**Migration Letters**

Volume: 21, No: S6 (2024), pp. 1279-1284

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

# Cyber Security: Issues, Challenges & Countermeasures

Ekta[1*], Ajit Singh[2]

**Abstract**:

*In the present era of information & communication technology, there is a huge amount of data to be communicated over the internet and everyone wants a secure communication to their data. But there are various issues related to the cyber security which diminishes the confidence of the people to use internet for communication. Keeping in View the same, this paper aware people about different types of attacks which can occur in a society and provide the solutions to protect themselves from these attacks. In the first phase, various popular types of attacks on data are described. Second phase describes various cyber crime histories at the national & international level. Finally, various challenges which are faced by people in information exchange along with the various techniques to resolve the issues of cyber security are defined which are beneficial in secure information exchange.*

## I. INRODUCTION

Cyber Security Risks are global as the world is marching towards connectivity through digital means. People need secure[1], trusted policies & techniques to address the issues related to cyber Security & Risk to assure success of safe and secure connectivity. Almost all the systems like satellites, social sites, banks, thermal power plants , government or Private Organisation etc. are attempting to be digital, are prone to cyber risks all over the world. In 2020, there is a looking for a world of 7 billion people, 50 billion devices connected to internet or 7 devices per capita. Therefore, as the internet use increases, the threats related to cyber security will also increase and will give an open surface to the attacker to attack easily. So, there is a need of better understanding on risks related to the cyber Security to get the secure & trusted connectivity.

## II. RISK INVOLVED IN CYBER SECURITY

The huge growth of connectivity via digital means has given various benefits to the users but also generates a large number of Security concerns. Some of very popular risks and challenges in cyber security are as follows [2][3][15]:

A. Identity Misuse: The impersonation of a legal user by an intruder can get all the personal details about a user and hence causes the misuse of user's identity. So, a user should not put plenty of personal information on public profiles.
B. Malware: Malicious Software is a program which causes the unwanted action in a user's side. It includes computer viruses, trojan horse, worms, adware, spyware and other intentionally harmful programs by attacker which seems to come from a trusted contact.
C. Zeus: This is a type of Trojan that steals the loin details of a user and spreads through clicking a link. It was specialized in stealing bank details.

[1] PhD Scholar, Bhagat Phool Singh Mahila Vishwavidyalaya, Haryana, India.

[2] Professor, Dept. of CSE, Bhagat Phool Singh Mahila Vishwavidyalaya, Haryana, India .

D. Trojan Horse: It impersonate as a regular or utility programs so that the user the user install it and after installing it, it carries the hidden destructive functions.

E. Koobface: it is an attack on social networking sites in 2009 by sending a message to a friend with comment “you look funny in this video” with a link. If user clicked on this link, the link will open a new page like some trusted website and seems to have a video as the name of that friend and gives an installation option to play that video. But if once get installed, the system will get hacked.

F. LOL Virus: It spreads through facebook chat function with simply a message “lol” and an attachment [14].

G. Computer Viruses: It is type of malware which spreads by embedding itself in some other executable files on the system without user consent and when user run it, virus spreads into other files.

H. Worm: It is a stand- alone malware means spread itself and transmits itself over a network to infect other systems.

I. Spyware: It targets to collect the secret information about a person or organisation like:
    - Internet surfing habits of user
    - Login details
    - Credit account details etc.

J. Ransomware: It threats the user to publish its personal data or blocks access of user to his personal account to get some ransom.

K. Rootkits: A collection of software which allows hiding the existence of malicious code into the system by the attacker so that the user cannot detect its existence.

L. Bootkits: It is a kernel level rootkit variant which can harm startup code like boot sector and can attack full disk encryption system.

M. Backdoors: This is a method mainly used by the designer of the system to bypass the normal authentication process for some testing like purposes. But sometimes designer forget to fix these backdoors intentionally or unintentionally.

N. Keystroke: It causes the recording of the letters pressed on the keyboard to get the logging details or some other personal information of a person.

O. Data Scrapping: When no other means of data interchange is possible then the attacker’s computer program extracts data from human readable outcome coming from other program.

P. Screen Scrapping: Getting the visual data from the display of a terminal screen.

Q. Logic Bomb: It is a code inserted into some software which will executes when a particular condition met.

R. Exploit: It is a piece of software, data command which takes benefit of a bug to cause unwanted behaviour of a system.

S. Denial of Service: It is a cyber attack which restricts the user by getting useful information by flooding the target machine with huge unwanted or false requests to overload the system [11][12].

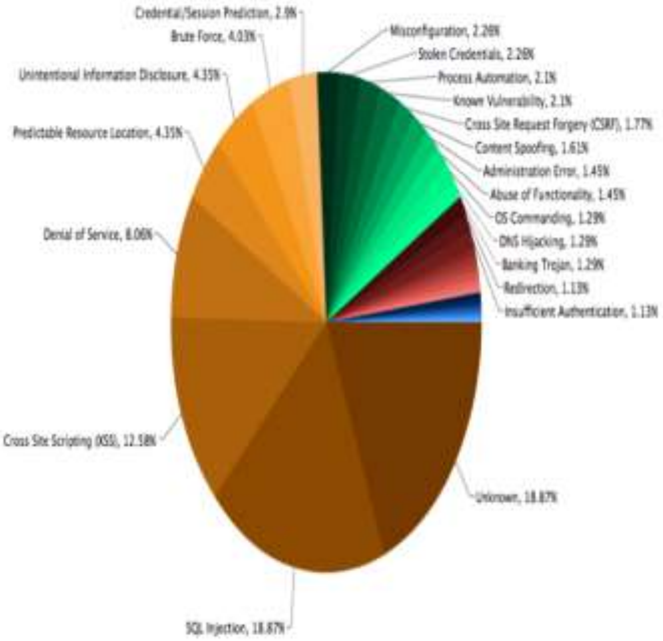

Fig. 1: percentage of data effected by various risks [1]

[Source:https://techtimely.wordpress.com/2011/04/22/web-hacking-threats/]

## III. CYBER CRIME

Cyber Criminals are the group of persons or a person which takes advantage of vulnerability of computer or network to access someone's secret data for their own profit. By AITP (Association of information technology professionals), computer crime can be defined as [7]:

- Unauthorised use or access of hardware, software or networking resources.
- Unauthorised piracy or copy of software
- Unauthorised revealing of information
- Denial of service to an authorised person who lawfully allowed to access that service.

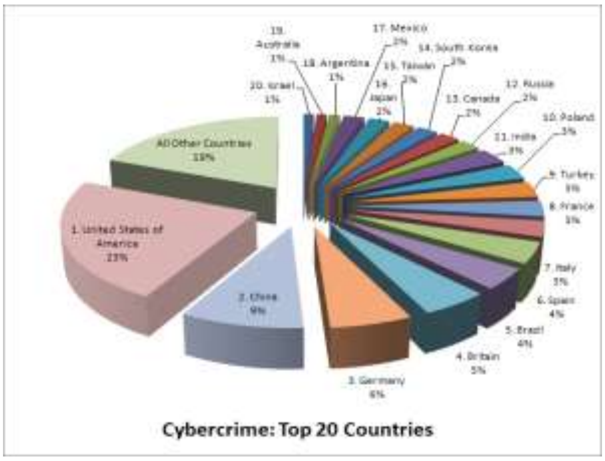

Fig. 2: Showing Cyber Crime in Top 20 Countries [4]

[Source:https://theluckylover.files.wordpress.com/2014/02/cybercrime-top-20-countries-pie-chart.jpg]

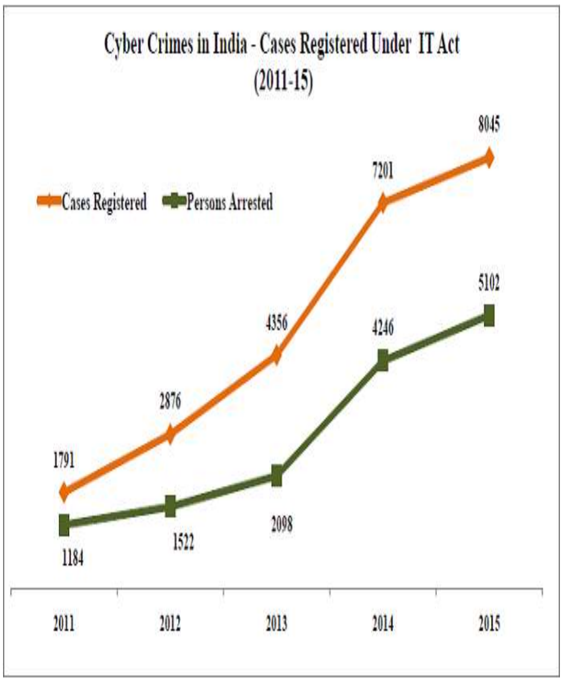

Fig. 3: Increase in Cyber Crime in India (2011-2015) [5]

[Source:https://i1.wp.com/factly.in/wp-content/uploads//2015/03/cyber-crimes-in-india_cyber-crimes-registered-under-it-act.png?ssl=1]

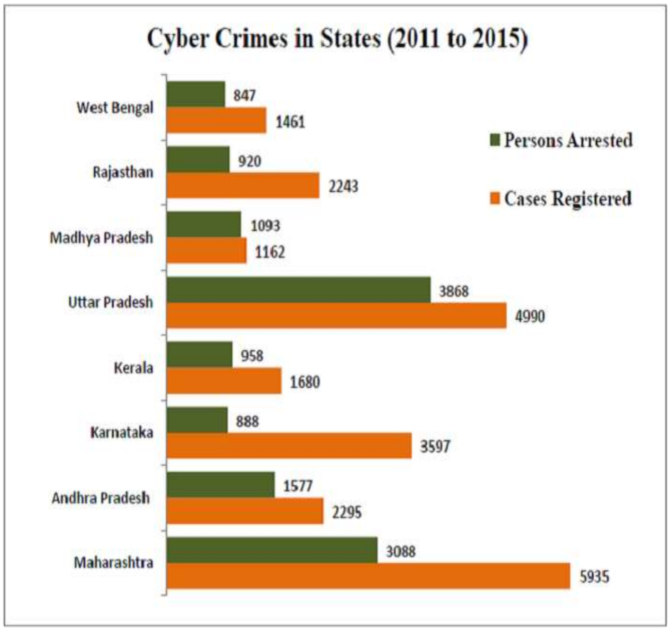

Fig. 4: Cyber Crime in Top Seven States in India [6]

[Source: https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/]

## IV. MAIN CHALLENGES IN CYBER SECURITY:

a. Hackers are not going to quit their bad activities.
b. The need of the future IT workforce is changing at a very rapid rate.
c. Stakeholders need to cooperate and help with one another on a great scale.
d. Leaders are aware of cybersecurity issues, but do not have the perfect knowledge of what to do next.

e. As we increase our global connections through The Internet of Things (IoT), so will provide more chances for the attacker to attack.

f. There is significant gap time between data breaches and detection [8][9].

## V. CYBER SECURITY TECHNIQUES:

A. Computer access control: Who can access what within a system should be fixed to get a better security. It basically consists:

- Identification
- Authorization
- Authentication

B. Application Security: It emphasis to improve the security of an application in different ways:

- Antivirus software
- Secure coding
- Security by design
- Secure operating system

C. Data centric security: This is an approach to security that emphasizes the security of the data itself rather than the security of networks, servers, or applications. Data-centric security is evolving rapidly as enterprises increasingly rely on digital information to run their business and big data projects become mainstream.

D. Encryption: It is a process of encoding the personal data into some other form which can br decoded by the authorized person only and not accessed by the person who is not authorised.

E. Firewall: A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware [13].

F. Authentication: Authentication should be mandatory for any document coming from other sources to know whether it is coming from an authentic user or not.

G. Intrusion detection system: It is a software placed to keep record of any irregular or unusual activity, policy violating activity happen to a system and trigger an alarm on occurrence of these.

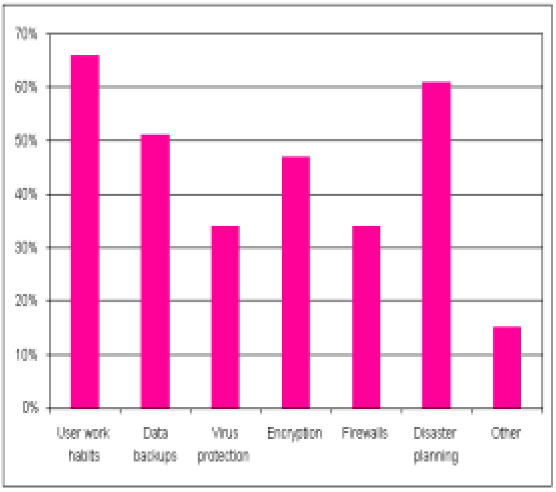

Fig. 4: Data Protection with Different Techniques

## VI. CONCLUSION

Cyber security is a vast concept that is becoming more important and delegate because the world is becoming highly interconnected, with networks or internet being used to carry out secret transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. Due to the enhancement in cyber-terrorism and crime, it is mandatory to build systematic education and to strengthen operational military, intelligence, police and civil centres for the protection from cyber-attacks. After having the knowledge of various kinds of threats increasing day by day, we can conclude that cyber security has become one of the major requirements of the democratic concept of life in the contemporary society.

## VII. REFERENCES

1. Online:https://techtimely.wordpress.com/2011/0 4/22/web-hacking-threats/. [Accessed: 08/03/2018]
2. Richa Garg et al. , "Security, privacy and trust in social networking sites", IEEE, 2015, pp. 14-18.
3. Mini Ulanat et al. , "Privacy security settings- Challenges of social media", IEEE, 2015, pp. 26-28.
4. Online:https://theluckylover.files.wordpress.com/2014/02/cybercrime-top-20-countries-pie-chart.jpg [Accessed: 09/03/2018]
5. Online:https://i1.wp.com/factly.in/wp-content/uploads//2015/03/cyber-crimes-in-india_cyber-crimes-registered-under-it-act.png?ssl=1. [Accessed: 10/03/2018]
6. Online:https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/. [Accessed:10/03/2018]
7. D. G Jha et al. , "Importance of Morality, Ethical Pratices and Cyber Laws as Prelude to Cybersecurity", IEEE, 2015, pp. 29-32
8. N. Choucri et al. , "Lost in cyberspace: harnessing the Internet, international relations, and global security," Bulletin of the Atomic Scientists, vol. 68, no. 2, 2012, pp. 70-77.
9. H. Lin et al. , "A virtual necessity: some modest steps toward greater cybersecurity," Bulletin of the Atomic Scientists, vol. 68, no. 5, 2012, pp. 75-87.
10. Duić et al.' "International Cyber Security Challenges" MIPRO, 2017, pp. 1525-1529, [Available: https://bib.irb.hr/.../878827.Duic_Cvrtila_Ivanjko_International_cyber_security_chall... ]
11. Roshan Jabee et al., " Issues and Challenges of Cyber Security for Social Networking Sites (Facebook)" International Journal of Computer Applications (0975 – 8887) Volume 144 – No.3, 2016, pp. 36-40, [Available: https://pdfs.semanticscholar.org/b501/886f966f87e47115d390afbbda017506e1.pdf]
12. Chakib Bekara et al. "Security Issues and Challenges for the IoT-based Smart Grid", ELSEVIER, Volume 34, 2014, pp. 532-537, [DOI:https://doi.org/10.1016/j.procs.2014.07.064]
13. Micheal Decker et al., "Location Privacy- An overview" IEEE, 7th international conference on Mobile Bussiness, 2008, [DOI: 10.1109/ICMB2008.14]
14. K Kimachia, "Five facebook threats that can infect your PC" Available: http://www.makeuseof.com/tag/five-facebook-threats-can-infect-pc-work/. [Accessed: 08/03/2018]
15. Online:https://en.wikipedia.org/wiki/Malware. [Accessed: 09/03/2018]