WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Investigate Recent Challenges Cyber Security and its Solutions

Prathamesh Valmik Patil

Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra
paddypatil2000@gmail.com

ABSTRACT

The current era, where the use of the Internet is increasing day by day, can be called the era of the Internet. Every coin has two sides, just like the coins of the internet. He shows on one page how easy it is to communicate, share information, market, and do business on the Internet. On the one hand, this comes with significant security concerns. Cybersecurity is a field committed to protecting networks, data, electronic devices, servers, and computers from malicious attacks. According to cybersecurity, it means staying one step ahead of hackers and preventing system abuse. Hackers are getting smarter every day, creating new challenges for cybersecurity professionals. Reports of threats like ransomware, phishing, vulnerability exploits, and IoT-based attacks are all around us these days. The current study describes well-known and common challenges, highlights some emerging challenges in cybersecurity, and proposes possible solutions to overcome them.

KEYWORDS: Cyber Security, Cyber Criminals, Hackers, DDoS, Phishing, Malware, Ransomware, Internet of Things, Artificial Intelligence, Cloud Risk, Mitigation, Technical Skills Gap, Anti-Security Tools, Antivirus.

I. INTRODUCTION

Cybersecurity refers to the process of providing protection to Internet-connected systems such as computers, servers, mobile devices, electronic systems, programs and data from attack, damage or unauthorized access. In other words, Cyber security is a set of methods, technologies, and processes that help protect confidentiality, integrity, and availability of computer systems, networks and data against cyber-attacks or unauthorized access. Cyber security sometimes is referred to as information security. Cybersecurity is critical because government, military, corporate, financial, and medical organizations collect, process and store unprecedented amounts of data on computers and other devices Telling Fraction this data may be sensitive information, whether it is intellectual property, financial data, personal data or other types data to which unauthorized access or exposure could have negative consequences. Organizations transfer sensitive data networks and other devices in the course of business. It protects all types of data from theft or damage, including sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, government and industry information systems. , and practiced by companies. Without a cybersecurity program, it's nearly impossible for an organization to protect itself from cyberattacks and threats. With the emergence of new technologies such as cloud services such as Amazon Web Services, the need for cyber security has increased. The current research identifies several emerging cybersecurity challenges, outlining some known common challenges and proposing solutions to overcome them. .

II. KNOWN SECURITY CHALLENGES

Below are some well-known cybersecurity challenges

2.1 DDoS Attack:

DDoS stands for Distributed Denial of Service Attack. In a DDoS attack, cybercriminals flood a network with large amounts of malicious traffic that is difficult to operate normally, freezing the normal operation of a website (generally legitimate packets). The goal of a DDoS attack is to overload a server with access requests until it eventually crashes due to a denial of service. DDoS attacks, among all other attacks, prevent clients and users from accessing all the benefits of services available from the server side [1]. A DoS attack is an attempt by an individual or group to stop an online service, with serious consequences, especially for companies such as Amazon and eBay, whose businesses depend on being available online [2]. As outlined in McAfee's Consumer Threat Report, the deployment of 5G, the proliferation of the Internet of Things and smart devices, and the industry's upcoming move online have created new targets for DDoS attacks. Cybercriminals are using leverage and in 2020 two of his biggest ever DDoS attacks were launched against his Amazon and Google.

DDOS attacks fall broadly into his two categories:

Flood Attack and Flash Crowd Attack. Flood DDoS attacks eat up resources such as network bandwidth due to overwhelmingly narrow connections and high packet volumes. Flash Crowd attacks take advantage of the predictable behavior of protocols such as TCP and HTTP to their advantage [2].

2.2 Phishing:

Phishing is the practice of circumventing security by using aliases or by sending emails falsely claiming to be from a legitimate organization [3]. This is usually combined with a threat or information request.

For example, your account is closed, your balance is due, or your account is missing information. The email asks the recipient to provide sensitive information such as banking details, PIN, and password. This data is used by website owners for fraudulent activities. The phishing website looks like her real website and the end user is unaware that they have been redirected. However, data hacking through phishing can be avoided by avoiding clicking unknown links from web aliens [4]. Phishing attacks impact organizations and individuals and face significant losses, including fines, information laws and regulations, reputational damage, recovery costs, and lost productivity [5]. Phishing in other directions launches attacks such as phone calls, instant his messaging, and physical letters in addition to email. However, technical methods include phishing scams, phishing emails, fake websites, phone phishing, and social media phishing [6].

2.3 Malware:

Malicious software (malicious software). Malware is delivered uninvited from multiple sources, including website pop-ups, spam, emails, and downloads from unknown sources [7]. Malware types are spyware, Trojans, virus attacks, worms, adware, and logic bombs. It is the most pervasive threat to systems [8].

Computer viruses are designed to replicate and spread. The virus spreads to each contact through the victim's email her account. Virus replication can cause network traffic to become very heavy, leading to network slowdowns [9]. Electronic Trojans work similarly to the famous story of a Trojan horse used to infiltrate the city of Troy. Malicious software disguised as a legitimate program [10]. Spyware is a program that monitors activities running on your computer system. As you browse the Internet, spyware is downloaded and uses your system browser to create plain text files. Saved to disk. Later, each data storage can be retrieved from any of his websites as a flat file, thus allowing the computer's entire internet browsing history to be tracked[11]. Another type of spyware is called a keylogger, which records every user's keystrokes. A worm virus is malicious, self-replicating software that spreads automatically over a network. Adware is software that supports advertisements.

2.4 Internal Abuse:

When an insider compromises access rights or steals data, it's called an insider exploit. People contribute secure data to public sources. Protected data can be strategy documents, customer data, or even proprietary source code. An insider performing an attack (an internal attack) has authentication to access the system and may also be familiar with the network architecture and system policies and procedures, thus making also have distinct advantages [12]. Employees can be authorized with a single trust for multiple physical devices within the organization to prevent damage or theft. Hardware such as a hard drive containing a lot of important data can be physically destroyed, stolen from a company, data duplicated, erased, or transferred to a USB drive. . In addition, stored data can be destroyed by disasters such as floods, fires, terrorism, and power outages.

III. RECENT CYBER THREATS

3.1 Ransomware:

Ransomware is a family of malware that uses security techniques such as encryption to hijack user files and associated file resources, demanding cryptocurrency in exchange for the locked data [13]. Some ransomware enter systems through social engineering, malicious ads, spam, and automatic downloads, while others use open ports and backdoors to break into systems and discover vulnerabilities. [14]. The infection process begins by injecting malware into network computers, targeting human or technical vulnerabilities. Human weaknesses often result from opening and clicking on spam her messages, known as phishing emails. Technical flaws are based on a variety of factors, including: B. publicly accessible WiFi networks, inadequate firewall protection, etc.; After the infection process, cybercriminals modify the file system by encrypting the entire computer files and only allowing the victim to view messages and Bitcoin payment processes [15]. If cybercriminals hack your computer, it is almost impossible to decrypt your files unless they have the decryption algorithm or the decrypted key. For this reason, victims tend to pay cybercriminals to recover hostage data from criminals [16]. Ransomware is considered to be the fastest growing cyber threat that is gaining attention. Encrypt your files, block access to your system, or sew. When someone is hit by ransomware, hackers demand money depending on how important the data is and the size of the organization. When this happens, victims who are on the verge of data loss also suffer financial and productivity loss.

3.2 Cloud Risks:

Organizations are migrating sensitive data from traditional data centers to the cloud because of the flexibility and costs associated with traditional data centers. Moving data to the cloud requires proper configuration and security measures. Otherwise, you risk falling into a trap. Cloud service providers

only protect their platform, and it is the responsibility of the enterprise to protect its infrastructure from theft or deletion via the cloud. For cloud services, traditional endpoint-centric security operations tools do not serve as perimeters, and security gradually shifts from endpoints to cloud security controls, losing much of the insight [17]. The top five cloud risks are access control, data breaches and leaks, data loss, insecure APIs, and improperly configured cloud storage.

3.3 Artificial Intelligence:

AI is generally an ally of humans, using problem-solving and learning techniques to understand the high-level activity in the functioning, decision-making, and emotional cycles of human-inspired elements [18]. Artificial intelligence runs in parallel with cyber attacks and defenses. AI has revolutionized this era through trading and defense. You can't miss that AI acts not only on defense but also on the attack side. Biometric logins are an example of artificial intelligence. After a lot of research and modeling, AI can learn behavioral anomalies that can be used as defensive tools. Unfortunately, attackers can use these similar techniques to launch cyberattacks. The previous generation of cyberattacks focused primarily on data theft (extraction) and braking systems (intrusion). New forms of attacks against AI systems are aimed at controlling the target system and altering its behavior. His three types of attacks are especially important for gaining control:

Data poisoning, classification model enhancement, and backdoors [19]. Each of them learns to change their behavior using the abilities of the artificial intelligence system. For example, cybercriminals can insert carefully designed, malformed data into legitimate data. This is used to train the system to change its behavior**.**

3.4 Internet of Things (IoT):

The Internet of Things (IoT) is a set of interconnected objects, services, people, and devices that can communicate and exchange data and information in various domains and applications to achieve common goals [20]. Organizations are increasing their reliance on technology and exposing it to attack. With the rapid adoption of the Internet of Things (IoT), security threats have also increased dramatically. The commonly accepted IoT architecture includes three layers: Perception Layer (PL), Network Layer (NL), and Application Layer (AL). PL uses sensors to gather information about smart objects in the environment. NL is responsible for transmitting and processing data from sensors and connecting with other smart things, servers and network devices. AL provides users with application-specific services and ideas such as smart city, smart home, and smart healthcare. Attackers can exploit your IoT infrastructure by creating vulnerabilities at each of these layers. Her IoT applications such as smart TVs, security systems and wearable health meters collect user information that some hackers can access or share for illegal reasons. Security challenges in PL are eavesdropping, attack replay, and attack timing. NL threats include DoS, RFID spoofing, and sinkhole attacks. Finally, AL challenges are phishing, cross-site scripting, and malicious form/virus attacks.

3.5 Technical skills gap:

Media and Cyberattacks are on the rise around the world, and the sophistication and success of targeted cyberattacks is on the rise. There is an urgent need for cybersecurity professionals with the motivation and skills to prevent, detect, respond to and even mitigate the impact of such threats. A recent study by the Department for Digital Culture, Sport (DCMS) found that around **48% of** UK organizations were unable to perform core operations as defined by the government's Cyber Essentials programme, such as firewall setup and data storage. not. . I will do it. The report also claims that 30% of companies have advanced cybersecurity skills such as penetration testing and forensics. Businesses and organizations continue to face a critical shortage of highly qualified and reputable cybersecurity professionals. Lack of expertise leaves you vulnerable to cyber threats, leading to theft of confidential information, financial loss, and reputational damage [21]. The rapid growth of technology and the technical nature of cyberattacks is widening the gap between the relevant security knowledge gap and the rapid growth of cybersecurity professionals.

IV. SUGGESTED SOLUTIONS

4.1 DDoS Countermeasures:

The antidote to DDoS attacks is predictive analytics. Helps IT professionals investigate attacks and predict their likelihood and origin. Predictive analytics software powered by machine learning can gather key information about known cyberattacks and correlate the results with existing security logs. This is particularly effective for proactive DDoS mitigation, as cybersecurity systems can detect threats and take proactive action to redirect operations before systems are compromised. Another measure is to back up important data. There are other workarounds. You must give a username and password to anyone who has access to your router. Make sure all static connections have RPF on the router interface, disable telnet on the vtys, only allow SSH-based connections, and use vtys filters to prevent public routers from responding from the router. The router uses TACACS (Terminal Access Controller Access Control System) as the password. Validate, set up a security lab if this is not possible, provide at least one spare router and server to test new services, instead implement directly into the live network, minimize the number of transit providers. Benefits such as lower (possibly one), hiring cleaning centers that connect to other local ISPs, out-of-band management, and perhaps even better security lab setups [22].

4.2 Countermeasures against phishing:

The first line of defense against phishing attacks is to educate end users, be aware of phishing, and avoid visiting malicious links. It then prevents vulnerability-level attacks from occurring on the user's device and detects attacks when they are launched through the network layer. Finally, use law enforcement as a deterrent to overcome attacks [23].

4.3 Countermeasures against malware:

Many measures have been proposed to reduce the impact of malware on systems. Malware protection includes firewalls, security software, manual malware removal, and training. A firewall is a protection mechanism that controls and monitors incoming and outgoing network traffic. Depending on the perceived threat, allow or block such traffic based on security rules. Firewalls come in two varieties: hardware and software. There are several software firewalls such as Check Point Next Generation Firewalls (NGFWv), SonicWall, Official G2 Survey, Cisco Next-Generation Firewall Virtual (NGFWv), FortiGate NGFW, SophosXG Firewall, Microsoft Windows Firewall, Macfree, Symantec, TrenMicro, Sygare . zone alert. There is a lot of security software that should be protected as an anti-malware computer system, such as antivirus software, internet security software, removal tools, etc. Malware removal tools are used to scan and remove malware in your computer system. Microsoft offers several removal tools. They are Security Scanner, Malware Removal Tool, Diagnostic and Recovery Toolkit (DaRT), Emsisoft Emergency Kit, Avast Free Scanner, Malware Removal Tool, Malware Bytes. The main features of antivirus software include scanning executable files and real-time activity (file downloads, application activity monitoring, etc.). Here are some antivirus lists:

McAfee, Symantec, Norton, AVG, Kaspersky, Quick Heal. Internet security software has the following additional features compared to antivirus programs:

Anti-spyware, family and privacy protection, cross-device and cross-platform website blocking, online storage security. Security awareness training should be provided to employees to identify various threats.

4.4 Countermeasures against internal abuse:

Data breaches are usually caused by people's mental weakness. To avoid abuse in your company, it is important to educate your employees about warning signs of security breaches, safe practices such as:

When opening email attachments, be careful where you look and what you do if you suspect a hijack.

4.5 Ransomware Countermeasures:

As stated in Kaspersky's online article [24], countermeasures against ransomware are:

Never click on dangerous links, do not disclose personal information when receiving emails, calls or texts from untrusted sources, do not open suspicious email attachments, do not use unknown USB sticks, programs And keep your operating system up to date, use only known download sources, and use a VPN service on public Wi-Fi networks. In addition to these measures, use anti-ransomware software such as antivirus programs, content Internet security filters, and solutions such as Kaspersky Internet Solutions, Bitdefender Total Security, McAfee Antivirus plus to protect against cyberattacks. increase.

4.6 Countermeasures against cloud risks:

There are various cloud security measures such as firewalls, multi-factor authentication, and virtual private networks (VPNs). Gray Stevens [25] suggests precautions against the top five cloud risks. they are:

You can circumvent access controls by carefully designing access policies and setting up authentication and identity verification tools. By establishing secure communications and connections, you can manage data breaches and leaks. Avoid data loss caused by frequent data backups. Careful vendor selection limits unsafe APIs. Check if your cloud storage is configured correctly. configuration settings .

4.7 AI Countermeasures:

Maria Rosaria Tadeo and others propose three countermeasures against AI vulnerabilities. First, have a trusted vendor design and develop the model in-house. B. System training and testing data collected, validated and maintained directly by the system provider. For example, she can sabotage cloud systems to give attackers access to her AI models and training data. Second, opponent training is a deep way to improve the resilience of AI systems. Feedback loops allow AI systems to improve performance by repeatedly adjusting their own variables. As a result, training adversaries across AI systems can make attackers more resilient and help identify system vulnerabilities. Finally, paralle and dynamic monitoring helps assess the robustness of AI systems, the deception of attacks, and the ability of target systems to learn.

4.8 IoT Countermeasures:

Al[26] of the three different layers of IoT measures proposed by Mohamed Litoussi et al.

• Implement Perception Layer (PL), hash-based cryptography, public key infrastructure (PKI protocols), and lightweight cryptography.

• NL measures include identity management frameworks, software-defined networking (SDN) with IoT, and interworking of node communication protocols.

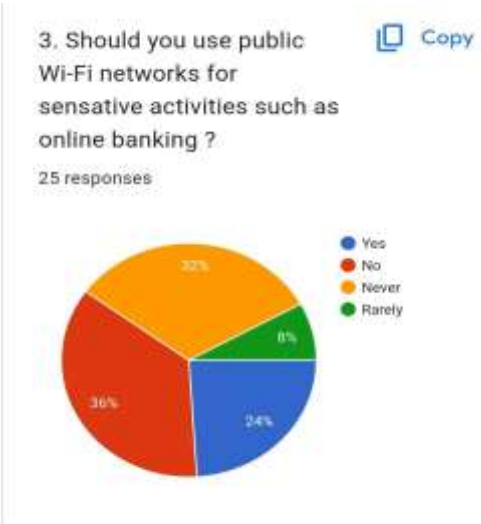
• Accordingly, AL protection is specific policies and permissions, antivirus, anti-adware and anti-spyware, and risk assessment techniques.

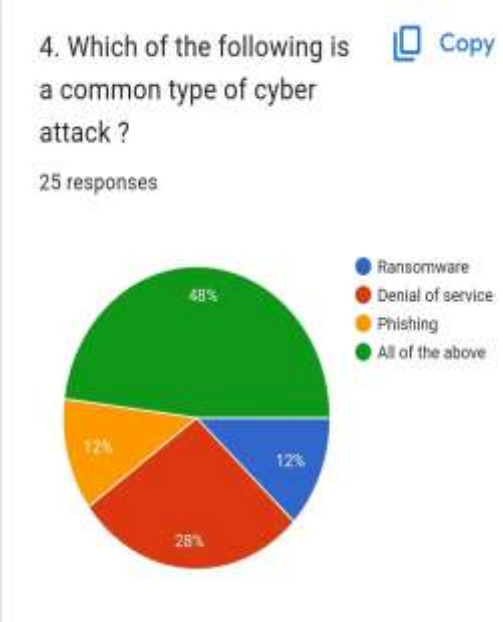
4.9 Technical Skills Gap Countermeasures:

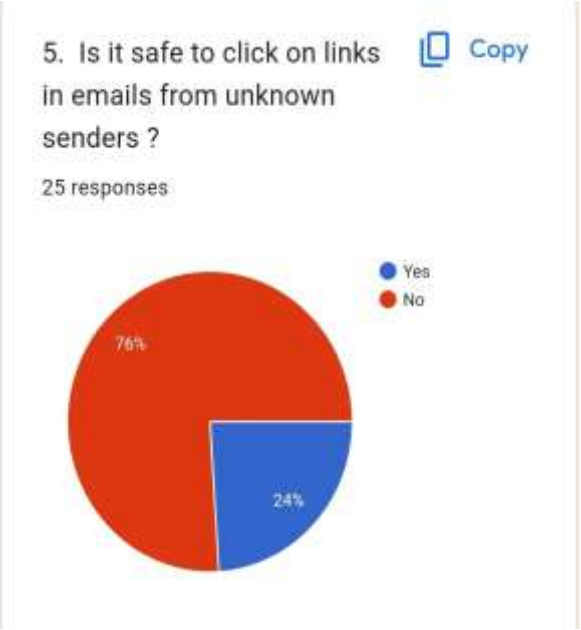
In 2020, thieves will be able to easily clone fraudulent identities, allowing hackers to exploit any vulnerability. Unless there is an equal number of resources with the right skills to solve the problem, it will only increase. Organizations must invest in training existing employees to prevent cyberattacks and hire new resources to analyze network threats. Otherwise, companies will have to accept huge financial losses.

V. PUBLIC SURVEY

We deployed our data gathering utility, often known as survey bot, to a variety of people and collection information on various facets of cybercrime/hacking impacts on young generation.







Conclusion

Cybersecurity is the set of methods, technologies, and processes that help protect the confidentiality, integrity, and availability of computer systems, networks, and data from cyberattacks and unauthorized access. Cybersecurity is sometimes called information security. Cyber threats and security attacks are nothing new to businesses and organizations. Thankfully, these have reached a certain degree of sophistication in recent years. Computer security is an important issue as the world is highly connected, including the networks used to conduct important transactions. Cybercrime, like information security, continues to evolve in many ways over the years. There are practices and technologies that businesses and organizations must employ to guard against external and internal threats. This research is being conducted to raise awareness of the challenges in dealing with various cyberthreats. These types of attacks also have an economic impact. End users should participate in training and awareness training to mitigate and manage these threats. Due to the complexity of the attack, historical user data and attack patterns should be investigated. Restructuring approach to minimize adverse impacts.

REFERENCES

[1] Sushmita chakraborty, Praveen kumar, Dr. Bhawna sinha, "A Study of DDoS Attacks, Threats and their Prevention", p. 1 International Journal of Research and Analytical Reviews (IJRAR) E-ISSN 2348-1269, P-ISSN 2349-5138, May 2019, Volume 6, Issue 2

[2] Anup Bhange, Amber Syad, Satyendra Singh Thakur, "The Impact of DDoS Attacks on Network Traffic and Their Detection Approaches," International Journal of Computer Applications (0975-8887) Vol. 40 - No. 11, February 2012.

[3] A. Summer, “Mitigating Phishing Attacks: An Introduction to Computer Science,” pp. 72-77, 2010

[4] Vayansky and S. Kumar, “Phishing—Challenges and Solutions,” Computer Fraud Security, Vol. NO. 1, pp. 15-20, 2018 [5] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, Imtiaz Khan, “Phishing Attacks: Recent Comprehensive Research and New Anatomy, Frontiers in Computer Science, vol. 3 March 2021, Item 563060

[6] Abdullah Fajar and Setiadi Yazid, "First socio-technical solutions to phishing attacks", Journal of Physics: Conference Series, IOP Publishing, 2020, 1502 012034

[7] Emma Megan, IEEE Computer Society, https://www.computer.org/publications/tech-news/trends/cybersecurity-threats-and-solutions - accessed 27 June 2021

[8] Chuck Easttom, "Computer Security Fundamentals", 3rd ed., Pearson Education, Inc., 2016, ISBN-13:978-0-7897-5746-3

[9] E. Filiol, Viruses and Malware, Information and Communication Security Handbook, 2010.

[10] A. Bettany and M. Halsey, Windows Virus and Malware Troubleshooting, Berkeley, CA:Prints, 2017

[11] Mariwan Ahmed Hama Saeed, “Malware in Computer Systems: Problems and Solutions,” International Journal on Informatics for Development, Vol. 9, No.1, 2020, pp.1-8, e-ISSN: 2549-7448

[12] Shilpa Pareek, Ashutosh Gautam, Ratul Dey, "Different Type Network Security Threats and Solutions, A Review", International Journal of Computer Science (IIJCS) ISSN 2321-5992, Volume 5, Issue 4, April 2017.

[13] Al-rimy B, Maarof M, Shaid S, “Ransomware threats, taxonomies, and countermeasure success factors: Research and Research Directions,” Computers and Security, 2018. 74: 144-166.

[14] Popli N, Girdhar A. Verma, Nishchal K, Ghosh AK, "Analyzing the behavior of current ransomware and predicting future attacks with polymorphic and metamorphic ransomware." (Edit) Computational Intelligence: Theory, Applications, and Future Directions - Volume II ICCI-2017. Springer, Singapore. 2018;799(4):65-80.

[15] Murat Ozer, Said Varlioglu, Bilal Gonen, Mehmet F. Bastug, “Ransomware Attack Prevention and Traction Systems”. 6th Annual Conference on Computational Science and Computational Intelligence (CSCI'19). 05.-07.12.2019.

[16] I DUNCAN, “‘Confused and Upset’: Baltimore Ransomware Attack Complicates Problems for Debt Payers,” Baltimore, May 2019 [online]. Accessible: https://www.baltimoresun.com/politics/bs-md-20190508-story.html

[17] Bharadwaj D. R., Bhattacharya A., Chakkaravarthy M., "Cloud Threat Defense - Threat Protection and Security Compliance Solutions". IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) 2018.

[18] Vishal D.K. Soni, “Artificial Intelligence Challenges and Solutions in U.S. Cybersecurity.” Artificial Intelligence in US Cybersecurity [Online] Available at: https://ssrn.com/abstract=3624487

[19] Mariarosaria Taddeo, Tom McCutcheon, Luciano Floridi, “Reliance on artificial intelligence in cybersecurity is a double-edged sword,” Nature Machine Intellegence, 42256-019-0109-1.

[20] Tasneem Yousuf, Rwan Mahmoud, Fadi Aloul, Imran Zualkernan, “Internet of Things (IoT) Security: Current Situation, Issues and Countermeasures”. International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015

[21] Mouheb, D., Abbas, S., and Merabti, M., “Designing a Cybersecurity Curriculum:

[22] Sushmita chakraborty, Praveen kumar, Dr. Bhawna sinha, “A study on DDoS attack, Danger and its Prevention,” p. International Journal of Research and Analytical Reviews (IJRAR) E-ISSN 2348-1269, P-ISSN 2349-5138, May 2019, Band 6, Ausgabe 2.

[23] B.B.G. Nalin and A.G.A. Kostas, “Defending Against Phishing Attacks:Method Taxonomy, Current Issues and Future Directions," Telecommunication System, vol. 67, no.2, pp. 247-267, 2018

[24] Kasperkey article on ransomware protection: How to protect your data in 2021 [online]. Available: HTTPS://WWW.KASPERSKY.CO.IN/RESOURCE-CENTER/THREATS/HOW-TO-PREVENT-RANSOMWARE

[25] Gary Stevens, “Cloud Security: 5 Critical New Cloud Computing Threats to Avoid,” May 26, 2020 [online]. Available: HTTPS://WWW.THESSLSTORE.COM/BLOG/CLOUD-SECURITY-5-SERIOUS-EMMERING-CLOUD-COMPUTING-THREATS-TO-AVOID/

[26] Mohamed Litoussi_, Nabil Kannouf, Khalid El Makkaoui, Abdellah Ezzati, Mohamed Fartitchou, “IoT Security: problem and solutions". 7th International Symposium on New Information, Communications and Networks (EICN 2020), 2-5. Madeira, Portugal, November 2020.

[27] Abuagoub, Ali MA, International Journal of Communication Networks and Information Security. Kohat Vol. 11, Iss. 3, (December 2019):342-351.

[28] Malatji, M., Von Solms, S., & Marnewick, A. Cybersecurity Framework for Sociotechnical Systems. Information and Computer Security 2019. doi: 10.1108/ics-03-2018-0031