International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

An Analytical Study on Attacks and Threats in Cyber Security and its Evolving Trends on Modern Technologies

Omkar Veerendra Nikhal

Department of Computer Engineering, Pune Institute of Computer Technology, Pune, Maharashtra, India

ABSTRACT

In today's dynamic and technologically advanced world, the Internet has become one of the most innovative and rapidly growing technologies. With its rise, it has also become vulnerable to a significant increase in occurrences of cyber-attacks, with detrimental effects. Typically, these cyber attacks are targeted at accessing, manipulating, or damaging confidential data, extracting users' money, or extorting an organization's or user's private information. Sensitive information, whether intellectual property, financial data, confidential information, or other forms of private data are exposed to unauthorized access or disclosure, which can have adverse consequences. Protecting data has become one of the greatest obstacles today as cyber attacks are constantly escalating. Along with the growth of internet services and the advancement of information technology, the importance of cybersecurity is crucial. Cybersecurity aims to ensure that the security interests of the company and users' assets are protected and preserved against relevant cyber threats in the digital world. The data and confidentiality of computing assets pertaining to the network of an organization are protected by cybersecurity. This paper mainly focuses on threats and issues in cybersecurity facing modern technologies. It also focuses on the latest cybersecurity strategies and developments that are transforming the face of cybersecurity.

KEYWORD: *Cybersecurity, Cyber Crime, Technology, Computer, Cyber Threats, Vulnerability*

How to cite this paper: Omkar Veerendra Nikhal "An Analytical Study on Attacks and Threats in Cyber Security and its Evolving Trends on Modern Technologies" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.1230-1235, URL: www.ijtsrd.com/papers/ijtsrd38195.pdf

IJTSRD38195

1. INTRODUCTION

Multitudinous recent developments are transforming today's world. These days, any sort of data can be transferred and received with the help of information technology and computer networks. Almost all of an individual's confidential information is digitalized. But due to the escalation of cyber attacks day by day with the augmentation of information technology, there is a major challenge in securing our private information. Every day, new privacy risks are emerging where, amid the best efforts of cybersecurity experts on a regular basis, well-resourced organizations are being hacked. This illustrates that modern technological developments are necessary when current systems may be constrained. Cybercrimes which include hacking of accounts, embezzlement, extortion, defamation, etc. have severe effects on a nation's development. The attackers have actively created new attack launch techniques, recalling the need for creativity and improvement of security technologies to ensure data protection in organizations. Economic transactions have gained a 77% increase currently, demanding a high degree of protection for secure and best-in-class transactions. With recent attacks, it seems like nothing is entirely secure online. Cybersecurity has thus become a crucial issue. With the impact of cybercrimes, organizations lose billions of dollars every year, resulting in losses for future businesses. The spectrum of cybersecurity is not only limited to information technology, but also to numerous other fields such as cyber space, etc.

Latest technologies require high-security standards and safeguarding since these technologies may contain some valuable information about an organization. For the security and economic well-being of every nation, improving cybersecurity is essential. In the development of new services as well as governmental policies, making the Internet safer has become integral. A robust and secure solution is required in the fight against cybercrime. Given that technological solutions will not deter any crime of their own, law enforcement authorities must be able to properly investigate cybercrime. Cybersecurity and law enforcement investigators are increasingly dealing with broad-scale cyber threats in almost real-time. Without the use of threat intelligence, big data, and machine learning techniques, the ability to detect, analyze, and defend against such threats in near real-time conditions is not possible. In order to stop the destruction of any critical information, many countries and governments are now enforcing stringent cybersecurity regulations. The key security aim is to use different rules to safeguard the system and to develop secure defenses against attacks over the internet.

2. BACKGROUND WORK

Several vulnerabilities are possible in the area of cybersecurity. Researchers have continuously analyzed and focused on them to minimize the risk, both ethically and lawfully, of breach of any privacy norms.

Some of the previous works are based upon the principle of advanced persistent threats (APT), which include security of cyber networks which implements APT-based cyber attack defense process modeled as a dynamical system to exhibit global stability [1], technique that can analyze efficiently high volumes of network traffic to reveal weak signals related to data exfiltration and other suspect APT activities [2]. [3] examined recent ransom ware infections in healthcare settings, the risk liabilities and costs associated with infections, and risk mitigation tactics.[4] proposed an approach to discover system vulnerability on the internet by cyber-attack, and to prevent unauthorized access and critical infrastructure cryptography with the help of code-scanning tools and user authentication respectively.[5] suggested a Protection Motivation Theory (PMT) framework for protecting organization information security related to self-reported cybersecurity protection action on the part of the employee. [6] Proposed Community Cybersecurity Maturity Model (CCSMM)1 to determine cybersecurity posture and maturity. [7] proposed a systems security analysis approach for understanding and eliciting security requirements for complex cyber-physical systems.[8] presented an adversarial risk-based approach for Network Architecture Security Modeling and Design.[9] developed a real-time method to detect compromised Software-Defined Network(SDN) devices.[10] explored threats to the cloud by investigating the linkages between threats, attacks, and vulnerabilities, and proposed a method to identify threats systematically in the cloud using the threat classifications.[11] introduced SlowDrop which is an attack characterized by a legitimate-like behavior and able to target different protocols and server systems. [12] generated IoT device fingerprints based on neural network algorithms.[13] developed Coupling Privacy with Safety (CPS) and maintained Quality of Service of Vehicular Ad-hoc Networks (VANETs) to provide security against three types of attacks.[14] studied the vulnerability in the existing ICT infrastructure.[15] evaluated applications of genetic programming (GP) and stream active learning for insider threat detection. [16] developed DMOS (Deep Mobile OS Security), a kernel-level mobile OS security technique for secure personal ubiquitous computing. [17] studied software vulnerabilities and weaknesses of Embedded Systems in Power Networks. [18] proposed information regarding SCADA systems with vulnerability, threats, and management in IoT and cloud computing.[19] focused on studying the influence of network characteristics on malware spreading.[20] presented Trust-Based Botnet Monitoring Countermeasure (TrustBotMC), a novel mechanism, that combines computational trust with specially crafted bot messages to detect the presence of monitoring activity.[21] proposed a modular structure architecture and also used sagishi within the active honeypot concept, which may be helpful to spot malware.

3. CYBER CRIME

As technology has become essential to business, entertainment, and government, cybercrime, particularly through the Internet, has risen in importance. Typically, cybercrime may be described as a crime perpetrated using a computer and the internet to steal the private information of an individual or stalk an organization or deploy malevolent program operations. Cybercrime is any type of illegal activity that uses digital means as the principal method of commission and fraud for any criminal activity. One of the most popular examples of cybercrime is Cyber Bullying. Cybercrime often entails a broad variety of disruptive practices, such as data-stealing or planting viruses. It also includes internet-enabled crimes, such as network intrusions and the transmission of computer viruses, as well as computer-based variations of current crimes, such as identity fraud, stalking, harassment, and terrorism, which have become a major concern for individuals and nations.

Cybercrimes can be categorized into two different categories: those that cause deliberate harm and those that cause unintended harm. The loss is financial in most situations, but not all. Cyber bullying, for example, is illegal because it poses a danger to the physical welfare of a victim, requires coercion, or demonstrates hatred or prejudice towards such protected groups. The loss is not financial in that case, but it is still a crime. Accidental damage may be a frustrated employee planting a harmless virus that in some way disrupts business. While it does not inflict the same direct financial damage as stealing confidential or financial information, it still causes collateral financial damage due to both lost employee time and any cash the company loses[26]. In addition to some novel unlawful acts, cybercrime, specifically concerning the Internet, represents an evolution of current criminal behaviour.

4. CYBERSECURITY

Data protection and security are the top security steps taken care of by every organization. Cyber-criminals will try to exploit various networks to steal private data in the case of organizations. The cybercrime economy allows advanced threats quickly to deploy and open to a wide range of mobilized opponents. An individual must take all the security precautions needed not only for social networking but also during financial transactions. Current technical developments have opened up new cybersecurity opportunities. Cybersecurity safeguards computers, networks, programs, and data from malicious entry or cyber threats that are intended at infiltration. These cyber attacks are targeted at accessing, exploiting, or damaging confidential data; extorting users' money; or disrupting normal business processes. A cybersecurity attack at an individual level will result in anything from identity fraud, to extortion attempts, to the destruction of sensitive data such as personal images.

Cybersecurity has established a crucial strategic challenge for digital business. In addition, companies want security approaches that allow them to concentrate on their market. This development is transforming the landscape of the data security industry, in order to be able to update and achieve their digital capacity with regard to any given business and customer target. In order to protect companies from digital threats and to fight advanced threats, cybersecurity tools and technology should integrate automation, artificial learning, and mutual threat intelligence. Cybersecurity investment worldwide is continuing to grow. Organizations are becoming conscious that ransomware is the universal asset that encourages becoming a cyber criminal for all as more businesses provide defense strategies that do nothing to protect them against threats. The data and integrity of computing assets belonging to or connected to the network of an entity are secured by cybersecurity. Throughout the entire life cycle of a cyber attack, the purpose of cybersecurity is to protect certain properties from all challenging entities.

5. THREATS IN CYBERSECURITY

Cybersecurity vulnerabilities have been established over decades against infrastructure systems. The security of vital infrastructure has also been given priority after the terrorist attacks. Insecure computer systems and networks can cause fatal disturbances, divulgation, and fraud. There are crimes that target computer networks or services directly like ransomware, viruses, or denial of services, and crimes enabled by networks or devices that are the principal target outside of networks or devices such as fraud, identity theft, phishing, and cyber stalking [22]. Cyber threats emerge from the exploitation of computer system vulnerabilities. This paper deals with recent threats such as Phishing, IoT Based Attacks, Ransomware, Insider Threats, Deepfakes, 5G-to-Wi-Fi Security Vulnerabilities, and Cloud Computing Threats.

5.1. Phishing

Phishing attacks are a sort of social engineering attack where the attacker produces a fake email, text, or web page which tricks a victim into handing down sensitive information — such as login credentials, passwords to accounts, credit card information, and so on. Phishing scams typically use social engineering to steal account authorizations for on-site attacks and cloud attacks. Almost 78% of cases involving cyber espionage were linked to phishing in 2019. In comparison to conventional emails, phishing attempts are launched via cloud applications. Implicit trust users have more vulnerable phishing techniques in their cloud systems in their office [27].

5.2. IoT Based Attacks

An IoT attack is a cyber-attack that uses victims to snap ransomware into their networks while using smart internet-linked equipment (e.g., Internet connectivity with Wi-Fi, alarm clocks, etc.). Specifically, since they are often lacking when installing security fixes, these attacks threaten IoT computers, making them easier for vulnerability. A Fortune Business report indicates that the Internet of Things (IoT) market is likely to grow to $1.1 trillion by 2026. Needless to say, this widespread use of IoT devices will herald a larger number of increasingly complex cybersecurity threats. There could also be a serious threat to the Internet of Medical Things (IoMT) that could become a grave Internet health crisis [27].

5.3. Ransomware

Ransomware Attacks normally entail a victim's device is compromised with a virus that encrypts all its info. The victim is then given an ultimatum—be it paying the ransom or ever losing their records. The rate of detections within businesses rose from 2.8 million in the first quarter of 2018 to 9.5 million in the first quarter of 2019. That's nearly a 340% increase in detections. The reason why ransomware has persisted for so long is the relative simplicity with which an attacker can achieve devastating effects. Ransomware kits are dirt cheap and readily available on the dark web [27].

5.4. Insider Threats

One of the greatest ongoing cybersecurity risks facing any company is its staff. Employees' internal access makes them likely to do more damage if they want to misuse their access rights. Or by mistake, they may encourage attackers to compromise their user accounts or inadvertently download unsafe malware on their workstations. The 2019 Verizon Data Breach Investigations Report (DBIR) shows that 34 percent of breaches involve internal actors. Insider threats not only involve malicious attacks, but also the negligent use of systems and data by employees. To protect against these threats, organizations need to quickly and accurately detect, investigate and respond to issues that could be indicators of insider attacks. Common antivirus and anti-malware (AV/AM) tools are usually ineffective against these threats. Insider threats require specialized tools[27].

5.5. Deep Fakes

Deepfakes refer to manipulated videos or other digital artifacts created by advanced artificial intelligence that create fabricated images and sounds that seem to be genuine. There's a lot of speculation that deepfakes might eventually emerge as a major cybersecurity threat, with it being used for malicious intent. We might also witness other cybersecurity threats, such as deepfake usage for committing fraud through synthetic identities, and the emergence of deep fake-as-a-service organizations[27].

5.6. 5G-to-Wi-Fi Security Vulnerabilities

Because of the cybersecurity gap and the increased demand for cyber threats, businesses have never had to find new ways to strengthen their protection. There is no doubt that attackers will discover new flaws in the 5G-to-Wi-Fi switch. Wireless providers will send more calls and data to WiFi networks, with 5G networks soon evolving, with bandwidth savings. Hackers have the chance to compromise safety because of the software bugs in this transfer process. While mobile devices possess built-in intelligence to silently and automatically switch between cellular and Wi-Fi networks, security researchers have already identified several vulnerabilities in this handover process. It is very likely that new, critical 5G-to-Wi-Fi security vulnerabilities will be exposed in 2020.3[27].

5.7. Cloud Computing Threat

There is also an increasing threat of cloud computing in 2020. According to Forbes, 83% of the corporate workload will be moved to the cloud in 2020[29]. Cloud services are typically on-hand to protect cloud data, but it is also the duty of the customer to keep cloud data secure in the end. Thorough knowledge regarding cloud security will be required for organizations to protect their resources better. The level of understanding about cloud security remains low, and security is often an afterthought when it comes to cloud deployments. Cybersecurity solutions need to involve new, flexible, and scalable cloud-based architectures.

6. RECENT TRENDS IN CYBERSECURITY

Cyber threats are on the rise, not just from the isolated hackers but from national-state actors who carry out these attacks to exfiltrate government and corporate knowledge. While companies are more conscious of the significance of cybersecurity now than ever before, many are continuing to identify and enforce the necessary protection measures needed. Below is the list of trends currently being implemented in cybersecurity:

6.1. Implementation of 5G

The introduction of the Mobile Internet of the next generation (5G) would make use of popular IoT devices better for humanity. However, it would also raise the exposure to cyber attacks. With the bandwidth that 5G technology enables, data volumes and the number of

connected devices and sensors is set to explode. Electronic health applications will collect data about a user's wellbeing, new car technology will monitor a user's movements, and smart applications will collect information about how users live and work. With so much personal data being collected from us, 5G technology will mean high levels of security against breaches and data theft will be required[30].

6.2. Cybersecurity skill gaps

According to the MIT Technology Review report(3), there will be about 3.5 million unfulfilled cybersecurity jobs in 2021, which means it's expected to grow by 350%. In 2020, the demand for cybersecurity professionals will continue to exceed supply, as security teams have to deal with more online threats than ever before. According to a DDLS survey, more than two-thirds of respondents said that ensuring their skills and the skills of their team were up to date was the biggest challenge, suggesting not enough is being invested to improve in-house cybersecurity expertise[30].

6.3. Data Breaches

Data breaches are one of the primary issues of cybersecurity, as long as personal data remains a lucrative asset for the black market. Providing data encryption and in particular, personal data security would undoubtedly remain at the forefront of organizations' minds. In part, this is due to increasingly stringent privacy legislation, such as the European Union's General Data Protection Regulation (GDPR), but organizations are also more and more aware of the negative consequences of a breach for their image. With web application flaws being a leading source of data breaches, ensuring web application security has become a top priority for all organizations[31].

6.4. Automation and Integration in Cybersecurity

Security professionals, developers, and engineers are all under pressure to do more with less, so automation and integration are essential across the board. By incorporating security into agile processes such as CI/CD and DevOps, organizations can effectively manage risk while maintaining the required pace and quality of development. Sprawling web applications combining multiple web services are increasingly hard to secure, and automated solutions are becoming a necessity to reduce the workload on understaffed teams[31].

7. CYBERSECURITY TECHNIQUES

In the light of a growing number of unauthorized attempts to steal confidential data to threaten or intimidate users into blackmailing of information, cybersecurity is gaining prominence. To overcome cybersecurity issues, the methods and strategies used are:

7.1. Authentication

This fundamental cybersecurity technique intends to verify the identity of the user based on the credentials stored in the security domain of the system. The most common mode of governance is password technology, however, there are numerous other implementations like the SIM card inserted in anyone's cell phone. SIM cards are equipped with unique ID numbers which are passed over a secure communication line for identification of a particular cell phone. The documents obtained after downloading must always be authenticated to verify if they came from a trustworthy and credible source and not changed. These records are normally authenticated by anti-virus computer tools. So it is also important to develop strong anti-virus applications to protect computers from viruses[32].

7.2. Encryption

Encryption renders data undecipherable without a proper key being applied to unlock it. In order to combat encryption, a solution to complex mathematical problems like the creation of large primes would be needed, which would take astronomical time and energy. Symmetric encryption utilizes the same key for the purpose of message encoding and decoding, and the security level is similar to that of the key. The distribution of the key will be accompanied by potential security risks. Asymmetric encryption utilizes a public key to encrypt the message and a private key to decrypt the same. A majority of present-day security protocols are employing asymmetric encryption for the distribution of keys[32].

7.3. Digital signatures

The mathematical algorithms that are used in asymmetric encryption can be used to build digital signatures. By getting some information encoded with it a user is free to test that he possesses a private key. Anyone can get the same decrypted by having the public key that will verify the person's credentials. This process is in essence the exact reciprocal of public-key encryption and likewise functions on the assumption that the authorized user only has the private key[32].

7.4. Antivirus

Antivirus software is computer software that detects, prevents, and removes malicious programs such as viruses and worms. Most antivirus programs include an auto-update function that allows the program to download new virus profiles so that as soon as they are discovered so that it can check for new viruses. For every system, antivirus software is a must and fundamental necessity. The threats of computer viruses or undesirable short programs that trigger unwanted commands without the explicit consent of the user have assumed monstrous proportions. Anti-virus software carries out two functions; it prevents the installation of viruses in a system and scans the systems for viruses that are already installed. Most viruses have been constructed to target Windows operating systems as it is the most preferred computing platform of the masses. Apple and Linux users can also come under the attack of viruses exclusively built for such operating systems[32].

7.5. Firewall

A firewall is a software or hardware tool that supports screening out of hackers, viruses, and worms that attempt to reach your computer over the Internet. The present firewall examines all messages entering or leaking the internet and blocks those that do not meet the specified safety criteria. Firewalls, therefore, play an important part in malware detection. Firewalls effectively hinder any attempt of unauthorized access to a computer when it is connected on the internet by hackers directly or via other network connections. Firewalls come bundled up with most operating systems and are turned on by default. The help of commercial firewalls can be sought if the security level of the default firewall is not strong enough or if it is posing interference to legitimate network activities[32].

8. CONCLUSION

The subject of cybersecurity is becoming increasingly relevant because the world is becoming extremely integrated, with sensitive transactions being carried out using networks. The emerging technology, the new cyber techniques, and risks that come to light every day threaten companies to protect their networks and information. In recent years the number of cyber attacks and vulnerabilities has grown considerably, and hackers are following people, organizations, corporations, and governments to steal critical IP and national secrets. This paper addresses different forms of threats in cybersecurity along with the vulnerabilities in vital infrastructures. Cybersecurity is a crucial concern, as the networks are used to carry out vital transactions. There is no ideal solution to cyber crime, but in order to have a safe and stable future in cyberspace, we should do our best to mitigate it. In order to avoid the destruction of any substantial knowledge, many countries and governments are nowadays establishing stringent cyber securities regulations.

9. REFERENCES

[1] Yang, L. X., Li, P., Yang, X., Wen, L., Wu, Y., & Tang, Y. Y. (2017). Security evaluation of cyber networks under advanced persistent threats. arXiv preprint arXiv:1707.03611.

[2] Marchetti, M., Pierazzi, F., Colajanni, M., & Guido, A. (2016). Analysis of high volumes of network traffic for Advanced Persistent Threat detection. Computer Networks, 109, 127-141.

[3] Spence, N., Bhardwaj, N., Paul III, D. P., & Coustasse, A. (2018). Ransomware in Healthcare Facilities: A Harbinger of the Future?. Perspectives in Health Information Management.

[4] Schneidewind, N. (2010). Metrics for mitigating cybersecurity threats to networks. IEEE Internet Computing, 14(1).

[5] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.

[6] White, G. B. (2011, November). The community cybersecurity maturity model.In Technologies for Homeland Security (HST), 2011 IEEE International Conference on (pp.173-178).IEEE.

[7] Span, M. T., Mailloux, L. O., Grimaila, M. R., & Young, W. B. (2018, June). A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems. In 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity) (pp. 1-8). IEEE.

[8] Wortman, P. A., Tehranipoor, F., & Chandy, J. A. (2018, June). An Adversarial Risk-based Approach for Network Architecture Security Modeling and Design. In 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity) (pp. 1-8). IEEE.

[9] Zhou, H., Wu, C., Yang, C., Wang, P., Yang, Q., Lu, Z., & Cheng, Q. (2018). SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices. IEEE/ACM Transactions on Networking (TON), 26(5), 2048-2061.

[10] Hong, J. B., Nhlabatsi, A., Kim, D. S., Hussein, A., Fetais, N., & Khan, K. M. (2019). Systematic identification of threats in the cloud: A Survey. Computer Networks, 150, 46-69.

[11] Cambiaso, E., Chiola, G., & Aiello, M. (2019). Introducing the SlowDrop Attack. Computer Networks.

[12] Yang, K., Li, Q., & Sun, L. (2018). Towards automatic fingerprinting of IoT devices in the cyberspace. Computer Networks.

[13] Trevisan, M., Drago, I., & Mellia, M. (2019). PAIN: A Passive Web performance indicator for ISPs. Computer Networks, 149, 115-126.

[14] Chaturvedi, M. M., Gupta, M. P., & Bhattacharya, J. (2008). Cybersecurity Infrastructure in India: A Study. Emerging Technologies in E-Government ', CSI Publication.

[15] Le, D. C., Khanchi, S., Zincir-Heywood, A. N., & Heywood, M. I. (2018, July). Benchmarking evolutionary computation approaches to insider threat detection. In Proceedings of the Genetic and Evolutionary Computation Conference (pp. 1286-1293).ACM.

[16] Lee, S., Lee, S., Kang, T., Kwon, M., Lee, N., & Kim, H. (2018). Resiliency of mobile OS security for secure personal ubiquitous computing. Personal and Ubiquitous Computing, 22(1), 23-34.

[17] Välja, M., Korman, M., & Lagerström, R. (2017, April). A Study on Software Vulnerabilities and Weaknesses of Embedded Systems in Power Networks.In Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids (pp. 47-52).ACM.

[18] Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. IEEE Access, 4, 1375-1384.

[19] Liu, W., & Zhong, S. (2018). Modeling and analyzing the dynamic spreading of epidemic malware by a network eigenvalue method. Applied Mathematical Modelling, 63, 491-507.

[20] Böck, L., Vasilomanolakis, E., Wolf, J. H., &Mühlhuser, M. (2019). Autonomously Detecting Sensors in Fully Distributed Botnets. Computers & Security.

[21] Oliveri, A., & Lauria, F. (2019). Sagishi: an undercover software agent for infiltrating IoT botnets. Network Security, 2019(1), 9-14.

[22] Parikh, T.P., & Patel, A.R.(2017).Cybersecurity: Study on Attack, Threat, Vulnerability.International Journal of Research in Modern Engineering and Emerging Technology

[23] Reddy, G.N.,& Reddy, G.J.U. (2014).A study of cybersecurity challenges and its emerging trends on latest technologies.

[24] Devi, R.S., & Mohankumar, M. (2019).An empirical study on cybersecurity threats and attacks.

International Journal of Scientific Research and Review

[25] Sandar, A. M., Min, Y., Win, K. M. N. (2019) Fundamental Areas of Cybersecurity on Latest Technology. International Journal of Trend in Scientific Research and Development

[26] https://www.iovation.com/topics/what-is-cybercrime-definition-and-examples-of-cybercrime

[27] https://www.kaseya.com/blog/2020/04/15/top-10-cybersecurity-threats-in-2020/

[28] https://www.compuquip.com/blog/4-cybersecurity-threats-to-watch-out-for-in-2018

[29] https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/?sh=62628cd16261

[30] https://blog.eccouncil.org/cybersecurity-trends-in-2020-the-threats-facing-the-industry/

[31] https://www.netsparker.com/blog/web-security/top-10-cybersecurity-trends-to-look-out-for-in-2020/

[32] http://www.crossdomainsolutions.com/cyber-security/tools-techniques/