iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4153

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Cyber Security for Social Networking Sites: Issues, Challenges and Solutions

Rituparna Das[1], Mayank Patel[2]
[1]UG-Scholar, [2] Asst. Prof., Department of Computer Science & Engineering, GITS

Abstract- ***In today's socio-economic environment one of the fastest growing areas of technical infrastructure development is the Internet. The increasing cyber-attacks over the past decade are posing a serious threat to the digital world. The paper focuses on the issues of cyber security for Social Networking Sites (SNS) since social media adoption among individuals and businesses is skyrocketing. Social Networking Sites have many areas of applications like digital marketing, social e-commerce and branding. The fact that the maximum number of users are not aware of risks and their lack of knowledge leads to further increase in cyber-crimes is a major challenge. All these issues would form a part of the paper. The security concerns and challenges on SNS like identity misuse, malware, phishing attacks and third party application threats have also been discussed separately. While highlighting the government initiatives to curb this serious issue, the paper also suggests some appropriate solutions which can be adopted by the individual users as well as the government in the collaboration with private sector for a cyber-safe digital world.***

Keywords- ***Cyber Security, Social Networking Sites, Security issues, Cyber Crimes, Digital world, Cyber-attacks, security awareness, National Cyber Security Policy 2013.***

I. INTRODUCTION

In today's era of Smartphone and computers the internet has changed the idea of communication. Due to lack of security, various cyber-crimes have emerged in the past decade. Cyber security plays a significant role in the current development of information technology and services. Cyber security is thus an attempt by users to keep their personal and professional information intact from the attacks on the internet. The main function of cyber security is to protect networks, computers, programs from unauthorized access and loss. Maximum number of users are not aware of the risks and share their information unknowingly and their lack of knowledge makes them vulnerable to cyber-attacks. So cyber security is the main concern in today's world of computing. According to IC3 [1] report 2015 (Internet Crime Complaint Centre) an alliance between the National White Collar Crime Center (NW3C) and Federal Bureau of Investigation (FBI) the top five countries by count in victim complaints as numbered by Rank as follows.

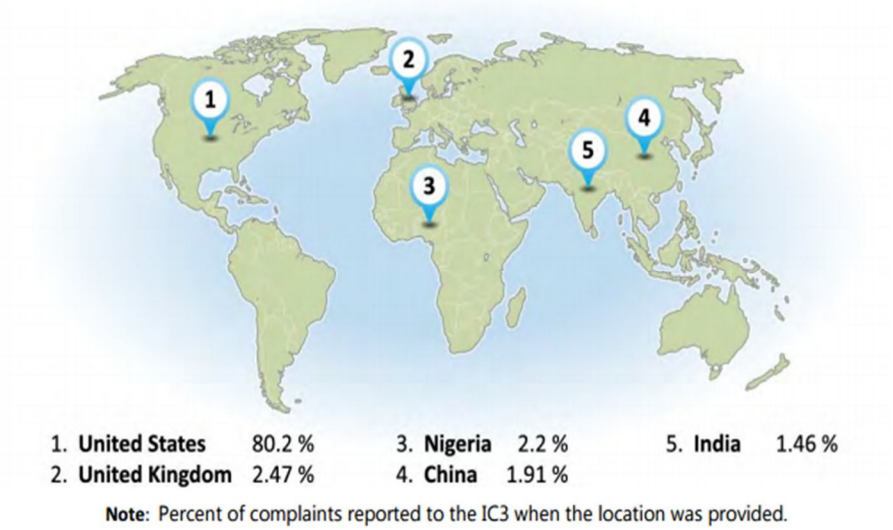


Fig. 1 The top five countries by count in victim complaints as numbered by Rank

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

II. CYBER SECURITY IN INDIA

As the internet usage has increased in India, cyber-crimes have also increased respectively. More than 32000 cyber-crimes were reported between 2011 and 2015, across India and more than 24000 of these cases have been registered under the IT Act and the remaining cases under the different sections of IPC and other State Level Legislations (SLL).Cyber-crimes are registered under three broad heads in India, the Indian Penal Code (IPC), the IT Act and other State Level Legislations (SLL)[2]. The cases registered under the IT Act include

A. Tampering with computer source documents (Section 65 IT Act)
B. Loss /damage to computer resources(Section 66 (1) IT Act)
C. Attempt Hacking (Section 66 (2) IT Act)
D. Accessing Digital Signature Certificate by misrepresentation of facts (Section 71 IT Act)
E. Publishing false Digital Signature Certificates (Section 73 IT Act)
F. Fraud Digital Signature Certificate (Section 74 IT Act)
G. Breaking of confidentiality or privacy (Section 72 IT Act)
H. Failure to aid in decrypting the information intercepted by Government Agency (Section 69 IT Act)

Cyber-crimes have increased more than 3 times in 5 years

Year	IT Act		IPC	
	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
2011	1791	1184	422	446
2012	2876	1522	601	549
2013	4356	2098	1337	1203
2014	7201	4246	2272	1224
2015	8045	5102	3422	2867
Total	**24269**	**14152**	**8054**	**6289**

Fig. 2 The table shows the cyber-crimes increase from year 2011-2015.

The numbers of cases registered under IPC and the IT Act have been growing exponentially. The cases registered under the IT act increased by more than 350% from 2011 to 2015. The cases registered under the IPC increased by more than 7 times from the time interval of 2011 and 2015. The government also is taking steps to curb the increase in the number of such cyber-crimes.

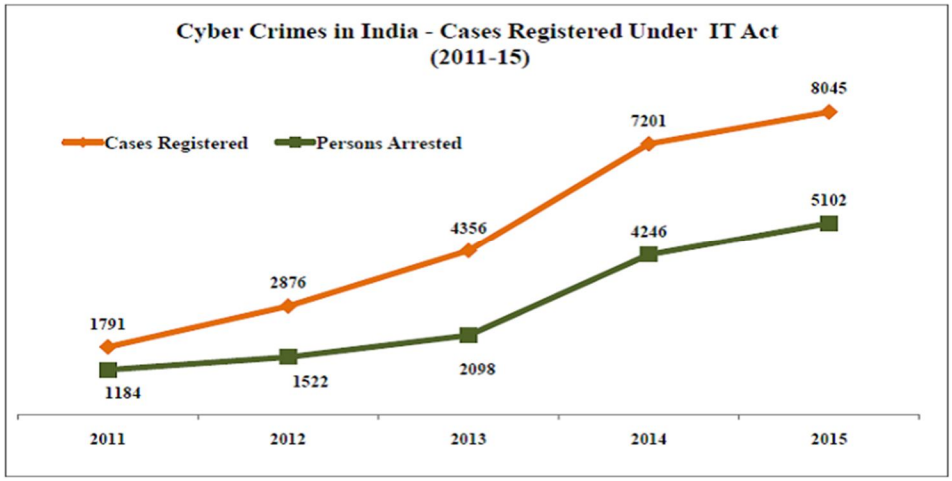


Fig. 3 The graph shows the cases registered under the IT Act (2011-15)

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

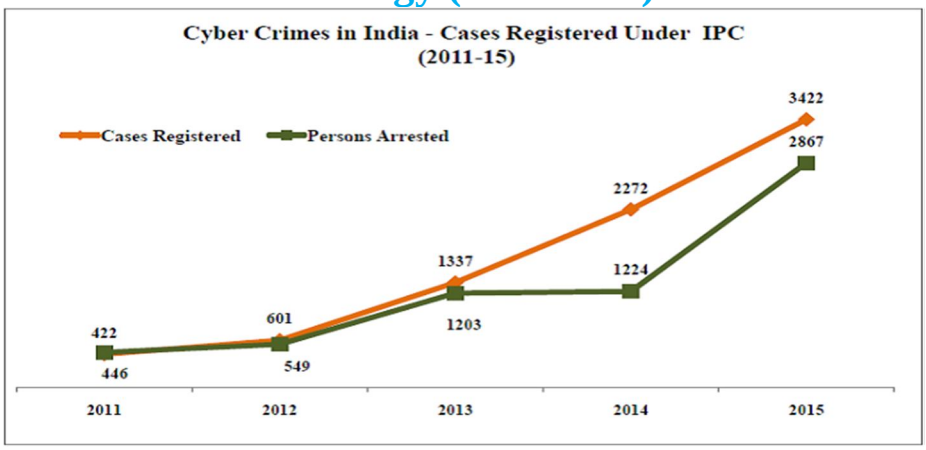


Fig. 4 The graph shows the cyber-crimes cases registered under IPC (2011-15)

I. Maharashtra & Uttar Pradesh are on the Top

The states with the highest rate of cyber-crimes form 2011 to 2015 are Maharashtra and Uttar Pradesh. Maharashtra leads the list with more than 5900 cases in the 5 years and Uttar Pradesh with close to 5000 such cases. Karnataka is third having more than 3500 cases. The top states in this list are the ones with a great internet subscriber base. The bottom 10 states are smaller states with less population and less internet penetration.

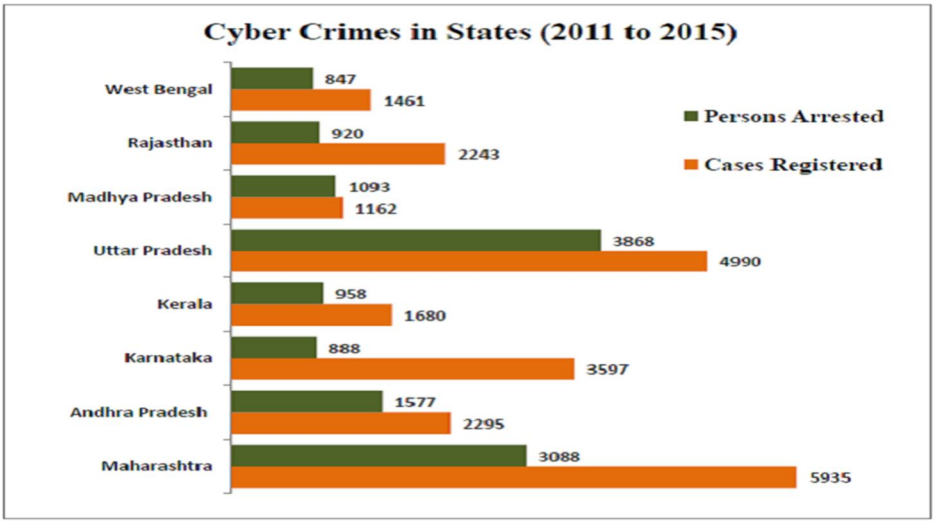


Fig. 5 The graph shows the Cyber-crimes in various states in India (2011-15)

III. NATIONAL SECURITY POLICY 2013

The Vision [3] of this policy is to develop a secure and strong cyberspace for citizens, businesses and for the government. The policy tries to protect personal information, financial and banking information.

Ministry of Communications and Information Technology (India) is working to create a secure cyber ecosystem in the country. And to Protect information in process, handling, storage and transit so as to shield the privacy of citizen's information and reducing economic losses due to cyber-crime or data theft.

A. The Ministry has also defined the strategies [3] of the policy

1) To create a safe cyber ecosystem.
2) To create a guaranteed framework.
3) To Encourage Open Standards.
4) To secure e-Governance services.

IV. CYBER SECURITY FOR SOCIAL NETWORKING SITES

The main purpose of social networking sites is to connect people and organizations. It has also developed many business opportunities for companies and firms. Social media has introduces significant change in the way people communicate. Social networking sites bring out a specific concern related to privacy and security of the user. The security and privacy of these sites mainly focuses on malware detection as it appears to come from a trusted contact, users are more likely to click on the link. The social networking sites have formed applications in many areas like-

Social e-commerce: The social networking sites can be used for the promotions and advertisements for e-commerce portal owners.

Branding: The social media provides a better platform to the companies to attract customers for more business opportunities.

A. Issues

As the growth of social networking sites has brought various benefits it also has brought various security concerns. It also provides a vulnerable platform to be exploited by the attackers. Some issues associated are as follows.

1) *Misusing Identity:* The attacker impersonate identity of any user results in misusing identity [4]. The attackers attack through the applications in which they ask for granting permission for accessing the information provided in Social Networking Sites. When a user allows doing so, they will gain access to all the information and that information can be misused without the knowledge of the user.
2) *Threats from using 3rd Party Applications:* These applications seek permission from the user to access personal information for all the various games and apps. The user grants the app a certain level of permission concerning user's information. And some of these applications which are playing at the foreground may download a malware on the user's computer or phone without their consent.
3) *Trusting Social Networking Sites Operators:* The contents that user uploads or posts on social networking sites, the information is available with the networking operators. The operators can save account data even after deletion.
4) *Viruses, Phishing Attacks and Malwares*: Viruses and malware often find their way onto your computer through those annoying ads. After gaining access to the network, the attacker can access or steal confidential data by spreading spam mails.
5) *Legal Issues*: Posting contents that is offensive to any individual or community or country. There are legal risks associated with the use of social networking sites like leaking confidential information on sites or invading on someone's privacy.
6) *Tracking Users*: It can cause physical security concerns for the user, as the third parties may access the roaming information of the user by collecting the real time update on user's location.
7) *Privacy of Data*: Users share their information on social networking sites and can cause privacy braches [5] unless proper security measures are applied. For example everyone can see the information of a user, if the user's default setting is 'public'. Accepting requests from unknown people can also create a security threat.

B. Risks and Challenges

With the increase in the number of users accessing social networking sites, has opened new routes for the attackers to gain access to the accounts of the individuals. The more Information that is posted creates a new threat on the privacy and security of the user. Social Sites are growing rapidly posing new risks for individuals and organizations in this modern world of technology. And some of the challenges are as follows-

1) *Phishing Attacks*: It is a technique for accessing sensitive information. The attackers make fake web pages that look like the legitimate ones and ask users to enter their credentials and the user gets in trouble when the user enters the credentials. Kaspersky Lab's statistics exposed that the fake social sites imitating Facebook user's accounts for nearly 22% of phishing attacks in 2014. According to Kaspersky Lab, phishing is a major threat in Russia and the Europe as the number of attacks has increased in this region, up 18% to 36.3 million attacks in Q3 2015 as compared with the same time period last year [6]. For example A Moldovan man ran a phishing scheme that ended in a loss of $3.5 million for a western Pennsylvania drilling firm. A school district was almost tricked by the same scam into sending almost a million dollars. The email contains a malware in a zip file attachment.[6]
2) *Identity Federation Challenges*: It is a technique used to share user credentials across multiple domains [4]. For example many sites offer users to login by their Facebook Account so that it is more convenient to the user and the user does not have to make multiple accounts across different sites. It may seem convenient but the user does not have the knowledge about on how and to what extent their personal information can be shared among third party applications.

3) *Malwares*: Malwares are the programs which are installed in the user's devices without the knowledge and consent of the user. This spreads fast and infects the devices. 390,000 malicious programs are registered every day by AV-Test Institute (AV-TEST, 2016) [7]. It causes security defects in the software viruses, worms, and Trojan horses are examples of malicious software. Attackers can gain access to the personal information of the user by monitoring the activities of the computer and the computer can also be controlled or can engage in mass attacks without the knowledge of the user as malwares can steal the identity of the user and malwares can also crash the computers. Also hackers can install forms of adware that can cause endless pop-up ads on the user's machine such as-

a) *'LOL' Virus:* This virus spreads through chat function of Facebook. This virus is sent to the user stating "lol" with an attachment. And when the user clicks on the link a malware is downloaded to the user's system. The virus infects the system and spreads through the network gaining access to the user's information.

b) *Zeus:* This is a Trojan which spreads by clicking on the link. And when a user clicks on the link it scans all the files on the user's system and steals the important information. The specialty of this Trojan is to steal bank credentials of the user.

4) *Click Jacking Attacks*: also called UI redress attacks. Where the Trojan in web pages asks the user to click on the malicious link, and a malware is planted onto the system. This is common in Facebook with the name like jacking that is when a user likes a page, a picture or a video the user is trapped by the attackers[8]. This type of attacks are done to do malicious attack or to make some page popular.

V. RECOMMENDATIONS

In this section, some recommendations are given to secure the information of the user

A. For a Company some policies should be made for mails so that the mails are not confused with any other spam mails or phishing

B. Good quality of anti-virus should be used both by the individual user and the company so that it can filter and block the malicious website

C. Authentication should be done at every level of the web sites to avoid attackers from access gain of the user's personal information

D. Cryptography based techniques should be used so ensure the security of the user's information provided on the social networking websites. Group key exchange, data mining, encryption are some of the examples which can be used to enhance the security on social media

E. Training and educational programs should be done by the government to spread the awareness about cyber security. The Government should conduct publicity campaigns and programs which includes seminars, contests, exhibitions about cyber security

F. Social Networking Sites which has the privacy security setting discusses the tools which available to make the account more secure. Like Facebook's privacy settings where the privacy basics [9] are subdivided as-

1) *Who-can-see-my-stuff*: This is priority setting for the Facebook users where the user can limit the audience who can see the posts from the user. Public posts should be avoided for security

2) *Login-Alerts*: This setting allows the user to get a notification when anyone logs into their account from an unrecognized device or browser.

3) *Third-party-authenticator*: This is the new setting added to the Facebook which enables to generate Facebook security code to authenticate any third party app

4) *How others interact with the user*: This helps user to manage how other people's activity affect the user's profile. And the user can manage tags, 'unfriend' or 'block' someone.

G. *Web Browser Security Settings [10]*

1) User should keep browsers up to date and automatic updates should be enabled for the browser.

2) Block plug-ins, pop-ups, and phishing sites.

3) Set browser not to store passwords.

4) Disable third-party cookies.

5) *Browser-Specific Settings:*

a) *Firefox:* install the NoScript add-on

b) *Safari:* Disable Java

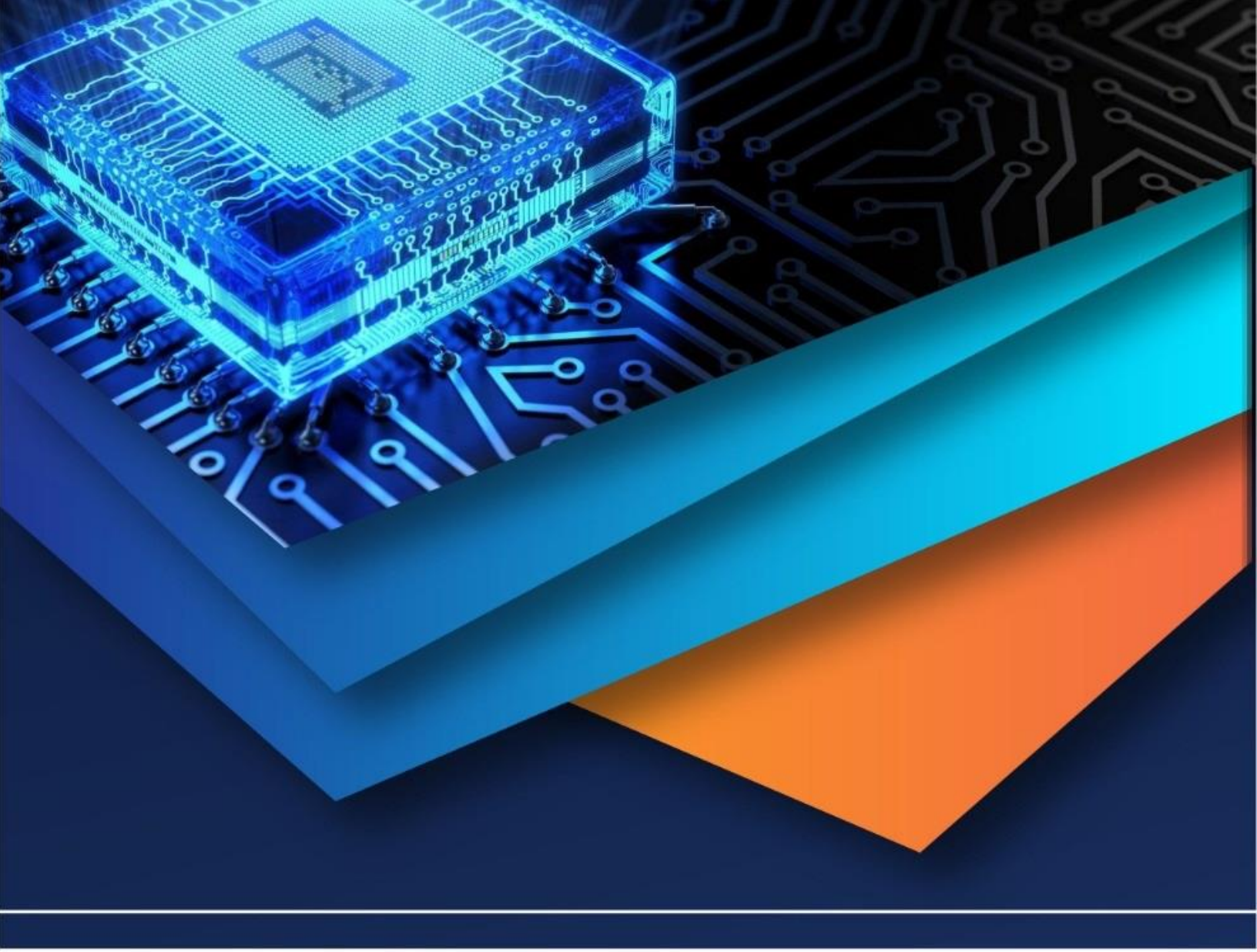
c) *IE:* Set up security zones.

VI. CONCLUSION

As growing popularity of the Social Networking Sites these have become a prime target for cyber-crimes and attacks. Cyber-crime is becoming a widespread and posing a major threat to the national and economic security. Both public and private institutions in sectors of public health, information and telecommunication, defense, banking and finance are at risk. So the organizations should take proper security measures to be cyber-crime safe and the users should protect their personal information to avoid and identity theft or misuse. The cyberspace is becoming a significant area for cyber-crimes and terrorist to attack on crucial information. So, there is a need of universal collaboration of nations to work together to reduce the constantly growing cyber threat.

REFRENCES

[1] http://www.ic3.gov/ "Internet Crime Report 2015"
[2] Most number of cyber crime reports. Available: https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/
[3] National Cyber Security Policy 2013. Available: https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013
[4] Security, Privacy and Trust in Social Networking Sites. Richa Garg, Ravi Shankar Veerubhotla, Ashutosh Saxena. CSI Communications ISSN 0970-647X| Volume No. 39| Issue No. 2| May 2015.
[5] Exploiting Vulnerability to secure user Privacy on a social networking site. Pritam Gunecha, Geoffrey Barbier, Huan Lui. ACM, SIGKDD International conference on knowledge Discovery and Data Mining, August 2011.
[6] Latest in phishing 2016. Available: https://info.wombatsecurity.com/blog/the-latest-in-phishing-first-of-2016
[7] Malware statistics. Available: https://www.av-test.org/en/statistics/malware/
[8] Dolvara Gunatilaka "A Survey of Privacy and Security Issues in SocialNetworks"www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.
[9] "Facebook Privacy Basics", [Online]. Available: https://www.facebook.com/about/basics.
[10] Browser Security Settings. Available: http://its.ucsc.edu/software/release/browser-secure.html



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY