Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 4, March-2019, ISSN 2230-7540

Cyber Security Challenges and Its Emerging Trends on Cloud Security Issues and Techniques

Dr. Sandeep Kumar[1]* Prof. Arjun Singh[2]

[1] MCA from Kurukshetra University Kurukshetra, PhD from Singhania University

[2] MCA, M. Tech (CSE), from Kurukshetra University, Kurukshetra

Abstract – Cyber Security plays an important role in the field of information technology. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many.

Keywords: Cyber Security, Cybercrime, Cyber Ethics, Social Media, Cloud Computing, Android Apps.

----------X----------

1. INTRODUCTION

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cybercrimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cybercrime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information.

2. CYBER CRIME

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cybercrime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent

programs. As day by day technology is playing in major role in a person's life the cybercrimes also will increase along with the technological advances.

3. CYBER SECURITY

Cyber terrorism (Section 66F) under the IT Act: There were 13 registered cases related to cyber terrorism across the country. Himachal Pradesh had 5 registered cases related to cyber terrorism, which was the highest in the country. While Assam had 4, other states such as Kerala, Tamil Nadu, West Bengal had 1 each.

Frauds related to ATM, online banking, One Time Password (OTP) under section 465, 468-471 IPC

ATM		Online Banking Frauds		OTP Frauds	
Maharashtra	598	Maharashtra	345	Madhya Pradesh	122
Bihar	324	Odisha	116	Andhra Pradesh	62
Odisha	168	Telangana	111	Telangana	61
Uttar Pradesh	120	Uttar Pradesh	69	Uttar Pradesh	18
Telangana	56	Gujarat	42	Rajasthan	16
India total	1543	India total	804	India total	334

Table I

Fake news on social media (Sec. 505) under the IT Act: Section 505 of the IPC is for statements conducing to public mischief. As per the report, a total of 170 cases were registered for cases related to fake news on social media platforms. List for the top five states has been given below:

State	No. of Cases
Assam	56
Uttar Pradesh	21
Madhya Pradesh	1
Odisha	13
Kerala	12
Total India	170

Online gambling under the IT Act cases: States such as Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Goa, Himachal Pradesh, Tamil Nadu, Rajasthan, West Bengal, and Tripura did account for any registered case for online gambling. Details for the top five states have been given in the table below:

States	No. of cases
Jharkhand	16
Madhya Pradesh	10
Uttar Pradesh	3
Maharashtra/ Punjab	2
Karnataka	1
Total India	45

It is worth noting that the central government had set-up the National Informatics Centre – Computer Emergency Response Team (CERT-In) and the Home Ministry had set up the Indian Cyber Crime Coordination Centre (14C) to combat cybercrime in the country.

4. TRENDS CHANGING CYBER SECURITY

Here mentioned below are some of the trends that are having a huge impact on cyber security.

4.1 Web servers:

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

4.2 Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words, the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

4.3 APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cybercrime ware. For years network

security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

4.4 Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile network's security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes a lot of care must be taken in case of their security issues.

4.5 IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cybercrime.

5. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information.

The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in *Global Risks 2013* report.

Though social media can be used for cybercrimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However, companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

6. CYBER SECURITY TECHNIQUES

6.1 Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

6.2 Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti-virus software present in the devices. Thus, a good anti-virus software is also essential to protect the devices from viruses.

6.3 Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

6.4 Firewalls

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.

6.5 Anti-virus software

Antivirus software is a computer program that detects, prevents, and acts to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti-virus software is a must and basic necessity for every system.

7. CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

- DO use the Internet to communicate and interact with other people**.** Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world
- Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- Do not operate others accounts using their passwords.
- Never try to send any kind of malware to other's systems and make them corrupt.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

8. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

1. A Sophos Article 04. 12v1.dNA, eight trends changing network security by James Lyne.
2. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
3. Computer Security Practices in Non-Profit Organisations – A NetAction Report by Audrie Krause.
4. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
5. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry "by G. Nikhita Reddy, G. J. Ugander Reddy
6. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
7. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

Corresponding Author

Dr. Sandeep Kumar*

MCA from Kurukshetra University Kurukshetra, PhD from Singhania University