015/9:00pm)
3. [www.scholar.google.co.in/22-01-2015/9:00pm](http://www.scholar.google.co.in/22-01-2015/9:00pm)
4. [www.cryptographyworld.com/des.htm/27-01-2015/4:00pm](http://www.cryptographyworld.com/des.htm/27-01-2015/4:00pm)
5. [www.google.co.in/22-01-2015/8:15pm](http://www.google.co.in/22-01-2015/8:15pm)
6. [www.scholar.google.co.in/22-01-2015/9:00pm](http://www.scholar.google.co.in/22-01-2015/9:00pm)
7. [www.scholar.google.co.in/23-01-2015/10:00pm](http://www.scholar.google.co.in/23-01-2015/10:00pm)
8. [www.google.co.in/23-01-2015/10:45pm](http://www.google.co.in/23-01-2015/10:45pm)
9. [www.google.co.in/22-01-2015/11:00am](http://www.google.co.in/22-01-2015/11:00am)

# Social Networking Security Loopholes

Shelly Taneja\*  
Shalini Rawat\*\*

---

## Abstract

In today's world, usage of social networking is very common through which people feel more comfortable to get connected to others and stay in touch even miles apart by chatting and sharing moments with each other, WhatsApp is among one of such platform. WhatsApp is an Instant Messenger which allows communication between one or more devices through internet without paying a penny for communicating. Almost all mobile platform namely Android, iPhone, BlackBerry, Windows, Nokia S40, Symbian users can easily use this application. It allows you to exchange messages, videos, audios, and images.

WhatsApp is an excellent tool to exchange ideas but at the same time proving harmful to its users. As people are getting more addicted to WhatsApp application they get into the trap of security pitfalls due to the heavy usage of it. This research paper tells about the concerning security pitfalls of WhatsApp.

**Keywords:** Social Networking, Instant Messaging, WhatsApp, Facebook

---

## Introduction

Social network plays a vital role in today's world to build social connections or relations among people who have common interests or activities. The concept of social networking with the growing age of internet has taken a complete changed shape in the form of social networking websites, instant messengers, and voice over internet etc. Among those WhatsApp is one of fastest growing instant messenger.

WhatsApp is a Cross-platform application through which user can transfer their messages to one another or can communicate with each other. WhatsApp provides various features like text messaging, sharing audio, video, voice notes, location, group chats and so on. Location can be known by using the Location and Map Services provided by the different OS'es. Despite of these things, privacy is the major issue which affects the user.

In India 76% of smartphone users use only WhatsApp as Instant messenger. This messenger has no restrictions on the length of a message and also you don't need to put a SIM card on a phone but you should have a smartphone or a supported phone with internet

connection and available storage space to use this messenger application.

There are certain advantages of using this application are:-

1. It does not cost, not even a penny for sharing texts and other related things.
2. It takes a less storage space, even smaller than normal application and games.
3. Convenient to get connected with many friends at the same time by starting group chat on WhatsApp.
4. One can broadcast a message to several people at the same time.
5. Sharing of Voice Notes, audio video files, images are made possible through WhatsApp.

On March 31, 2013 the Saudi Arabian Communications and Information Technology Commission (CITC) issued a statement regarding possible measures against WhatsApp, user cannot block contact on whatsapp as well as no feature of friend request.

In November, Whatsapp comes up with a new feature known as Read Receipts which alerts senders when their messages are read by recipients. Within a week, The public authority for data privacy of the German state of Schleswig-Holstein has advised against using

---

**Shelly Taneja\***  
M.E.R.I, GGSIPU  
**Shalini Rawat\*\***  
M.E.R.I, GGSIPU

WhatsApp, as the service lacks privacy protection such as end-to-end client side encryption technology.

Recently, WhatsApp has launched a web based WhatsApp application. It has been released only for android for now and as a plugin for google chrome browser.

With some good there's always a bad side, WhatsApp is also a no exception. There are some security issues and pitfalls with WhatsApp instant messenger application which is proving to be harmful for the users round the world.

### **Impact of Social Networking Platform**

Social networking platform has become a most significant part of our society.

It has integrated with our communication medium and extended our social interactions. People who feel shy interacting face to face with one other, feels great while interacting with each other over these platforms. They without hesitating share their perspectives and thoughts.

It allows people to communicate easily and enormously, irrespective of time and distance.

It has following impacts:

- Social Networking has emerged as a voice if common people throughout the world.
- It has created a wide interaction of people with instant communication between people anywhere anyplace and anytime.

### **Whatsapp**

WhatsApp is an alternative for SMSs, which are once very popular among the youth, this application software is a pun on "what's up". It has been developed targeting mainly the smartphone users with an internet connection.

It is one of the social networking platform giant which has very user friendly features and possess the ability to run on multiple platforms like iPhone, BlackBerry, Android, Windows Phone and Nokia smartphone.

### **How it grew up**

WhatsApp came up with a broad vision and emerged as a great deal for the smartphone users besides all

other SMSs alternatives like BBM, TELEGRAM, WeChat.

There are over 400 million users of WhatsApp proving it as the best SMS replacement technology and platform. The issues faced by the users in any other social networking platform is eliminated by WhatsApp in a very better and easy to use manner.

The excitement of using WhatsApp results in sudden boom of smartphone sale in Asia-Pacific region, especially in India.

The drastic growth in use of WhatsApp made the Mark Zuckerberg, founder of Facebook Inc., to acquire it, with a \$19 Billion valuation.

With this move he cemented himself as the global leader in mobile media by using a very unique acquisition strategy. Even after the acquisition, WhatsApp seems to be growing at very good rate all over the globe. Benefits of WhatsApp are:

- WhatsApp provides us with sharing messages, pictures, audios, vedios in just a one go without charging a single penny.
- Provides with group message where one can interact with more than one people at the same time.
- It also facilitate users with message broadcasting.
- Good marketing mode: Now a days many organisations and individuals like politicians are using it as a marketing tool for promoting themselves.

### **Survey on Whatsapp**

From Survey, data has been collected from US, Brazil, China, South Africa, and Indian Smartphone.

As shown in above fig, Survey says that 43 per cent users use Whatsapp in India and just 35 per cent use Facebook Messenger used in US.

### **Security in Whatsapp.**

WhatsApp requires a microSD card storage to store its data on the users' phone. After WhatsApp installation, it synchronizes with the phone's contact showing users who have a WhatsApp account associated with their number.



**Figure 1. Usage of Whatsapp in Different countries. [4]**

When a mobile with WhatsApp installed is turned on, “com.WhatsApp” process receives a signal to start the “ExternalMediaManage” and “MessageService” services which runs in the phone’s background till the phone is turned on.

Exchanges messages are stored in ‘msgstore.db’ i.e, SQLite database. Researchers found in earlier version of WhatsApp this was the main security concerns. When news hits internet, security researchers started researching with Whatsapp database (msgstore.db) to



**Figure 2 Average monthly Whatsapp usage per active user. [4]**

retrieve the conversation even the deleted ones from the chat option. But Whatsapp reacted soon and came up with an encryption mechanism to protect its database.[1]

### Whatsapp Flaw can Expose your Messages in a Minute

Users must be careful while downloading WhatsApp. User should read an application permissions carefully before installing it, your messages history could access by others.

There is a trick which provides granting access to database. Since, WhatsApp have criteria to store their messages into microSD card, applications can access all messages if permission is granted.

The Netherlands-based technical consultant says that, if screenshots contain code and added to Android games, it is easy to retrieve data from a database.

According to Thijs Alkemade, a computer science and mathematics student Utrecht University in the Netherlands, WhatsApp send as well as recieved messages are encrypted with the same key, means if hacker can intercepts all messages, he or she can easily analyze them to cancel out the key and recover the plain text.[9]

### Issues Related to Whatsapp

#### General Issues

- **Anyone can contact you over WhatsApp:** WhatsApp uses mobile numbers as the unique ID. Setting up WhatsApp is a easy task. Once you set up your WhatsApp account you are automatically shown into the list of WhatsApp contacts of who so ever is on WhatsApp and has saved your number in their mobiles. So it becomes more easier for anyone to contact you without seeking your permission which sometimes may results in bullying or harassing anyone over whatsapp.
- **No much security required:** Operating WhatsApp doesn't required any password, it doesn't provides any password security to secure it from other users.
- **No permission for contacting or adding in a group:** Before adding into a group no notification

or request is received, which may lead to become a part of a unwanted group. Though one can delete and exit the group but chances of distributing of your number among unknowns and unwanted people are same and later those unknowns of the group may bother you by contacting you over WhatsApp as anyone can contact anyone over WhatsApp just by your WhatsApp numbers.

- **Anyone can view your mobile number and profile picture:** If you are a part of any group consisting of some of the unknown people too, then they can view your numbers and can even see your personal data like profile picture & status if unknowingly you have set privacy to public.
- Sometimes there may be people who are saved in your contact lists and to whom you don't wish to show your profile pictures in this case there is no option of customise your privacy settings.

#### Network Issues

- **Chat backup on their servers:** WhatsApp automatically generates backups every day at 4 AM and stores them in the WhatsApp folder of your Android phone. This folder is either located in your device's internal memory or external microSD card. It may restores less recent or most recent backups only, for this you have to uninstall and reinstall WhatsApp. They can get to read chats. If ever their server gets hacked your data might be stealing and could be misused.
- **Man in middle attack:** The hackers can easily get to read one's personal chats and data if they can get into server through Man in the Middle attack on server and as encryption and decryption keys are same as used by Whatsapp they can easily decrypt the data.

#### Psychological issues:

- It has decreases the self-esteem among the people and increases the psychological disorder.
- People are getting divorced: Introducing of second tick, blue tick (when read) results into fights and raised misunderstandings when people didn't get replies.

## Remedies

Intelligent use of WhatsApp may reduce these psychological or to some extent these network related issues and the other concerning issues.

Also WhatsApp developers must provide with more strong security and privacy features which can protect one's privacy and personal data and other contents.

## Conclusions

The social networking is growing and it is somewhat good to people in general as it provides with true meaning of freedom of speech and expression, but in some ways it is also harmful too. So one should use this platform for his own good but with a cautious mind that these can also hamper one's privacy and can get into the personal life without the permission of the users.

WhatsApp though on one hand is a good tool to communicate with everyone around the globe and

provide a best and cheapest way for the messaging, but at the same time it is also not away from the drawbacks which one should keep in mind while using. One must be capable enough to protect its privacy and personal wellbeing, without that there won't be much use of such platform.

So, while using such application one must be cautious enough to know that what sort of data they are sharing with the developers and how they will be using it to intrude in the personal life.

## Acknowledgement

I would like to thank Ms **Navneet Popli**, my family & friends for their support and guidance while going through this research.

I would also like to thank my other faculty and college staff and members who keep me motivated throughout the research.

## References

1. Mr. Shubham sahu "An Analysis of whatsapp Forensics in Android Smartphones".
2. Pranav Dixit "Backup whatsapp to keep your precious messages forever".
3. Business Insider India- "Hackers claims this crucial whatsapp flaw can expose your messages in minutes".
4. "Customer satisfaction towards Whatsapp- a" project report(30-01-2015, Friday, 8.55 pm) .
5. Forouzan "Data Communication and Networking", Fourth Edition..
6. Tanenbourn."Data communication and Communication", Fifth Edition..
7. <http://en.wikipedia.org/wiki/WhatsApp>.
8. [https://www.google.co.in/?gws\\_rd=ssl#q=social+networking+sites](https://www.google.co.in/?gws_rd=ssl#q=social+networking+sites).
9. Sebastian schrittweise, "Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications".
10. <https://www.WhatsApp.com/>
11. <http://alkarbalacia.net/top-3-advantages-of-using-WhatsApp-to-send-free-text-messages/>
12. Johnson yeboah, "The impacts of whatsapp messenger usage on students performance in tertiary institutions in Ghana".
13. WhatsApp web version Released:chrome plugin,android,blackberry, and windows phone.

# Cloud Computing: Vulnerabilities, Privacy and Legislation

Amit Kiran\*

Priyam Lizmary Cherian\*\*

---

## Abstract

Cloud computing is an indispensable part of the current business and service industries, its usage raising many issues. These issues range from those intrinsic to the nature of cloud itself and those stemming as a result of inability of the legislature to keep up with the dynamic nature of technology. This paper discusses the nature of conflicts and issues that may arise in providing cloud services. Starting with the possibility of security threats to cloud computing, the paper discusses the overlap of cloud services with intellectual property. It further looks at the legal regime for protecting and regulating cloud related activities. The need for standards and best practices is also reviewed. The paper concludes with a call for regulatory reforms both at a national and international level.

**Keywords:** Cloud Computing, Data Breaches, Green grid

---

## Introduction

In its simplest form, cloud computing maybe said to be the infrastructure provided in the form of computer resources over a network connection, typically the internet, which is determined by the needs of the end user. The National Institute of Standards and Technology define cloud computing as, ' a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'[1]. In essence, cloud computing involves self-service, commonly pooled resources, broad network access, elasticity of use and a measured service. Normally, while this service may exist in many forms, it is most commonly used as Software as a Service (SaaS), where programs operating on cloud software are provided to clients, Platform as a Service

(PaaS), where the client is allowed to develop software or programs that operate on the cloud services, and Infrastructure as a Service (IaaS), where processing, storage, networks, and other fundamental computing resources are provided for the use of the client. Cloud computing might exist as a private cloud, a public cloud, a hybrid cloud or as a community cloud.

On analysis of cloud computing in its current form, it is clear that many difficulties exist in its regulation, control and classification. For example, servers hosting cloud computing might not operate in the same country as the client themselves, thereby limiting the territorial jurisdiction of the country in regulating and safeguarding such services. Further, while cloud computing is regulated by the standards set by the country hosting such services, offences or breaches of protocol in any other country cannot be contested without a treaty between the countries or a clause in the contract between the parties that specifically deals with the issue of jurisdiction.

Cloud computing is indispensable as most businesses and service providers as well as all online transactions primarily rely on cloud based computing services for any transaction or interface on an as per need basis. In this light, the problem of security in cloud computing is pivotal, as any breach would lead to the loss of crores of rupees (with the value of cloud computing predicted

---

### Amit Kiran\*

5<sup>th</sup> year, B.A. LL.B.

University Law College, Bangalore

2, 5<sup>th</sup> Cross, P&T Layout, Horamavu, Bangalore

### Priyam Lizmary Cherian\*\*

3<sup>rd</sup> year, LL.B.

Faculty of Law, University of Delhi

1989, Outram Lines, Kingsway Camp, Delhi

to be 5 percent of the total investments in India by 2015[2]), with little or no possible legal recourse.

### Security Threats to Cloud Computing

According to the Cloud Security Alliance, the top threats in cloud computing are as follows[3]

- Data Breaches- where sensitive and valuable information is gained by parties who have access to such software.
- Data Loss – of valuable data through malicious processes or physical destruction of such hosting servers.
- Account or Service Traffic Hijacking – through the use of the security clearances or credentials of actual parties to gain unauthorised access to information.
- Insecure interfaces and Application Programming Interfaces – flaws in the basic interface systems would lead to various security issues.
- Denial of Service – by the actions of malicious third parties so as to delay the delivery of any cloud service or increasing the cost of such services.
- Malicious Insiders – where due to improper configuration of cloud services system administrators are allowed unauthorised access to the sensitive data of customers.
- Abuse of Services – by using cloud services, such as computational power, to facilitate hacking of servers or for the distribution of pirated software, etc.
- Insufficient Due Diligence – leading to a lack of internal controls and in the case of breach of contract, ambiguity in its enforcement.
- Shared technology vulnerabilities – with the use of software by customers where any breach in the software could lead to a breach of the entire cloud based system.

### Intellectual Property and Cloud Computing

In the process of uploading and storing data on the cloud, there is a possibility of creating new Intellectual Property. For instance, in the service model of PaaS, the consumer may create applications using libraries

and tools supported by the provider[4]. In absence of any clause to this effect, it would be difficult to determine who would be the author/owner of the patentable or copyright work that is created on such a platform. A clear claim in the contract(for instance clause 5 of Dropbox business agreement expressly provides that Dropbox would not have any intellectual property in the consumer data)or assignment of copyright would help in determining the ownership over the/any newly created work.[5]

Primarily, the work that has already been created and thereafter placed on the cloud may indicate clear ownership of the author, i.e. the cloud service user.

While acting as a platform for exchange and storage of huge amounts of data, the cloud service providers are constantly running the risk of storing infringing material. The service providers in such situations are often protected under the safe harbour provisions. In cases where the cloud services provider allows recording and storing of content that may infringe the copyright of a third party, any liability would depend whether the country's statute allows copying for personal use or grants time-shifting exceptions under its copyright laws. (an example is Section 111 of Copyright Act, 1968 of Australia which provides that any recordings made for domestic use and to be viewed or heard at a later time does not infringe the copyright in the work) [6]

An IP owner needs to keep a constant check and be aware of possible loss of confidential data stored on cloud as a result of data mining. Clearly defining and demarcating the confidentiality obligations of the service provider, the customer and other third parties thereby becomes imperative.

### Legislation

In India cloud providers can be held liable for any illegal data that they might host, however this is limited to cases where it can be proved that the provider was aware of the 'illegal nature of the data' hosted, and have not taken any steps to limit or remove such data, even when they were made aware of such an infringement. India is currently not a signatory of the Budapest Convention of Cyber Crime[7]; a pivotal international treaty which overruled the principal of

location as a connecting factor from a legal perspective, thereby weakening our position on the matter.

Excluding the provisions of the Indian Contract Act, 1872 the only legislation that governs cloud computing in India is the Information Technology Act, 2000. This Act contains four provisions that specifically deal with breach and misuse of data. Section 43 protects the owner of the computer /computer system/network/ resource from any damage to computers or computer systems with regard to unauthorized copying, extraction, database theft, and digital profiling. In case of cloud services, the owner can be the consumer using the services of the Cloud Service Providers (CSP's). Section 65 protects the cloud service users against the tampering of computer source documents. Such an act is punishable by either or with a combination of a fine up to two lakh rupees and imprisonment up to three years.

Section 66 of the Act deals with computer hacking and protects users from intentional alteration/misuse of data on their computers. The penalty is the same as that for Section 65. Section 72 imposes a fine of one lakh rupees and an imprisonment term of up to two year for any breach of confidentiality or misuse of private data.

These provisions have been widely interpreted by Courts to cover most of the cases involving breach of security or violation of privacy with regard to cloud based computing. However, the absence of specific laws governing cloud computing and the lack of a strong supervisory role of the Telecom Regulatory Authority of India (TRAI), leaves much to be desired. While protection is mentioned in the form of penal liabilities, it is wholly insufficient inasmuch that the economic loss that caused by such infringement is far more severe. In this light, the current legislative regime as it lies is wholly insufficient in dealing with the issues of regulation, protection and supervision of cloud based services and the problems that exist or may arise in its functioning.

### **Cloud Computing Standards**

A plethora of players in the sphere of cloud computing offer varied services. The different terms and standards of these services often pose difficulties to service

adopters in migrating to other CSP's, integrating data and applications over CSP's or maintaining effective audit processes across service providers. The lack of a standard in cloud computing not only poses serious questions on interoperability but also creates hurdles at the initial stage of comparing and evaluating the cloud services.

These incompatibilities in transition are broadly categorised as [8] –

1. Technical
2. Business
3. Semantic

*Technical:* This aspect is related to the reliability and security issues associated with the cloud services. The security related cases in interoperability may include user authentication in cloud, data access authorization policies, and user credential synchronization between enterprises and the cloud. [9]

*Business:* This may be associated with unavailability/ want of a standard interface that may provide audit or assessment of the environment.

*Semantic:* It refers to portability and interoperability of CSP's. Interoperability means the ability to communicate with entities to share specific information. Portability on the other hand is the ability to migrate workload and data from one provider to another.

One would assume that transfer and interoperability would be facilitated by setting out one uniform standard. The present scenario suggests otherwise. Instead of collectively creating a single definitive regulation, the top organisations seem to be suggesting their own set of norms.

There are more than 30 standardisation initiatives from around 20 organizations. These initiatives range from The Institute of Electrical and Electronics Engineers Standards Association's P2301 [10] and P2302 [11] working groups looking at standardisation in cloud management and interoperability to the National Institute of Standard and Technology's Cloud Computing Standards Roadmap [12] advocating best practices and standards. Other organisations that have proposed best practices for use of cloud computing

include The Green Grid, The Cloud Security Alliance, The Distributed Management Task Force, The European Telecommunications Standards Institute and The Storage Network Industry Association.

In October 2014, International Organization for Standardization (ISO) also released new standards for cloud computing [13]. These set of rules are said to have seven distinct cloud services categories including Network as a Service (NaaS) and Data Storage as a Service (DSaaS) as opposed to the three categories identified by NIST (as discussed above) [14].

These varied and overlapping standards seem to be further delaying creation of a uniform practices.

### Conclusions

On analysis of the current legislative regime on cloud computing in India, it is clear that there are lacunae that need to be addressed in order to strengthen the security and regulation of Cloud Services in the interest of protecting sensitive data and the privacy of the users. Such reforms are a double edged sword as they must be strict enough to ensure compliance and liberal enough not to discourage companies from using cloud services.

There must be a greater involvement of the TRAI in line with the National Telecom Policy [15]. The TRAI in governing Internet Service Providers (ISP's), can ensure the co-operation of the ISP's in preventing such breaches in privacy, security or violation of any intellectual property rights, a necessary action in the light of voluminous online traffic.

### References

1. Peter Mell and Timothy Grace, "The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology", *National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145*, p.2
2. Shipla Shanbag, "Emerging from the Shadows," *Dataquest*, Vol. XXIX No. 10, May 31, 2011 at 22.
3. "The Notorious Nine: Cloud Computing Threats in 2013", *Cloud Security Alliance*, February 2013, p.6
4. Mell & Timothy, supra note [1] at p. 2
5. Dropbox Business Agreement- [https://www.dropbox.com/terms#business\\_agreement](https://www.dropbox.com/terms#business_agreement) [February 12, 2015]
6. Copyright Act, 1968- <http://www.comlaw.gov.au/Details/C2014C00291> [February 12, 2015]
7. Gowri Menon, "Regulatory Issues in Cloud Computing: An Indian Perspective", *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, Volume 2, No.7, July 2013

In the absence of clear contractual terms, disputes may arise over accountability of data and its security. Though the Information Technology Act can be of help in cases of any data security breach, ambiguous terms of contract may lead to complex issues when the data is being used by the CSP's for their management and development. Provisions for notification on any breach, and smooth transfer of data on termination of services can also be some aspects that may be considered in the contract of service.

The next big leap in the regime of interoperability of cloud service is definitely the creation of one determinate standard of operation and services. The multiple, overlapping standards proposed are adding to the numerable drafts. The need of the hour is for the stakeholders to come together under one umbrella and adopt one single standard that may be used by the CSP's worldwide. An international treaty setting minimum standards for cloud service could be the way forward for solving the issues surrounding jurisdiction, and interoperability.

The Cloud is increasingly changing the way enterprises are modelling their innovation and development strategies. With its on demand access, elasticity to meet varying demands and its dynamic nature, cloud has redefined the IT and business sectors' operations. The increased subscription to CSP's is a clear indicator of the sailing future of clouds. To avoid any turbulence, the Indian legislature needs to fill the lacunae and make appropriate provisions facilitating trade and transactions over cloud in order to deal with any current or novel issues that are bound to arise.

8. RajinderSandhuand InderverChana, “Cloud Computing Standardisation Initiatives: State of Play”, *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.2, No.5, October 2013, pp. 351-362 ISSN: 2089-3337
9. Grace A. Lewis, “The Role of Standards in Cloud Computing Interoperability”, Software Engineering Institute, Technical Note CMU/SEI-2012-TN-012, October 2012, Carnegie Mellon University
10. Guide for Cloud Portability and Interoperability Profiles-<http://ieee-sa.centraldesktop.com/p2301public/> [February 12, 2015]
11. Standard for Intercloud Interoperability and Federation-<http://grouper.ieee.org/groups/2302/> [February 12, 2015]
12. NIST Cloud Computing Standards Roadmap -[http://www.nist.gov/itl/cloud/upload/NIST\\_SP-500-291\\_Version-2\\_2013\\_June18\\_FINAL.pdf](http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf) [February 12, 2015]
13. Standards Catalogue -[http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_tc\\_browse.htm?commid=601355](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=601355)[February 13, 2015]
14. ISO publishes new cloud computing standards and definitions-<http://www.cloudcomputing-news.net/news/2014/oct/20/iso-publishes-new-cloud-computing-standards-and-definitions/>[February 12, 2015]
15. National Telecom Policy,2012-<http://www.trai.gov.in/WriteReadData/userfiles/file/NTP%202012.pdf> [31.01.2015]

# The Exigency in Accretion of Cyber Warfare Legislation

Raman Solanki\*  
Ankit Verma\*\*

---

## Abstract

Recent advances of internet over the two decades of more than two billion users. The expansion resulted in developing applications for the cyber world, which bolster further expansion and more applications. To compute to the rise of a cyber-economy, commercial transactions and accentuating in the storing and sharing of hypersensitive information. Storing of sensitive information on networks eventuated to cyber espionage against the government and cyber economic warfare against the businesses and the need of the legislation dealing with newly developed cyber laws came into existence.

**Keywords:** Cyber Attacks, Web Vandalism, Legislation, laws, Disavowal of service

---

## Introduction

Cyber warfare is delineated as a major interruption to critical infrastructure, despite it is the least liable-result. Assaulting an outland via the internet has an intense chain-reaction also a collateral global damage. Cyber warfare occurs continuously across cyberspace connections giving rise to minor disruptions, website vandalism, heist of national defense information, and rational property defraudment. We are on the point of a considerable bend in the attribute of warfare as military-competition bolsters into the cyber field. Characteristically, it reconnoiters concerns among senior-policy builder and leaders of the military in extensive cyber powers that their non-state and state adversaries to execute-prompt cyber defilement that could administer adversity on their rivals to give rise to catastrophic level of destruction on the cyberspace. The credible targets of cyber-attacks are the power grid, financial sector, energy reservoir (gas and oil pipelines) and communications [1]. The increasing dependence on information structure in generic and connections to the Internet in minute, hypercritical infrastructure is augmenting more liable to cyber-attacks. Leaders

---

### Raman Solanki\*

Student (BCA)  
IITM, Janakpuri, New Delhi-110058

### Ankit Verma\*\*

Assistant Professor  
IITM, Janakpuri, New Delhi-110058

around the globe have embodied concerns of the exigency of cyber “Unforeseen Attacks” are developing. Cyber Weapons’ possibility to oversee damage to that of Nuclear weapons is valid. The Legislations ought to safeguard its populace from these virtual weapons of mass-destruction of the economy and the information by enforcing and updating laws [2].

## Types of Cyber Attacks

The use of Information-Technology and computers to complete acts of war on the government and large scale framework is the true delineation of cyber-attacks. The assailant of cyber-attacks can be a definite person, a formulation, or another government. There are many different forms of cyber-warfare from specialized-hacking jobs on an unambiguous server to the conventionally targeted denial of service attacks. The definitive in cyber-attack is a blitzkrieg that completely abstracts the dexterity for all of the members of the government and the organization to connect to the internet. The adversaries are so clever even when one method gets done then they are ready with their other method to add to the destruction. The most commonly used methods for Cyber Attacks are Web Vandalism and Disavowal of Service Attacks.

### *Web-Vandalism*

Web-Vandalism is characterized by website disfigurement and denial of Service invasion. Website defacement is the most quotidian contour of web

**Table 1: Webserver**

	<b>2005</b>	<b>2006</b>	<b>2007</b>
Apache	308	486	319
IIS/6.0	72	181	114
IIS/5.0	100	66	24

**Table 2: Operating System**

	<b>Linux</b>	<b>Windows</b>
2009	276	180
2010	446	258
2011	306	140

vandalism; Website-defacement is an imperative threat to many internet-facilitated businesses. It hostilely affects the public image of the Organizations. Organizations may suffer from loss of important data, trust of people and business. The following are the steps on how website defacement works [4].

- The number one step would be to search for a username for instance strutting as administrator and calling an employee; the administrator information can also be fetched from a Whois database.
- Using various executions such as brute-force, the password can be salvaged.
- As one has the access to the administration access, the next step will be to annex administrative privileges.
- Ensconcing a backdoor; the defacing of the website may begin.

#### **How to defend against website defacement?**

- Avoid using the server as a client (e.g., web browser)
- Remove buffer overflow vulnerabilities in your programs.
- Use a different user(s) other than root for managing the website contents.
- Enable access logs.
- Update.

Web vandalism is not only present in the United States. It is also a problem in many other countries particularly Kyrgyz. The published statistics of registered website defacements every year is given in the table. The following tables are subset of those statistics:

#### **How to recover from website Vandalism and avoid future defacements?**

- Change all user passwords, if the web server provides user-authentication, and you have evidence/reasons to think the passwords may have been compromised. This can require a large user communication.
- If backup server has been used, restore the primary web server component as nominal

#### *Disavowal of Service*

The disavowal of service malicious deed is an attempt to exhaust all of an available contrivance in order to keep those resources from its contemplated end-users. The disavowal of service is one of the most banal blitz upon the internet done by the attackers. Its use is so outspread because it is comparably accessible to implement and it is very arduous to defend-against. Conventionally an assailant-builds an alluvion of ersatz requests to a service, scorning the results. The server is bogged-down by huge number of approaching requests, taking long times to haft both the fraudulent requests and any licit requests that come in during the attack. In supreme cases, the server will not be able to haft the strain of the approaching-connections and will

crash, enduringly breaking the server until it is manually renewed. A disavowal of service attack may subsist of an entreaty which is crafted to coup a specific vulnerability in the server, inciting it to crash without coercing a large number of requests. The assailant-sends request from more than one system making it a distributed disavowal of service attack (DDoS). A disavowal-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. A DoS attack can be perpetrated in a number of ways. Attacks can fundamentally be classified into five families:

- Consumption of computational resources, such as bandwidth, memory, disk space, or processor time.
- Disruption of configuration information, such as routing information.
- Disruption of state information, such as unsolicited resetting of TCP sessions.
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

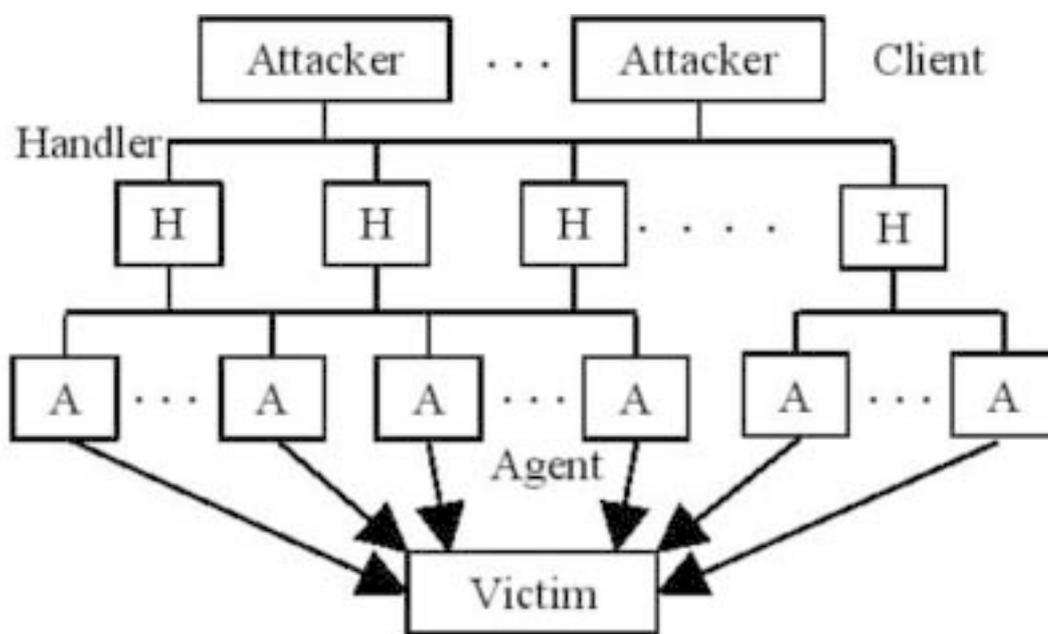
A DoS attack may include execution of malware intended to:

- Max out the processor's usage, preventing any work from occurring.
- Trigger errors in the microcode of the machine.
- Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
- Exploit errors in the operating system, causing resource starvation and/or thrashing, i.e. to use up all available facilities so no real work can be accomplished or it can crash the system itself
- Crash the operating system itself.

In most cases DoS attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and

to prevent filtering of the packets based on the source address. Two types of DDoS attack networks have emerged: the Agent-Handler model and the Internet Relay Chat (IRC)-based model. The Agent-Handler model of a DDoS attack consists of clients, handlers, and agents (see Figure 1). The client is where the attacker communicates with the rest of the DDoS attack system. The handlers are software packages located throughout the Internet that the attacker's client uses to communicate with the agents. The agent software exists in compromised systems that will eventually carry out the attack. The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents. The owners and users of the agent systems typically have no knowledge that their system has been compromised and will be taking part in a DDoS attack. Depending on how the attacker configures the DDoS attack network, agents can be instructed to communicate with a single handler or multiple handlers. Usually, attackers will try to place the handler software on a compromised router or network server that handles large volumes of traffic. This makes it harder to identify messages between the client and handler and between the handler and agents. In descriptions of DDoS tools, the terms "handler" and "agents" are sometimes replaced with "master" and "daemons", respectively.

The IRC-based DDoS attack architecture is similar to the Agent-Handler model except that instead of using a handler program installed on a network server, an IRC (Internet Relay Chat) communication channel is used to connect the client to the agents. An IRC channel provides an attacker with additional benefits such as the use of "legitimate" IRC ports for sending commands to the agents [4]. This makes tracking the DDoS command packets more difficult. Additionally, IRC servers tend to have large volumes of traffic making it easier for the attacker to hide his presence. Another advantage is that the attacker does not need to maintain a list of the agents, since he can log on to the IRC server and see a list of all available agents [4]. The agent software installed in the IRC network usually communicates to the IRC channel and notifies the attacker when the agent is up and running. In an IRC-based DDoS attack architecture, the agents are



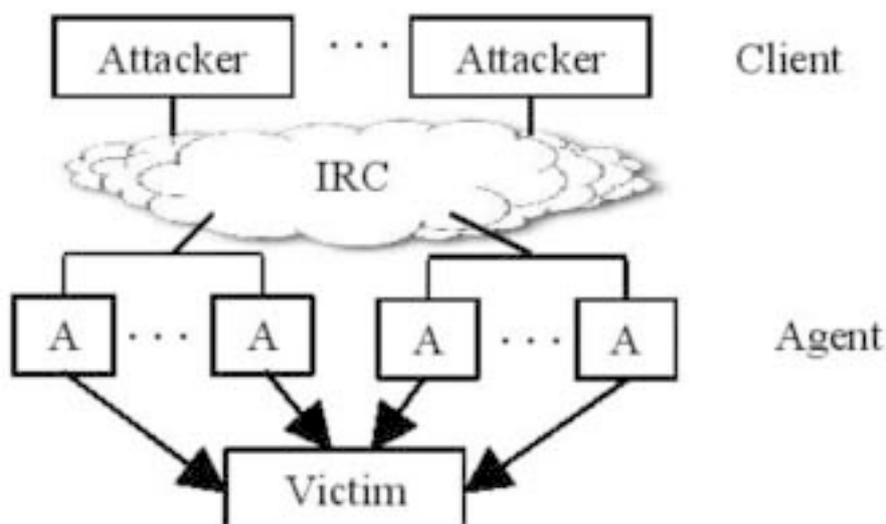
**Figure 1: DDoS Agent-Handler Attack Model**

often referred to as “Zombie Bots” or “Bots”. In both IRC-based and Agent-Handler DDoS attack models, we refer to the agents as “secondary victims” or “zombies”, and the target of the DDoS attack as the “primary victim”. Well-designed agent software uses only a small proportion of resources (memory and bandwidth) so that the users of secondary-victim systems experience minimal performance impact when their system participates in a DDoS attack.

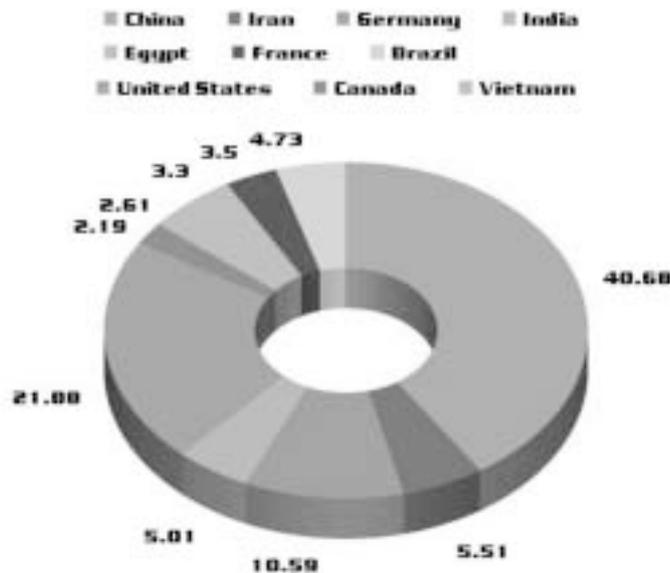
The following pie-graph represents the top source countries for Distributed Denial of Service Attacks [6].

**Cyber Warfare Legislation**

Various countries use various legislatures for protecting or advancing Cyber Warfare. It varies from enrooting, maturing a stratagem, to be oblivious to certain attacks. Disparate nations affiliate different approaches



**Figure 2: DDoS IRC-Based Attack Model**



**Figure 3: Top Sources for Distributed Denial of Service Attacks**

to the cyber espionage and sabotage conducted by the assailants' government-forces; Myriad nations don't have a legislature to hedge their populace from these cyber-war and attacks by their assailants' government forces. Different zones in the world have different laws to treat and react against/for Cyber-attacks and the laws are necessary to safeguard people from various techniques of cyber-attacks.

**EMEA**

The Middle East, Africa and Europe, the cyber-warfare attacks have been comparably less than the other two time zones. Various Countries in this time zone don't even have a legislature to guide or bulwark from cyber warfare or attacks, The United Kingdom of Great Britain and Northern Ireland, to foster their networks also ordained cyber war games dubbed 'Waking Shark 2' to hedge their financial-organizations followed by the Wall-street. Britain has also endowed up a cyber-security and "operations-center" based in Government Communication Headquarters (GCHQ). The Police and Justice Act 2006, of the United Kingdom, amended the Computer Misuse Act 1990 and specifically outlawed disavowal-of-service attacks and set a maximum penalty of 10 years in prison Germany; the German Law gives the right to the German agencies to cyber scrutiny capability to twenty percent of total internet traffic [8]. Netherlands has various centers to

support scrutinizing eye on the other networks ranging from National Cyber Security enter (NCSC), Joint IT branch (JIVC), Joint Signet Cyber Unit (JSCU) and Defensive Cyber Command (DCC), these clutch of various agencies have been set up by many other countries of this time zone.[9] The Europe has also entrenched ENISA (European Union Agency for Network and Information Security) The governmental agencies in this time zone have opened up to protect themselves from these unforeseen- cyber-attacks than just military [8-9].

**APAC**

The Asia-Pacific region has been the origin or the most cyber-attack-bearer than any other time zone because of its size and new developing economy and rivalries; this has been the major hotspot for Cyber Attacks also the inducement of these acts of war. China has been the most controversial country when referring to the origin of Cyber Attacks, China is gripped culpable for a twine of Cyber-attacks on numerous private and public institutions in countries ranging from France, Russia, Canada, India and the United States of America; the Chinese government disclaim any involvement in these campaigns and they believe that they are not the hazard but rather the victim of an rapid increasing number of Cyber-Attacks. The Chinese government uses-New space based intelligence

gathering systems and surveillance systems, infrared decoys, false target generators and anti-satellite systems. They have been information zing their military through increase educations of military person in Cyber Warfare, developing the information network for military training and have digital campuses and libraries for advancement [10]. Under Section 27A and section 161, the Chinese government is protecting and also includes imprisonment against unauthorized access to computer by telecommunication extended by Article 285,286,287. The Korean Peninsula has also been the victim and the impel of Cyber Attacks, North Korea is aggrandizing its workers through military academics specializing in hacking and other forms of Cyber-Warfare. During the military dictatorships of Park Chung-hee and Chun Doo-hwan (1961-1987), anti-government speech was frequently suppressed with reference to the National Security Act (NSA, 1948) and the Basic Press Law (1980). Although the Basic Press Law was abolished in 1987, the NSA remains in effect. The government has used other “dictatorship-era” laws in order to prosecute critics in contemporary contexts; [11] India is also-the sufferer and antecedent of various sponsored Cyber Attacks and has been late like many other developing nations around the globe in perceiving the Cyber Attacks, The government of India has taken various steps in developing a safe and resilient cyberspace for its citizens, businesses and government and have a National Cyber Security Policy 2013 also addressed by the Information Technology Act, 2000 to safeguard itself. Many nations in this time zone are not alert and have no legislature to safeguard its populace and economy [12].

### *The Americas*

The New world in the western hemisphere of North and South America has dealt with various and the oldest forms of Cyber Attacks. The United States of America has the uttermost organized military for such cyber-attacks. Cyber warfare is a constituent of the American military-strategy of spirited Cyber defense and the use of Cyber-Warfare as a platform to attack. The United States Department of Defense has formally recognized cyberspace as a new sphere in warfare and has set up a new Cyber Command (USCYBERCOM) to shield America Military Networks and attack other

countries systems. In the US, denial-of-service attacks may be considered a federal crime under the Computer Fraud and Abuse Act with penalties that include years of imprisonment and fine. The Computer Crime and Intellectual Property Section of the US Department of Justice handles cases of (D)DoS. The Canadian Armed Forces have also revealed to entrench a new systems; the executives of Cybernetics, guided by Chief Administrative Officer, the director General Cyber (DG Cyber). Within that cabinet the newly stationed CAF Cyber Task Force charged to design and construct Cyber Warfare proficiencies for the Canadian Armed forces. The Sub-continent of America, the South America has also risen up and understood the severity of the situation in the Cyber World and has an urge for all the countries in South America to form a joint cyber Shield to protect them from their adversaries and protect the vital data and growing economy however they have not made any law to protect themselves [7] [13] [14].

### **Conclusion and Suggestions**

The Cyber World has only given the nations another more advanced “Field in Warfare” in which the assailant and rivals are not sending rockets and missiles to annihilate cities. They are not landing on the oceanfront for armed warfare. They are attacking with suave attacks by virtue of Internet borders away. With very little investments and wearing the cloak of invisibility/anonymity harming the national interests. The Cyber Space is confronting in both traditional and irregular conflicts. It will expanse from an artless novice to a highly schooled polished hacker, Through Cyberspace rivals will point academia, industry, government, military on land, maritime, and space empire. The exigency in accretion on cyber warfare legislation is vital and needed to develop by each and every nation around the planet as the current laws have failed to prevent the number of the victims from increasing at an escalating rate. The identification of source of Cyber-Attacks is nugatory as the assumed country’s government may deny any involvement in these acts of war; With the current trends in rise of the Cyber Warfare; the nation’s may choose to develop an exceptionally protected networks or choose to go back to the traditional ways to connect. In many countries, changes in legislation have resulted in the arrest of

computer virus writers. With widespread press coverage, these arrests have probably deterred many youths from developing malicious code. The governmental body has to foresee their own country's networks for any allusion of starting the Cyber Attacks, an intergovernmental organization to promote international co-operation in cyber space must be established and developed. The Cyber Space is only

giving another field for antagonistic people to channel their cynicism which has to be disciplined, counseled and stopped by a regulatory organization common around the world. The years of imprisonment and fines imposed on people breaking the law must increase and laws common around the world should be come into existence as laws of some countries may be illegal to use in another countries.

## References

1. ANDREW F. KREPINEVICH, Cyber Warfare, a "Nuclear Option"? Defense policy analyst Center for Strategic and Budgetary Assessments. 2012.
2. The Whitehouse National Cyber security Communications Integration Center Arlington, Virginia January 13, 2015, 3:10 P.M. EST.
3. WHITE HOUSE CYBERSPACE STRATEGY, Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel November 16, 2011.
4. Zener Bayudan, Brandon Pitman, John Oleynik, CS4235 at the Georgia Institute of Technology.
5. McAfee, local content white papers hollanderdefacement.
6. Source Country for DDoS Attack [www.foxbusiness.com/technology/2013/04/17/intensity-ddos-attacks-explode-in-firstquarter-average-bandwidth-surges-61/](http://www.foxbusiness.com/technology/2013/04/17/intensity-ddos-attacks-explode-in-firstquarter-average-bandwidth-surges-61/), access on 10th Jan'14.
7. Dancho Danchey's Blog, Security consultant "trends and fads, tactics and strategies, intersecting with third-party research, real time CYBERINT assessments"
8. Cyber Security Strategy for Germany Federal Ministry of the Interior Alt-Moabit 101 D 10559 Berlin, February 2011.
9. Minister of Security and Justice, Ivo Opstelten, Opening NCSC One Conference 2014, World Forum, the Hague, 3 June 2014.
10. Gorman, Siobhan (April 8, 2009). "Electricity Grid in U.S. Penetrated By Spies". The Wall Street Journal. Retrieved November 2, 2010.
11. Kim, Eun-jung. "S. Korean military to prepare with U.S. for cyber warfare scenarios". Yonhap News Agency. Retrieved 6 April 2013.
12. "National Cyber Security Policy of India 2013 (NCSP 2013)". Centre of Excellence for Cyber Security Research and Development in India (CECSRDI). Retrieved 14 August 2014.
13. Khang Pham, Cyber Security: Do Your Part, The Maple Leaf, Vol. 15, No. 2, February 2012.
14. Dilanian, Ken. "Cyber-attacks a bigger threat than Al Qaeda, officials say", Los Angeles Times, 12 March 2013.

# Cyber Terrorism - An International Phenomena and An Eminent Threat

Biny Pal Singh\*  
Ankit Verma\*\*

---

## Abstract

This paper goes into the conception of terrorism, who the terrorists are and tries to establish a grasp of why they conduct the activities they do. Understanding the attacker will allow recognize the type of attack they may plan and the aftereffect they are likely to try and accomplish. It looks at the main encouragement of Terrorist groups and considers their use of the Internet for various forms of a terrorist Campaign such as implantation/advertising and recruitment. It will acknowledge the various channels that have been used and how the Internet has provided a new liberty for terrorists to conduct their campaigns and how it has been adapted by them for their purposes. It examines the probable threat of a cyber-attack by terrorist organizations and how they can use the Internet and Cyber Space to their liberty and attack a target with similar results to a conventional physical attack. The paper will briefly examine some of the possible defenses against this form of terrorism.

**Keywords:** Terrorism, Terrorist encouragement, Cyber-attack, Terrorist use of the Internet

---

## Introduction

If 10 security experts who create various forms of protection against 'cyber terrorism' are asked what 'cyber terrorism' is, you will get at least nine different definitions! When those 10 experts are in the field of computer security, this discrepancy moves from comedic to rather worth consideration and serious. When these 10 experts represent varied departments of the governmental agencies tasked with protecting the infrastructure, defense and assets of our nation, it becomes a critical issue. However, given the lack of scientific groundwork/platform to incorporate various aspects of computer-related crime into the category 'cyber terrorism', this situation should not be surprising.

## Understanding Terrorism

Most people who are asked about terrorism would say that they know who terrorist are and what terrorism

---

### Biny Pal Singh\*

Student (BCA)

IITM, Janak Puri, New Delhi-110058

### Ankit Verma\*\*

Assistant Professor

IITM, Janak Puri, New Delhi-110058

is, but surprisingly there has never been internationally agreed definition. but considering violence or threat of violence as theme there have been literally hundreds of definitions that have tried to throw light on this international phenomena. The only other elements to appear in more than 50% of definitions are "Political" and "Fear, terror emphasized" [2]. Terrorism dose differ from other crimes in its core; it is done with a purpose in mind and an aftereffect that is expected from its occurrence. Considering who the terrorist are is most important. Considering size and ability there are literary hundreds of terrorist groups, which to some extent, warrant the label of terrorist. Terrorism has 4 classic encouragements [3]. Firstly there are terrorist with single issue, those who have faith in one particular cause and are ready to use violence to protect their message in the faith of ending the issue. Although commonly small and at less devastating rate, these groups can use the cyber world to their aid as in cyber environment they can effectively push forward there cause and end the issue with very less lethality rate. The terrorist who use violence to effectively promote their political ideology are the ideological terrorist. Religio-political terrorist groups are more dangerous as there believe is that they are acting for GOD himself or on a spiritual order and that those not of their belief

are against GOD [3]. There are extremist groups spanning all major religions and some minor cults who have resorted to terrorism. These terrorist have acted outside their religion and abused it, they misrepresent their religion in their claims and must not be confused. Although warfare and violence have been circumstantially justified in many religions, none, with the exception of a doomsday cult such as Aum Shinrikyo, would apply this as indiscriminate targeting of security forces or civilians outside the legal borders of warfare. The Groups who evolve there motivation or have heterogeneous aims can be hybrid terrorist groups, as with any definition of labeling model. The Provisional IRA are an example, they were a Nationalist group as they wanted Northern Ireland to cede from the United Kingdom to the Irish Republic but were also an Ideological group as they wanted Ireland to become a Socialist state. Considering the terrorist themselves, consideration on their psychology is important to get to the point where we can understand how to defeat them. Terrorist don't have a clear profile, they come from all aspects of life and have varying motivation, educational, employment and wealth. That all not being mentally unstable is the only common factor among them all as, terrorist organizations want the ability to think and reliability to exist among all of its activists. The role of the terrorist be decided on their intelligence level and also by any

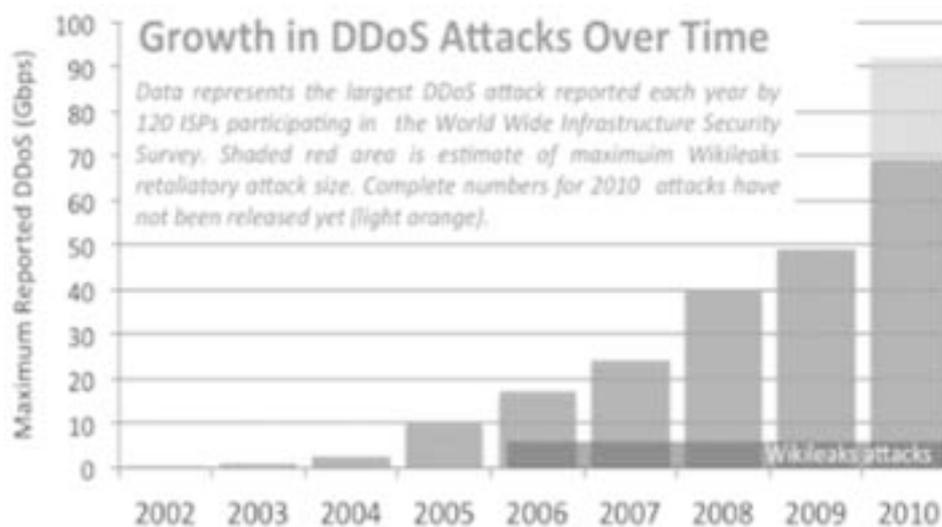
specialist skills such as chemistry or IT. And there must be a requirement for college level members as well they have more basic standard of education. It must be accepted that most of these terrorist groups are comprised of skilled and exceptionally-intelligent people who are acting out of genuine belief (self-formed, independent) and not a group of clueless idiots. Cyber defense plan against terrorism must consider this; they will study, take time, make plans and hire experts of the highest caliber to achieve their aim.

### Hacking Techniques – Types of Attacks

According to Galley's discussions from 1996 there are three types of attacks against computer systems:

- Physical
- Syntactic
- Semantic.

Conventional weapons are used in a physical attack, such as bombs or fire. Where as to disrupt or damage a computer system or network a syntactic attack uses virus-type software a semantic attack can be taken as a more subtle approach. It attacks users' confidence which is done by causing a computer system to produce errors and results which are unpredictable. Syntactic attacks are categorized under the term "malicious software" or "malware". The use of viruses, worms,



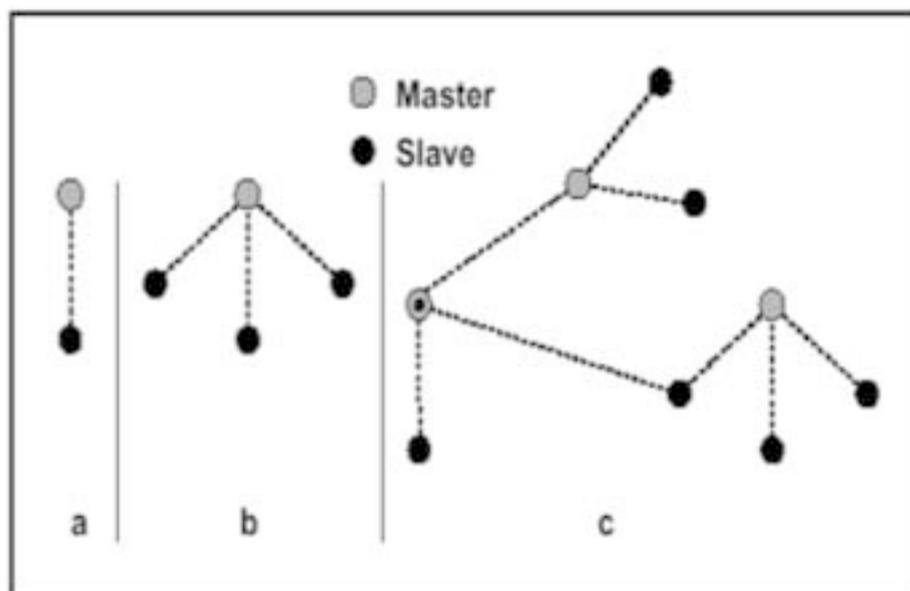
**Figure 1: Growth In DDoS Attacks From 2002 Till 2010.**

and Trojan horses is done in these types of attacks. Email is one of the most common vehicles of delivery for such malware. Denial of service (DOS) and distributed denial of service (DDOS) attacks are also included in Syntactic attacks. In recent years attacks such as these have become more widespread. Ping saturation is one of the most common technique forms of DOS and DDOS (Vatis, 2001). Ping is an Internet utility used commonly to verify that a device is available at a given Internet address. Ping saturation occurs when ping is used in an attack to overwhelm a system. The intent in these types of attacks is to disrupt services on a network or system by flooding it with requests. Modification of information or dissemination of incorrect information is involved in Semantic attacks (Schneider, 2000). Even without the aid of computers, Modification of information has been perpetrated, but new opportunities to achieve this have been provided by computers and networks. Also, mechanisms such as email, message boards, and websites help in dissemination of incorrect information to large numbers of people.

### Pure Cyber-Terrorism

Pure terrorism is a category that consists of all those terrorism activities are carried out totally (entirely/ primarily) in the virtual world and have a drastic

aftereffect. There are some many ways over the internet where one can meet like-minded individuals in a (comparatively) safely and share information and on a secure line which are used by these terrorist organizations to maintain a contact. No further prerequisite rather than knowledge is required for a successful cyber terrorism event. Knowledge is something that is essentially free to the owner once acquired, and an asset that can be used over and over again. Further, such environment could be facilitating the creation of an entirely new terrorism group. There won't be requirement of any head or chief and the member could organize themselves quickly and easily through cyber-space that could be a threat to the global security and the counter terrorism department itself. This is very different from some examples given above, where the cyber space could aid the activities terrorists, but the real resources are still required for execution of the real plan. The Danger possessed by the cyber terrorists and the significant barrier of our ability to protect ourselves is what writer's means when they toss around pure cyber-terrorism. There is always one question that has never been appropriately addressed in the literature is that what this terrorism might look like. There is a large amount of confusion at this time because of the lack of agreement in an international and intellectual definition for the above question.



**Figure 2: The encounter of Cyber-Terrorist activities in U.S.A and china Cyber-Space**

### **Increase in Cyber-Terrorist Activities**

Figure 2 shows that how the cyber terrorism has been increasing its activities and has made the world feel its presence in last 7 years. Till 2007 these activities had seen an increase of 32% and shows that in future it can be an international phenomena and affect every corporate and government of this world.

### **Computer Weapon of Cyber Terrorism**

Following on from the foundation above, the most obvious and curtail weapon of this eminent threat of global cyber terrorism is the 'computer'. So, the question arises that are we purposing that we should restrict the use of a computer on all bases, just as the access to explosives and radio-active stuff is restricted? Not quite it, but close. We mean that the Heap of connected computers needs to be protected. May laws define how one should protect and ensure the security of firearms from illegal/Dangerous use like the gun can fall in wrong hands and can pose danger which is secured by the mandatory use of trigger lock and the RDX explosive material is not sold over the shop at the corner of the street? Computer is certainly not entirely equivalent to explosives or a gun. Thus, a wide number of laws are already present in current system of judiciary that discusses damage done to/by the third party by the intentional/unintentional misuse of corporate/personal piece of information/property/data. The definition of 'misuse' in these laws and there application is unclear till date. However, these laws and standards need to be more clear which will require the operators of large network of interconnected computers take forward appropriate steps to keep these systems safe.

### **Conclusion**

The Development if the internet was done primarily as an open architecture which was unregulated. We are not only witnessing the backlash to the 'corporatization' of the network, Where the Equipment for drastic destruction can be easily be placed in the hands of backward and mindless people, We must also deal with the fact that this infrastructure was/is ideally suited for criminal activities on a wider base. Some of

these activities are being promoted as cyber-terrorism. The government and the corporate organizations security is at the risk who are not capable of defending themselves from this eminent threat. Events can are to analyzed in terms of their critical factors that may exist can legitimately be called terrorism. However, if all these factors don't exist then it doesn't means that the corporations are safe. Unfortunately, the structure of corporation are built around the premises that people will do right thing. But as we have seen this is not necessarily the case. We do not use the term 'chemical terrorism' to define bombing of chemical factories, nor will we use it to define terrorism carried out with chemical. Thus, the question arises why the term cyber-terrorism is used to describe any sort of threat or criminal activity carried out with or against computer in general. At the same time, there are some who insist on treating "Pure Cyber-terrorism" as Cyber terrorism who are completely missing the true threat that the addition of acts in the virtual world to the terrorist playbook possess. Finally, the cyber-terrorism has to be given attention separately and cannot be mugged with common terrorism. This artificial fragmentation of our defense System is an advantage for the enemy and is to be avoided at all cost. This brings us to the final Point of this ongoing study: turning the tables on terrorism. As we have seen, computer can play an enormous role in terrorism. But they are also our biggest defense against terrorism its self if used to our advantage, this begins when we re-examine basic beliefs about cyber-terrorism which must take place in industries, academia, government and defense sectors. Analysis of the information must be shared at each level, collated and redistributed across the states, local government boundaries, industries, academia, and in some cases to the citizens as well. The lack of consideration of cyber-terrorism and the overall insecurity of the networks of the World Have allowed a situation to develop which is not best for the country or the computer user. The computing resources are to be protected, and the job of these terrorists is to be made difficult which can be accomplished by only re-examining the commonly held believes about the very nature of the computer system and its counterpart cyber-terrorism.

## References

1. Record, Jeffery: Bounding the Global War on Terrorism, Strategic Studies Institute, US Army War College, Leavenworth, 2003.
2. Schmid, Alex and Jongmans, Albert et al: Political Terrorism: A new guide to Action, Authors, Concepts, Data Bases, Theories and Literature, Transaction Books, New Brunswick, 1988.
3. CSTPV St Andrew's University Certificate in Terrorism Studies.
4. COE DAT Information Collation Managemant Cell database.
5. Weimann, Gabriel: Terror on the Internet, USIP, Washington DC, 2006.
6. Weimann, Gabriel: WWW.AL-QAEDA: The reliance of Al-Qaeda on the Internet7.
7. COE DAT Cyber Terrorism Couse IV Mar 09.
8. COE DAT Strategic Communications Workshop May 09.
9. Huizing, Harry: Cyber Terrorism Briefing Note, COE DAT, Ankara, 2008.
10. Krone, Troy: Gaps in cyberspace can leave us vulnerable, Platypus Magazine (edition 90, Mar 2006).
11. COE DAT Cyber Terrorism Workshop Oct 07.
12. Bunker, Robert J: Networks, Terrorism and Global Insurgency, Routledge, Abingdon, 2005.
13. Hennessy, Joh L and others: Information Technology for Counterterrorism, National Academies Press, Washington DC, 2003.
14. Hoffman, Bruce: Inside Terrorism, Columbia University Press, New York, 2006.
15. Huntington, Samuel: The Clash of Civilizations, Free Press, London, 2002.
16. Laqueur, Walter: The New Terrorism: Fanaticism and the Arms of Mass Destruction, Oxford University Press, New York, 1999.
17. Sageman, Marc: Understanding Terror Networks, Penn, Philadelphia, 2004.
18. Stern, Jessica: The Ultimate Terrorist, Harvard University Press, Cambridge MA, 1999.
19. Tuman, Joseph S: Communicating Terror, Sage, Thousand Oaks, 2003.
20. Whittaker, David (ed): The Terrorism Reader 3rd Ed, Routledge, London, 2007.
21. Wilkinson, Paul: Terrorism versus Democracy, Routledge, London, 2006.