Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 4): pp. 3981-3987
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.435

Cyber Security: Challenges And Emerging Trends On Latest Technology

Kamelsh Chandra Purohit[1] , M. Anand Kumar[2] and Anuj Singh[3] , Ms. Shweta Chauhan[4]

[1] Associate Professor, Department of Computer Science, Graphic Era Deemed To Be University, Dehradun, India.

[2] Professor, Department of Computer Science, Graphic Era Deemed To Be University, Dehradun, India.

[3,] Assistant Professor, Department of Computer Science, Graphic Era Deemed To Be University, Dehradun, India.

[4]Assistant Professor, School of Management, Graphic Era Hill University, Dehradun
Purohit_kaml@rediffmail.com

Abstract- With advancement in technology day by day, technology made our life very easier and smart. However, there are some issue and challenges are come with these new technologies. In this paper, we are going to discuss current challenges and latest emerging trends about Cyber-security under Network Security. Today, all the information of any office, bank, state, country and many more are stored on cloud infrastructure. But the internet hackers break the security of these cloud server which is the very danger crime. So, Network-security helps us to protect our data from Cyber-attacks. It is also known as Information Technology Security. This study first discusses importance of cyber security today like about different types of Cyber-crime and its effect. Second, we will discuss block chain, and hash function of Network security. Further, we will discuss some new idea for improvement in Network Security.

Keywords- Cyber Security, Block chain, Hash, Cyber-attack, IT, Security.

1. INFORMATION:

The information technology industry is the main component at present time. This industry mainly deals in e-commerce service, IT enabled service, software service, application service, social media platform and many more. Today, IT industry is providing free communication platform like WhatsApp, Facebook, Messenger, Telegram and may more. People are able to communicate with other through these platforms. They are sending their private information, audio and video through these platforms. We all think that the information which we are sharing is fully safe. Even the service providers companies claims that they use end to end encryption security to secure our communication. But, is our communication is really secure? We all have same question. Almost 55-60% of total trades are conducting on web platform in now days. With these above changes in IT industry, Cybercrimes are also growing day by day. Cybercrimes are the main challenges of IT Industries today. Some of the IT service like Net Banking, online payment, distributed computing etc. need high secure protection. This service contains person important data, his financial wealth and personal data. Also, there is need to be aware the people about Cyber security, since maximum no of people don't know whether the website which they are using is secure or not. Website phishing incident is increasing day by day. [1] [2] Since all countries are preparing to enabled all type of communication through online mode. They are using their own cloud service to store all types of data, secret documents. So, there is possibility that any country can try to hack these secret documents, data of other country. Here Cyber Security play a big role to secure our data, data and secret document of any country. In this paper, we are going to discuss new challenges, latest trends in Cyber Security. We will discuss how important is the Cyber Security important for any country.

The current cybercrime search system used by the police, because there is no mathematical method to effectively analyze search records, the complexity of information, it is difficult to reflect the spatial logic and relationship of cybercrime [2]. Second, cybercrime has the characteristics of criminals, criminal acts and spatial separation of the results of criminal activity. The scope of crimes is not limited by location. In particular, large numbers of simultaneous crimes, coordinated crimes in multiple locations and overseas criminal behavior are very difficult to track and prevent. However, cybercrime itself often has strong mathematical characteristics of spatial and temporal distribution [3]. For more than 30 years, factor space theory has been a preliminary framework for concept representation, decision reasoning, neural networks, information fusion, etc., and has achieved initial successes in the field of applications. Liu Zengliang [5] proposed a factorial neural network for military science. The attribute theory proposed by Feng Jiali [6] is also complementary to the study of factor space theory. For more than 30 years, factor space theory has been a preliminary framework for concept representation, decision reasoning, neural networks, information fusion, etc., and has achieved initial successes in the field of applications. Liu Zengliang [5] proposed a factorial neural network for military science. The attribute theory proposed by Feng Jiali [6] is also complementary to the study of factor space theory.

ABOUT CYBER CRIME:

Cybercrime is a type of criminal activity in which computer, network device and computer related device are involved. Cybercrimes are happened either to generate income and profit for Cyber criminals or to damage and disable the computer and security devices. Sometimes, Cyber criminals use their computer to spread malware to get illegal information like images, videos, secret documents and other materials. [3] To damage any system, they target the computers to infect directly with a computer virus, this virus then spread to all entire machines which are connected to that targeted computer. As technology is growing day by day, The Cyber attackers are constantly seeking new methods and techniques to carry out their goals while avoiding the trace and arrest. We can divide the type of Cybercrime in some parts and they are:

a) Cyber-Extortion: When a Cyber attacker gains an access of any organization's computer network and access all files and documents of that organization to denied the access of Organization's access. This type of attack is called Cyber extortion attack. Usually, the Cyber attackers do these types of attacks to demand the money, and when they get their ransom, they give back their computer access to him. The money they demand are in the form of Cryptocurrency. Below figure 1 is showing the statistic of Cyber Extortion.

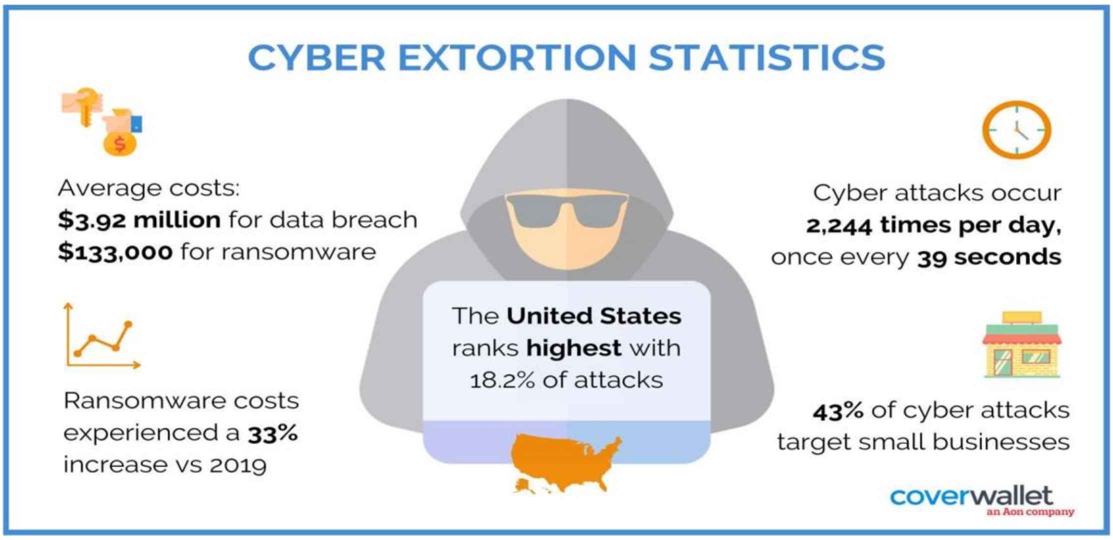

CYBER EXTORTION STATISTICS
Average costs:
$3.92 million for data breach
$133,000 for ransomware
Ransomware costs experienced a 33% increase vs 2019
The United States ranks highest with 18.2% of attacks
Cyber attacks occur 2,244 times per day, once every 39 seconds
43% of cyber attacks target small businesses
coverwallet
an Aon company

Figure 1. Cyber Extortion Statistics

b) Credit/Debit Card Fraud: In this type of Cyber fraud, the Cyber criminals collect the person data like, contact, name, bank account in which the person has account, by paying the money to call centers and other it companies. After that they call the user and make him trust that they are calling from bank or any other financial institution, and ask them to share their transaction OTP, and after sharing the OTP, the attacker’s nil their bank account [4][5].

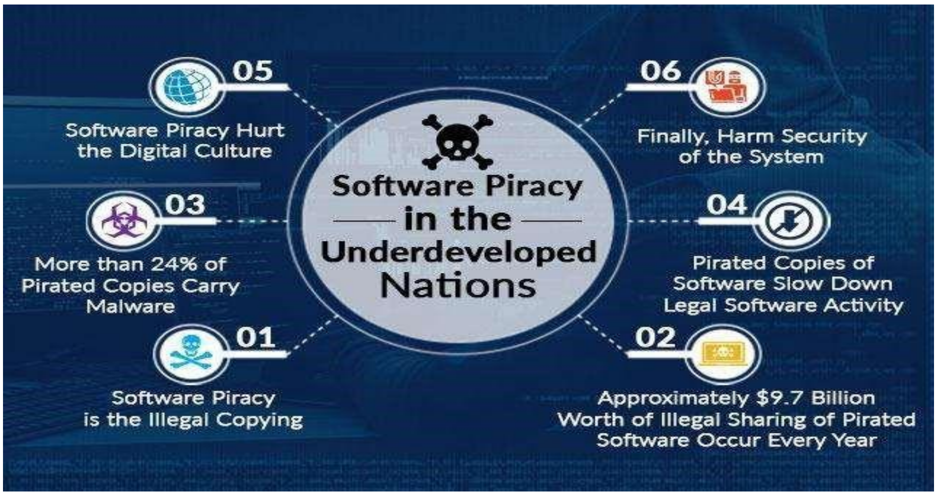

Software Piracy in the Underdeveloped Nations
05
Software Piracy Hurt the Digital Culture
06
Finally, Harm Security of the System
03
More than 24% of Pirated Copies Carry Malware
04
Pirated Copies of Software Slow Down Legal Software Activity
01
Software Piracy is the Illegal Copying
02
Approximately $9.7 Billion Worth of Illegal Sharing of Pirated Software Occur Every Year

Figure 2. Software Piracy Issue in Undeveloped Country

c) Software Piracy: In this, the Cyber attacker make the website/software which is same as the bank or any company are used. The attacker shares the pirated website link to user through social media link, text messages. Hackers are using this method for Cyber attacking in now days. Above figure 2 is showing that how the software piracy is the one of the challenging for the underdeveloped country [9].

Crypto jacking Cyber-crime: Today, new innovation in every field is growing day by day. Cryptocurrency is one of the new types of currency, which is very famous today in the world. This is the common virtual currency for all the country. What Cybercriminal do is they continuously track the user website and when the user opens their account in browser and in the same browser, they open one other tab which is unauthorized, they take access the user account and nil their Cryptobalance. Figure 3 is showing the latest reports of Crypto Jacking in the UK.

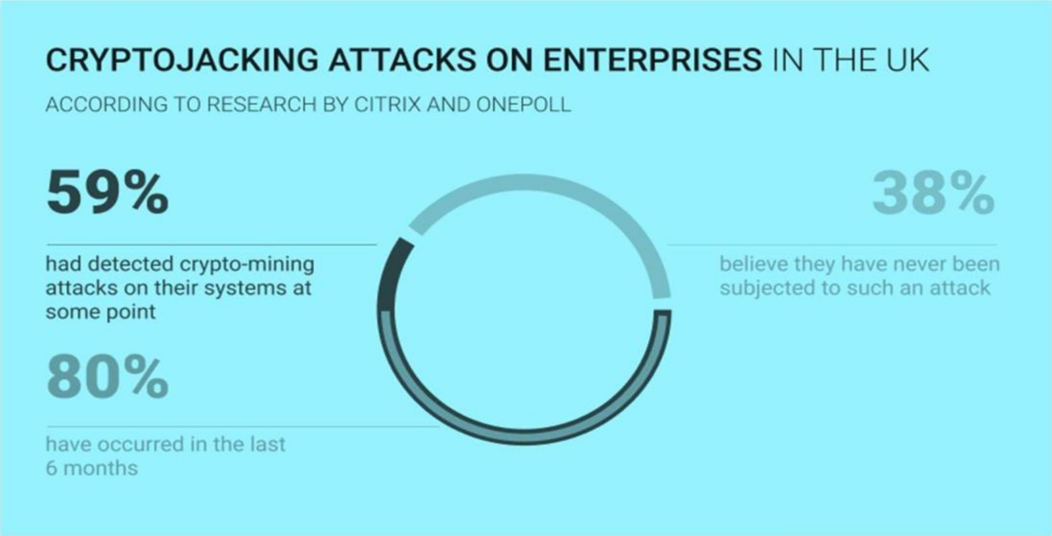


Figure 3. Crypto Jacking Attacks in UK

d) Cyber Espionage: This is the most dangerous attack by Cyber attackers. The only motive behind this attack is to disrupt and theft the legal/private documents, latest research documents either of any competitive company or any country. We may call this attack as a SPY. Behind of this attack, there may be any corporate company or any country.

2. EFFECTS OF CYBER CRIME:

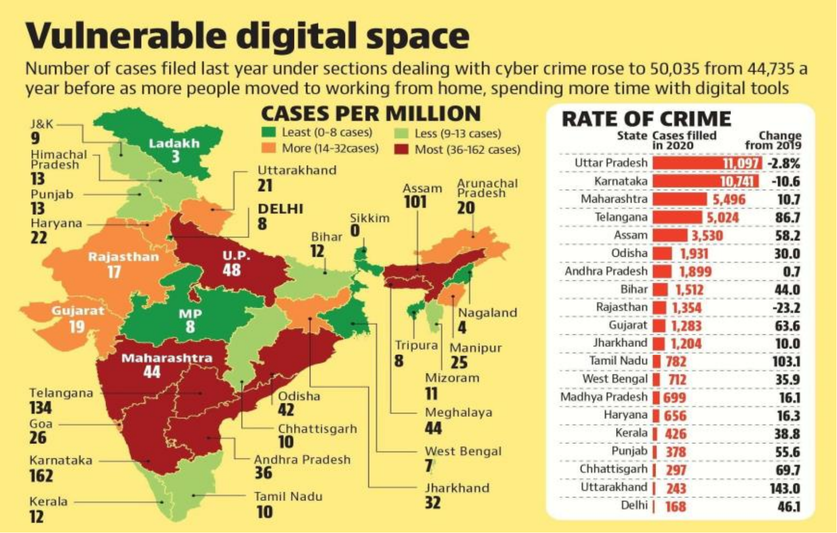
Actually, we can’t estimate and get the true cost of damage happened by Cybercrime fraud currently. However, we are sharing some current reports of Cybercrimes here.

a) Effect on Business: As per report published by McAfee on December 2020, the report is saying that the growing of Cybercrime Day by day is going to cost the world economy by $1 Trillion, which is more than the 1% of the World GDP.
Comparing with previous report of 2018, this damage is jumped by 50%.

b) Damage the Company: Attack on Network Security of any company totally damages the base of that respective company. The value of the share of that company is fallen down. They get loss data, projects information, patent etc.

c) Effect on National Defense Security: Attack on National Defense Security is going to be big challenges for any country. Today, every country is using cloudbased storage service to store, share private data, information. However, it has been seen that one country is attacking on other country which is called CYBER WAR. Figure 4 is showing the official data released by NCRB in which we can see the no of Cybercrime reports records in India during financial 2019-20. Same Figure 5 is showing the Cybercrime records in other country. [8]

.



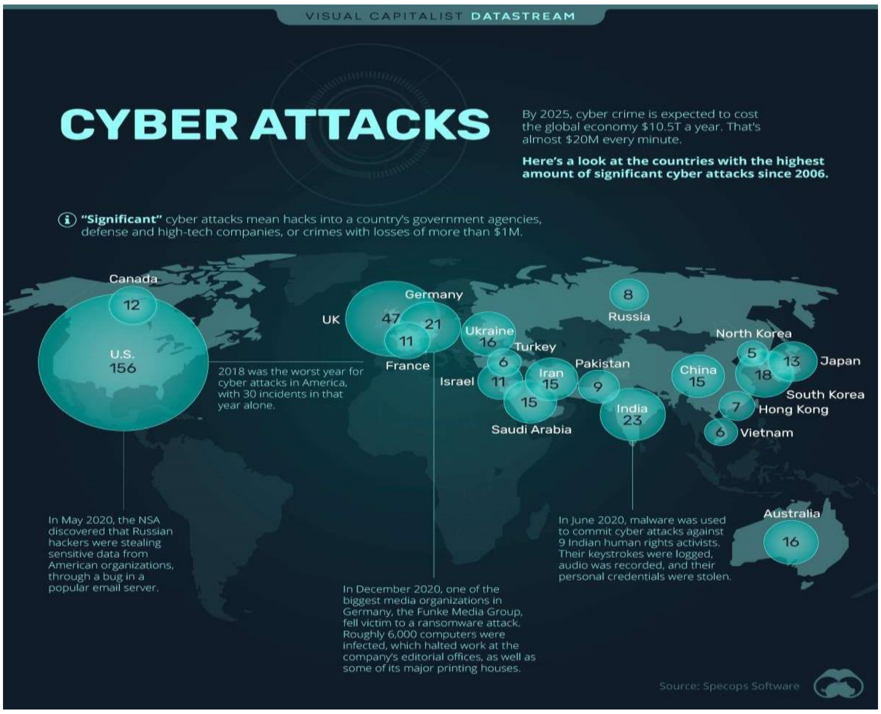
Vulnerable digital space

Number of cases filed last year under sections dealing with cyber crime rose to 50,035 from 44,735 a year before as more people moved to working from home, spending more time with digital tools

RATE OF CRIME

State	Cases filled in 2020	Change from 2019
Uttar Pradesh	11,097	-2.8%
Karnataka	10,741	-10.6
Maharashtra	5,496	10.7
Telangana	5,024	86.7
Assam	3,530	58.2
Odisha	1,931	30.0
Andhra Pradesh	1,899	0.7
Bihar	1,512	44.0
Rajasthan	1,354	-23.2
Gujarat	1,283	63.6
Jharkhand	1,204	10.0
Tamil Nadu	782	103.1
West Bengal	712	35.9
Madhya Pradesh	699	16.1
Haryana	656	16.3
Kerala	426	38.8
Punjab	378	55.6
Chhattisgarh	297	69.7
Uttarakhand	243	143.0
Delhi	168	46.1

Figure 4. Cyber Crime Reports Recorded in India in 2019-20.



VISUAL CAPITALIST DATASTREAM

CYBER ATTACKS

By 2025, cyber crime is expected to cost the global economy $10.5T a year. That's almost $20M every minute.

Here's a look at the countries with the highest amount of significant cyber attacks since 2006.

"Significant" cyber attacks mean hacks into a country's government agencies, defense and high-tech companies, or crimes with losses of more than $1M.

2018 was the worst year for cyber attacks in America, with 30 incidents in that year alone.

In May 2020, the NSA discovered that Russian hackers were stealing sensitive data from American organizations, through a bug in a popular email server.

In December 2020, one of the biggest media organizations in Germany, the Funke Media Group, fell victim to a ransomware attack. Roughly 6,000 computers were infected, which halted work at the company's editorial offices, as well as some of its major printing houses.

In June 2020, malware was used to commit cyber attacks against 9 Indian human rights activists. Their keystrokes were logged, audio was recorded, and their personal credentials were stolen.

Source: Specops Software

Figure 5. Cyber Attacks in Different Country.

4. CYBER CRIME PREVENTION & TYPES OF NETWORK SECURITY:

As discussed above, there is a need to develop network security tools so then it becomes more effective. Today, the world is changing into digitalization. With this digitalization, the service provider company, organizations want to protect their organization data so then their service will run smoothly. Below we are discussing some important network security protections types, which can be useful for these organizations.

a. Network Access Control- NAC is a type of network security which only allows the trusted and authenticated endpoint devices to access the respective network resources and infrastructure.

b. Application Security- It is the process to develop and add the latest security features within an application.

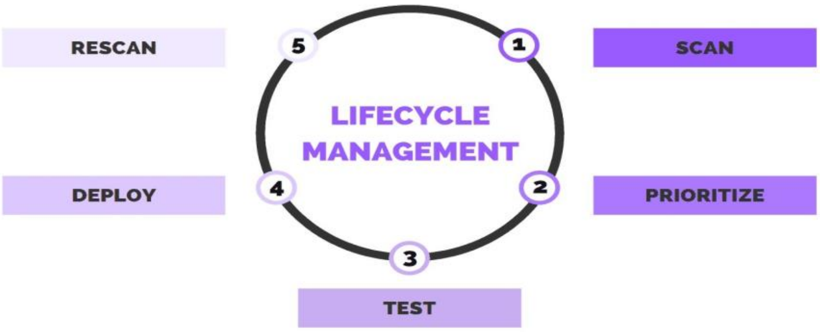


Figure 6. Application Security Process

c. Network Penetration Testing- It is used to test and measure security concern of IT infrastructure for safely exploiting vulnerabilities.

d. Antivirus Software- It is the most important type of software used in any computer to scan, identify and prevent or delete the virus from the computer.

Figure 7. Antivirus Working Structure

e. Endpoint Detection and Response- EDR technology is used to continuously record any system activities and detect if any event takes place on endpoint.

f. Hashing- Hashing is basically a procedure in which any given key translates into a code. Any hash function is used to replace the newly generated hash code. Hash algorithms are used to change the provided file into digital copy so then no virus or intruder can change the original file. Hash functions are also used to encrypt the operating system passwords.

g. Virtual Private Network- VPN provides an encrypted connection between the connected device over the networks. This encrypted network connections ensure the transmission of sensitive data safely [8-10].

5. CONCLUSION:

In this paper we have discussed about the latest challenges because of cybercrimes and then we have discussed different types of network security which can help the IT industries to protect against Cybercrimes. In 2020, India ranked the highest number of cybercrimes cases, which was almost 4.5 million. Cybercrime is one of the fastest growing criminal behavior in which cybercriminals access the any organization computer system using unauthorize access called hacking. We have discussed different types of cybercrimes in this paper above. We have also discussed latest network types and discussed that how the network security can prevent the hacking.

REFERENCES

[1] Upadhyay, V. and Yadav, D. S., “Study of Cyber Security Challenges Its Emerging Trends: Current Technologies”, (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018.

[2] Mitra， D., and Wang, Q. “A model-based study of the impact of managed services and the spawning of applications in broadband networks”. International Telegraphic Congress, 2012.

[3] Mavodza, J. “The impact of cloud computing on the future of academic library practices and services”. New Library World 2013, vol.114, pp.132-141

[4] Wang P Z, Sugeno M. The factor fields and background structure for fuzzy subsets. Fuzzy Math, 1982, vol.2, pp.45-54.

[5] Zhengliang, L., and Youcai, L. “Research on Factor Neural Network Theory and Implementation Strategy”. Beijing Normal University Press, 1992.

[6] Jiali, F. “The theory of nature in thinking and intelligent science”. Atomic Energy Press,1990.

[7] Ping He, Kaiqi Zou, “Research of Crime Inversion Fuzzy Neural Network Based on Factor Space”. 2016, vol. 10, pp.1943-1950.

[8] Rajasekharaiah, K. M., Chhaya S. Dule, and E. Sudarshan. "Cyber security challenges and its emerging trends on latest technologies." IOP Conference Series: Materials Science and Engineering. Vol. 981. No. 2. IOP Publishing, 2020.

[9] Rajasekharaiah, K. M., Chhaya S. Dule, and E. Sudarshan. "Cyber security challenges and its emerging trends on latest technologies." IOP Conference Series: Materials Science and Engineering. Vol. 981. No. 2. IOP Publishing, 2020. doi:10.1088/1757899X/981/2/022062

[10] Reddy, G. Nikhita, and G. J. Reddy. "A study of cyber security challenges and its emerging trends on latest technologies." arXiv preprint arXiv:1402.1842, 2014.