Current Scenario about Virtual Private Network (VPN) Cyber Security Threats

C.Deepika,M.Sc.,Mphil
Research Scholar
Vels Institute of Science Information and Technology,
Dr.K.Abirami,M.Sc.,M.Phil.,Ph.D
Assistant professor,
Dept of computer science
Vels Institute of Science Information and Technology,

Abstract:

One of the most crucial issues today is cybersecurity.topics in the arena of information security. Cybersecurity risk in context of emerging DMs assesses manufacturing impact and identifies approaches for securing DMs. In this article, we examine how a new model of cyber resilience developed and presented can be used to improve cybersecurity and cyber defense. In the condition of Cybersecurity(Cybersecurity and Emerging Risks) presents a novel conceptual cyber resilience model that integrates cybersecurity and information security. The model integrates machine learning, natural language processing, behavioral analytics, and deep learning to bolster cybersecuritydefenses and guard against a variety of cyberthreats, such as malware, phishing attacks, and insider threats. In order to get findings, this study used descriptive and analytical methods. This outcome emphasizes the growing relevance of cybersecurity. Without a doubt, businesses are aware of the risks and threats that hackers represent to their operations.

Keywords: cybersecurity, VPN, cyber crime, malware attacks, cloud network.

1. Introduction:

Cyber security is the shield from cyber security about connections related to the internet including hardware, software, and mainly data from cyber attackers. This is primarily the people, processes, and activities to cover the full spectrum of threat reduction, vulnerability reduction, deterrence, international engagement, and recovery policies and activities, including computer networking, information assurance, law enforcement, etc. It's all about technology. Scammers on the Internet know the way to access it in various manners. Without our knowledge that our data is being scammed, they intentionally convince us to send the data. So our safety is more important while using the internet[1].

Issues such as data from attack, modification, threat, damage and unauthorized access are in the current period, To avoid such issues and protect network devices, programs, and data from such issues concept of Information Technology security is currently a scenario for protection.Virtual Private Networks (VPNs) are growing in popularity. However, as the use of VPNs grows, so do the cybersecurity threats targeting these networks. This blog post delves into the current scenario surrounding VPN cybersecurity threats and explores the risks

and vulnerabilities that users need to be aware of. By understanding these threats, we can better protect ourselves and ensure the safety and privacy of our online activities.

2. Cyber Security:

Cybersecurity is a field aimed at eliminating cybercrime. It is the backbone of network and information security involves safeguarding against cyber threats. Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from harmful attacks. It's also referred to as information technology security or electronic information security. Cybersecurity can be split into two components: 'cyber' and 'security.' 'Cyber' encompasses technology like systems, networks, programs, and data, while 'security' focuses on safeguarding systems, networks, applications, and information. This field is also known as electronic information security or information technology security". The goal of cybersecurity is to defend sensitive data and important systems against online attacks. Cybersecurity measures, commonly referred to as information technology security (IT security), are designed to fend off threats to networked systems and applications, whether they originate from within or outside the organization [2].

Figure 1: Cyber Security

3. Cyber Crime:

Unauthorized entry into a computer system is considered a cybercrime. Cybercrime is any criminal activity that targets or uses a computer, computer network, or connected device. Most cyber crimes are perpetrated by cyber criminals or hackers to make money. However, in some cases, cybercrime aims to damage computers and networks for reasons other than profit. These may be political, or they may be personal. The number of attacks is increasing day by day. Hackers are getting smarter about what they do. Cyber security provides in-depth knowledge of how to control or recover from cyber attacks.Cybercrime is a form of crime involving computers or computer networks. This computer may have been used or targeted in a crime. Cybercrime can endanger someone's safety or finances. International cybercrime, such as financial theft, espionage, and other transnational crimes, is committed by both state

and non-state actors. Cyber warfare is sometimes used to describe cybercrime that crosses national borders and includes at least one of her states. Warren Buffett called cybercrime "humanity's greatest problem" and said it "posed a real risk to humanity"[3].

Figure 2: Cyber Crime

3.1 Various Cyber Crime:

3.1.1 Email frauds:

Email fraud is another name for phishing attacks. Phishing starts with false emails and other forms of communication meant to entice victims. It indicates that the sender of the communication is a reliable one. If tricked into this, victims are tricked into exposing sensitive information, often on fraudulent websites. In some cases, malware is also downloaded onto the victim's computer. Attackers may occasionally be happy to gain victims' credit card numbers and other personal information if it will help them financially. Phishing emails may also be sent to gather employee login information and other information that will be utilized in sophisticated attacks against certain corporations. Phishing is frequently a crucial step in cybercriminal attacks like Advanced Persistent Threats (APT) and ransomware.[4]

3.1.2 Social media frauds:

A social media crime is any illegal activity that occurs on or originates from a social media platform. The most common social media crimes include cyberbullying, stalking, harassment, and online threats that can affect people's reputation, safety and well-being. Another common crime on social media is phishing. This is a type of scam that sends malicious emails that appear to come from trusted sources but contain malware or viruses that can steal your personal information. Identity theft is also a common crime on social media. Using someone else's personal information to commit fraud, such as opening a credit card or taking out a loan in your own name.

3.1.3 Banking frauds:

Bank fraud is the practice of impersonating a bank or other financial institution to obtain money, assets, or other property of a financial institution or, in some cases, using illegal means to obtain money from depositors. is. Bank fraud is often a crime. The specific elements of a particular bank fraud law vary by jurisdiction, but the term bank fraud refers to conduct involving the use of conspiracy or deception, in contrast to theft from or robbery at banks. In view of this, bank fraud is occasionally categorized as a white-collar crime.

3.1.4 Ransomware attacks:

Cryptovirological virus known as ransomware threatens to either permanently limit access or otherwise divulge a victim's personal information unless a ransom is paid. Simple ransomware can lock down your system without deleting your files, but higher-level software use a tactic known as crypto-virus extortion. Files belonging to the victim are encrypted to make them unavailable, and a ransom is demanded to unlock them. Without a decryption key, retrieving files with a well-implemented cryptocurrencyransomware is an impossible task, and digital currencies like Paysafecard is and Bitcoin are hard to track down. Ransomware is harder to find and prosecute as other cryptocurrencies are used for ransom. perpetrators[5].

3.1.5 Cyber espionage:

Cyber espionage is cyber espionage in which a threat actor maliciously accesses, steals, or discloses sensitive data or intellectual property to gain commercial, political, or competitive advantage in a corporate or government environment. A type of attack. It can also be used to damage a person's or company's reputation. Cyber espionage operations can involve complex tactics and long-term, patient attacks on targeted networks. Common techniques include APT (Advanced Persistent Threat), social engineering, malware attacks, and spear phishing. Cyber espionage, cyber espionage, or cyber harvesting, without the permission and knowledge of individuals, competitors, rivals, groups, governments, and owners of information for personal, economic, political or political purposes acts or practices, secrets, and information Purpose The purpose of gaining military superiority by using means on the Internet.

3.1.6 Identity theft:

Identity theft occurs when someone uses another person's personally identifiable information, such as a name, identification number, or credit card number, without permission to commit fraud or other criminal offenses. The term identity theft was coined in 1964. Since then, the definition of identity theft has been legally defined as theft of personally identifiable information in both the UK and US. Identity theft is the intentional misuse of someone else's personal information to gain financial, goodwill, or other advantage, and in some cases, harm or loss to others. A person whose identity is stolen can be adversely affected, especially if held unfairly responsible for the perpetrator's actions. Personally identifiable information typically includes an individual's name, date of birth, social security number, driver's license number, bank account or credit card number, PIN, electronic

signature, fingerprint, password, or access to personal financial information. It contains other information that you can use to means.

3.1.7 Click jacking:

Clickjacking (classified as a user interface repair attack or UI repair) tricks a user into clicking something different than what the user perceives to divulge sensitive information or cause other users to do so. A malicious technique is used to gain control over a computer by clicking on a seemingly harmless object, such as a web page. Clickjacking is an example of a confusing proxy problem where computers are tricked and abused. Her one form of clickjacking exploits vulnerabilities in an application or her website to allow attackers to take control of users' computers for their benefit[6].

3.1.8 Spyware:

Spyware (a term for spyware) collects information about an individual or organization and distributes that information to another organization in a way that harms the user, such as by violating the user's privacy or compromising the security of the device. Malicious software that is intended to transmit. This phenomenon can occur with both malware and legitimate software. The website may use spyware behavior such as web tracking. Hardware devices may also be affected. Spyware is often associated with advertising and causes many of the same problems. Providing an accurate definition of spyware is a difficult task, as these behaviors are very common and cannot be exploited.

Figure 3: Cyber Crime And cyber Secrity

3.2 HOW THE ABOVE CRIMES ARE EXECUTED:

Malware - code (Trojan horses, viruses, worms) written to steal data or destroy things on your computer

Phishing – Phishing emails prompt users to click links and enter personal information

DDoS Attacks – Denial of Service (DoS) attacks focus on disrupting network services. An attacker sends a large amount of traffic over the network until the network becomes overloaded and stops working.

Man-in-the-middle attack – A man-in-the-middle attack can masquerade as an online information exchange endpoint to obtain information from end users and communicating entities.

Drive-by download attacks – Clicking "accept" on software and visiting a website, or simply driving past, causes malicious code to be downloaded onto your device in the background.

Figure 4: Various Crimes

4. VPN- Virtual Private Network:

A VPN (virtual private network) is a method of creating a secure connection by means of an unrestricted communication channel, such as the public Internet, between a computing device and a computer network or between two networks. A VPN masks the identity you use online and encrypts your internet activity. As a result, it is more challenging for outside parties to monitor your online behaviour or steal your data. Real-time encryption takes occur.

Figure 5: Virtual Private Networks

4.1 VPN is Not Secure:

A VPN is not secure as it exposes the entire network to malware, DDoSattacks, spoofing attacks, and other threats. If an attacker enters your network through a compromised device, it can bring down the entire network.

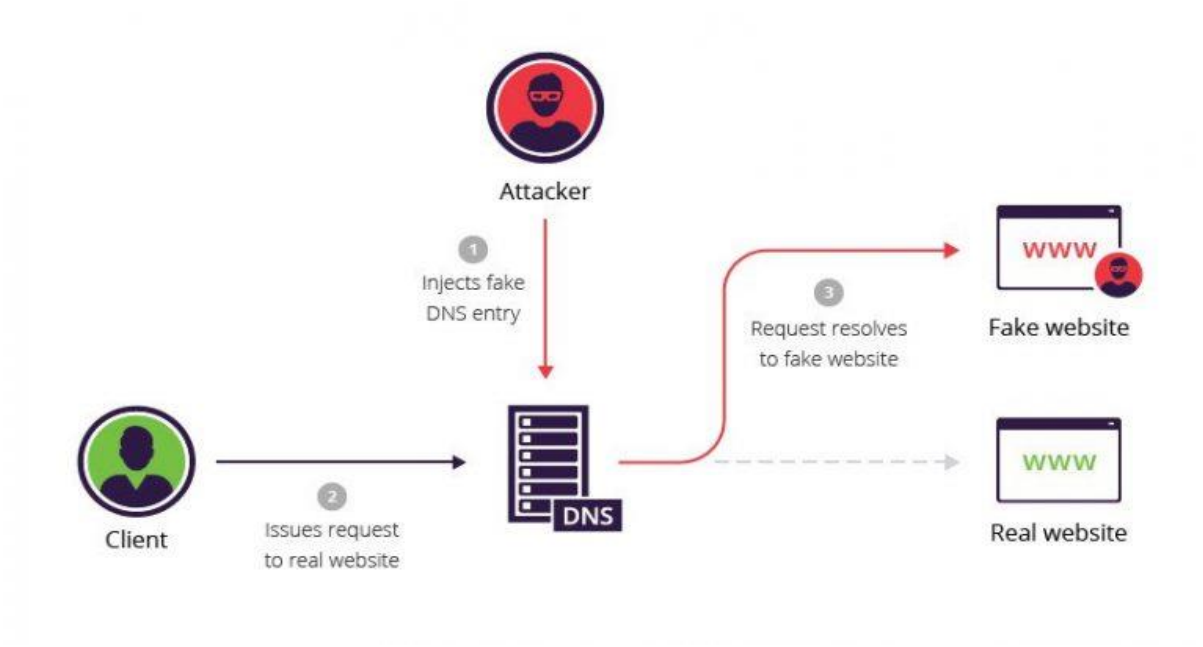

Figure 6: Example of VPN Cyber crimes

4.2 VPN Security Vulnerabilities Types:

There are many types of security vulnerabilities are occurs

Operating System Vulnerabilities – These vulnerabilities can be used by hackers to access or harm assets where operating systems are installed.

Process vulnerabilities – Some vulnerability may be brought on by specific procedures or controls, or by their absence.

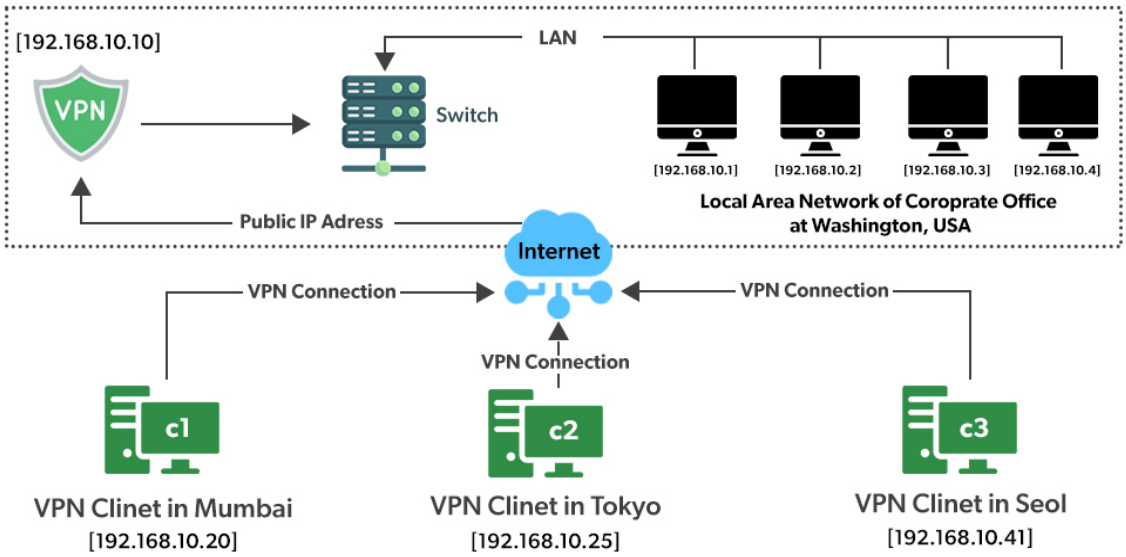

Figure 7: Real time Example of VPN at Washington, USA

Network Vulnerability – Your network has hardware or software issues that could lead to third-party intrusion.

Human Vulnerabilities – User mistakes can easily leak sensitive data, create exploitable entry points for attackers, and disrupt systems.

4.3 Case Study about VPN by an example:

Consider a situations where the bank's head office in Washington, USA. In this about 100 systems where connected via LAN. Assume that the bank has other branches in Tokyo (Japan) and Mumbai (India).Dedicated lines are between branch offices and headquarters used to be employed to create a secure link between headquarters and branch offices, but this was exceedingly expensive and tedious. This issue can be successfully resolved by using a VPN. A VPN server (a properly configured server with a public IP address and a switch to connect all computers laying on our local network, i.e. our US headquarters) is used to link all 1000 machines at our headquarters in Washington. Here I am. If someone in the Mumbai office dials up to her VPN server, the VPN server responds with an IP address from the subset of IP addresses that are part of the headquarters' local area network. If a person in the Mumbai branch connects up to her VPN server, the connection to the VPN server responds with an IP address from the subset of IP addresses that are part of the headquarters' local area network (LAN). As a result, employees from the Mumbai branch will be based at the corporate headquarters and have access to secure public Internet communication. As a result, it is a logical way to expand your local network across borders[7].

VPN with Real Time Example:

Spotify is a Swedish music app that isn't available in India, but since we are based therein we use it exclusively. So how ?? You can mask your geolocation with a VPN. Let's begin by assuming you have the IP address 101.22.23.3 and are an Indian citizen. This prevents the device from using the Spotify music app. The Android program Psiphon transforms the IP address of the device to the IP address of the target location (for example, the US, where Spotify functions without a hitch). Using VPN technology, the IP address is changed.In essence, your device establishes a connection with the VPN server located in the nation you selected for the Psiphon app's location text field and receives a new IP address from that server. "What is my IP address?" I typed. Unexpectedly, the IP address has been altered to the USA's 45.79.66.125. Additionally, Spotify is now reachable in India (effectively in the US) because it functions so well there. Isn't that excellent? Very helpful. Unexpectedly, the Internet Protocol (IP) address was changed to the USA's 45.79.66.125. Additionally, Spotify is now reachable in India (effectively in the US) due to the fact it operates perfectly there. Isn't that excellent? Really helpful

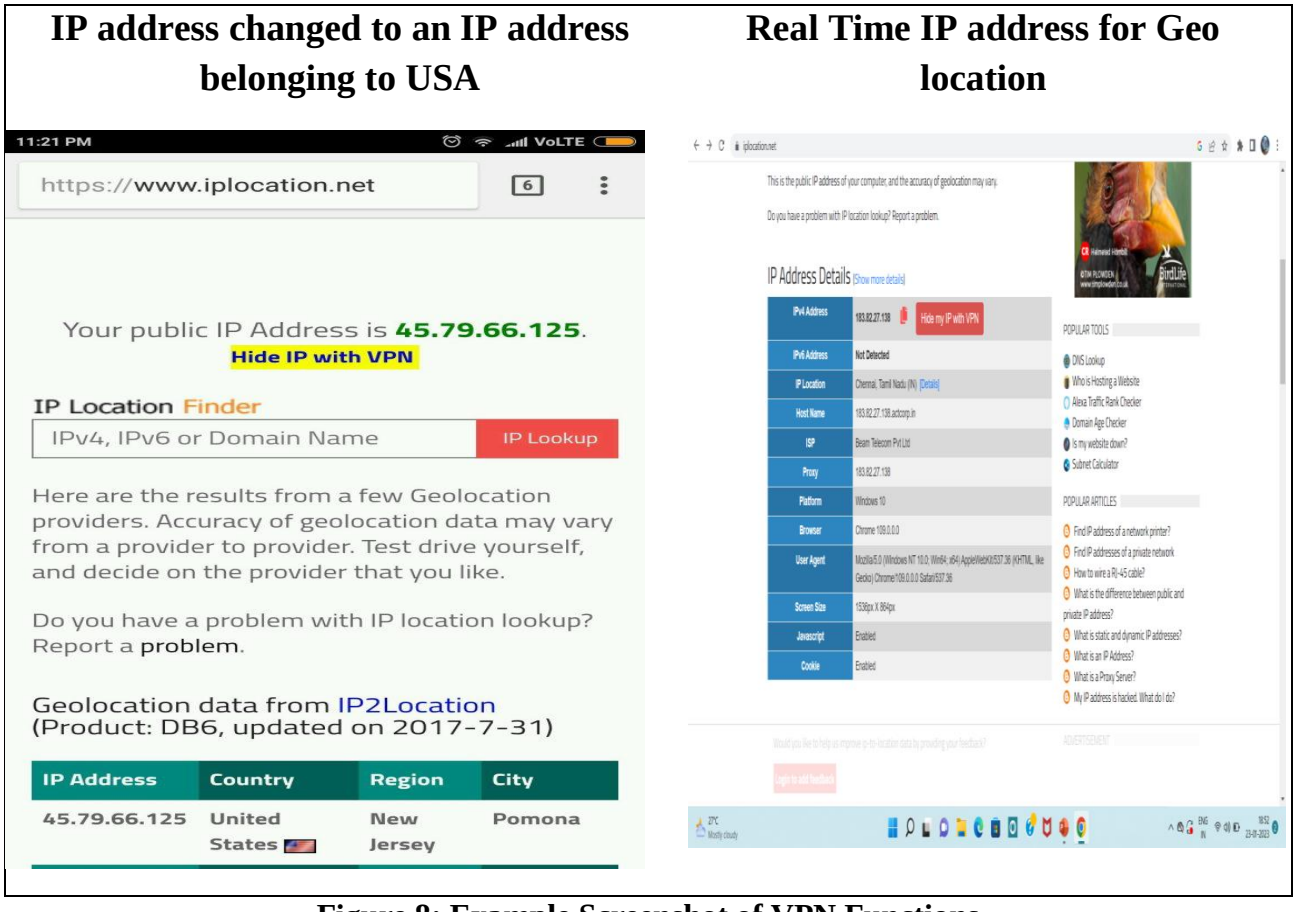

Figure 8: Example Screenshot of VPN Functions

In this paper the concepts of VPN, Cyber security and issues are analyzed well. Various papers are discussed below how the cyber security, the crimes and how the malware

are controlled and challenges faced by the people everything are well discussed. How the system are encrypted to protect the data from traffic through various algorithms.

5. Literature Review:

S.N.Matheu et al.,The survey paper, mainly focused on cybersecurity certification to facilitate that fit in emerging states such as the IOT pattern. By using technical tool and integrating research,governance structures and policies which is under processes were analyzed against a set of identified challenges[8].

Mahesh et al,The evolving DM context's risks from cyber security determine the effects on manufacturing and determine solutions to secure DM. Case Study 1: An assault by a Drowned Morning. Cyberattack on the Honda Auto Plant is Case Study 2. Case Study 3: Attack on Firmware for Additive Manufacturing (Attaches, Countermeasures, and Metrics)[9].

S.Bagui et.al, Our attention is on how to differentiate between traffic that is encrypted normally (non-VPN transmission) and traffic that is encrypted when it is tunneled through a VPN. In our work, we contrast supervised machine-learning methods for classifying VPN traffic from non-VPN traffic. Logistic regression (LR), support vector machine (SVM), Naive Bayes (NB), k-nearest neighbor (KNN), Gradient Boosting Trees (GBTs), and Random Forest (RF) are the machine-learning models that are being compared. GBT, KNN, LR, NB, RF, and SVM are examples of approaches for supervised machine learning[10].

Al-Turjman Et Al,The primary applications for smart cities address the most important privacy and security concerns in their design. It also examines a few of the current approaches to the security and privacy of apps for information-centric smart cities and outlines upcoming research problems that still need to be taken into account for performance enhancement[11].

A. Razaque et al, From the literature,. discuss a number of cybersecurity architectures for the medical industry. We examine the countermeasures from earlier papers and architectures that still have weaknesses in terms of resource exhaustion, attack mitigation, applicability, etc. Information gathering attacks, database assaults, website attacks, and operational device attacks are all examples of information gathering attacks[12].

DARKO GALINEC, A wide range of procedures, instruments, and ideas that are closely related to information and operational technology security are included in the field of cyber security. The employment of information technology on the offensive to attack enemies makes cyber security unique. Customers and security professionals are misled and the important distinctions between these disciplines are obscured when the word "cyber security" is used as a primary challenge and a synonym for information security or IT security. Security executives are advised to limit the use of the phrase "cyber security" to security procedures relating to defensive activities involving or depending on technological infrastructure and/or

operational technology environments and systems.Cyber defense is a computer network defensive system that comprises action response, critical infrastructure protection, and information assurance for corporations, government bodies, and other potential networks [3]. With the unique model of cyber resilience devised and presented in this work, we study how cyber security and cyber defense can lead to cyber resilience. In addition, within the same model, the authors investigate actions for cyber security and cyber defense in the face of increasing cyber-attack challenges and limited capabilities to respond to this threat, describing the process of creating, performing, and sustaining EU Cyber Rapid Response Teams (abbr. CRRT) and Mutual Assistance in Cyber Security, introducing a novel approach to cyber security and cyber defense at the EU level[13].

Syed Adnan Jawaid Washington,The cyber security sector has been altered by artificial intelligence, which has enabled organizations to systematize and expand on obsolete safety practices. AI can increase threat detection and response capabilities, as well as vulnerability management and compliance and governance. Artificial intelligence (AI) technologies such as machine learning, natural language processing, behavioral analytics, and deep learning can improve cyber security defences and protect against a wide range of cyber threats such as malware, phishing attacks, and insider threats. The theoretical foundations of AI in cyber security are covered, including deep learning, machine learninglearning, NLP - natural language processing, and behavioural analytics are discussed. The benefits of adopting AI in cyber security, includes its speed and accuracy, adaptability and capacity for continual learning, and scalability. It's crucial to remember that AI cannot serve as a panacea for cyber security and must work in concert with other defence strategies to offer a complete protection. The modern digital era's approach to cyber security has been revolutionized by AI. It has developed into a crucial tool for enterprises trying to safeguard their assets from cyber threats by quickly and accurately processing enormous amounts of data[14].

A. Panneerselvam,Threats to cyber security can take many different forms, such as ransomware, phishing, malware assaults, and more. India is now ranked 11th in the world for the volume of local cyberattacks, and in the first three months of 2020, it has already seen 2,399,692 of these occurrences. Businesses are surely aware of the risks and concerns that hackers pose to their companies because cyber security is a subject that is becoming more and more important. But cybersecurity would still be an issue that is difficult for three reasons: It involves a lot more than just an issue with technology. Different rules apply in cyberspace than they do in the actual world. Cybersecurity law, policy, and practice are still in the early stages.Considering the increase in cyberattacks, each business requires an analyst with security expertise to guarantee that their IT infrastructure is secure. These security specialists have to secure private enterprise servers, protect governmental organizations' confidential information, and deal with a variety cybersecurity-related challenges. In accordance to research, India has an enormous requirement for skilled cybersecurity workers, and this demand is expected to increase quickly. Employers predict a shortage of skilled cybersecurity experts. The study's objective is to evaluate and clarify India's cyber security framework and challenges. To arrive at a conclusion, the study combined descriptive and analytical

techniques. The study also employed the thematic software application QADMAX to assess the qualitative information used for secondary sources[15].

6. Conclusion:

Cybersecurity is the backbone of network along with data security. Sometimes it is referred as electronic information security or information technology security. Any criminal conduct that uses, targets, or involves a computer, computer network, or related device is referred to as cybercrime. Hackers or cybercriminals commit the majority of cybercrimes in order to make money. malware, etc. DDoS Attacks – Denial of Service (DoS) attacks focus on disrupting network services. Man-in-the-middle attacks – Man-in-the-middle attacks can masquerade as online information exchange endpoints to obtain information from end users or communicating entities. Drive-by Download Attacks - When you click "I agree" on software, visit a website, or simply drive by, malicious code is downloaded to your device in the background.

A virtual private network (VPN) is an approach for establishing a secure connection via an unsecured communication channel, such the public Internet, between a computing device and a computer network or in between two networks. A VPN encrypts your internet traffic and disguises your online identity. VPNs are insecure because they expose your entire network to malware, DDoS attacks, spoofing attacks, and other threats. If an attacker enters your network through a compromised device, it can bring down the entire network. Operating System Vulnerabilities – Hackers can exploit these to access or damage resources where the operating system is installed. Process vulnerabilities – Some vulnerabilities can be caused by specific process controls (or lack thereof). Network Vulnerability – Network has hardware or software issues that could lead to third-party intrusion. Consider a situation where the head office of a bank is in Washington, USA. This office has a local area network with about 100 computers. Spotify - Swedish music app. We are not active in India, but we are based in India so we are fully committed. So how?? A VPN allows you to hide your location.From the above discussion the VPN attacks are taken into consideration and future works will be taken from an the above said content.

7. Reference:

[1] K. Senthilkumar and S. Easwaramoorthy, “A Survey on Cyber Security awareness among college students in Tamil Nadu,” in *IOP Conference Series: Materials Science and Engineering*, Dec. 2017, vol. 263, no. 4, doi: 10.1088/1757-899X/263/4/042043.

[2] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Working from home during COVID-19 crisis: a cyber security culture assessment survey,” *Secur. J.*, vol. 35, no. 2, pp. 486–505, Jun. 2022, doi: 10.1057/s41284-021-00286-2.

[3] R. Karimnia, K. Maennel, and M. Shahin, “Culturally-sensitive Cybersecurity Awareness Program Design for Iranian High-school Students,” Feb. 2022, pp. 121–132, doi: 10.5220/0010824800003120.

[4] A. Sheth, S. Bhosale, and F. Kurupkar, “Emerging Advancement and Challenges in Science, Technology and Management " 23 rd & 24 th April, 2021

CONTEMPORARY RESEARCH IN INDIA."

[5] D. Al-, "Virtual Private Networks (VPN) Research Paper Course: Computer and Networking MIS3301."

[6] P. Subashini, M. Krishnaveni, T. T. Dhivyaprabha, and R. Shanmugavalli, "Review on Intelligent Algorithms for Cyber Security," 2019, pp. 1–22.

[7] N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang, and Y. Xiang, "Data-Driven Cybersecurity Incident Prediction: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1744–1772, Apr. 2019, doi: 10.1109/COMST.2018.2885561.

[8] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, "A Survey of Cybersecurity Certification for the Internet of Things," *ACM Comput. Surv.*, vol. 53, no. 6, 2021, doi: 10.1145/3410160.

[9] P. Mahesh *et al.*, "A Survey of Cybersecurity of Digital Manufacturing," *Proceedings of the IEEE*, vol. 109, no. 4. Institute of Electrical and Electronics Engineers Inc., pp. 495–516, Apr. 01, 2021, doi: 10.1109/JPROC.2020.3032074.

[10] S. Bagui, X. Fang, E. Kalaimannan, S. C. Bagui, and J. Sheehan, "Comparison of machine-learning algorithms for classification of VPN network traffic flow using time-related features," *J. Cyber Secur. Technol.*, vol. 1, no. 2, pp. 108–126, 2017, doi: 10.1080/23742917.2017.1321891.

[11] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3677.

[12] A. Razaque *et al.*, "Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain," *IEEE Access*, vol. 7, pp. 168774–168797, 2019, doi: 10.1109/ACCESS.2019.2950849.

[13] D. Galinec, "Cyber Security and Cyber Defense: Challenges and Building of Cyber Resilience Conceptual Model," *Int. J. Appl. Sci. Dev.*, vol. 1, pp. 83–88, Mar. 2023, doi: 10.37394/232029.2022.1.10.

[14] S. Adnan Jawaid, "Artificial Intelligence with Respect to Cyber Security," 2023, doi: 10.20944/preprints202304.0923.v1.

[15] A. Panneerselvam, "Framework and Challenges of Cyber Security in India: An Analytical Study," *Int. J. Inf. Technol. Comput. Eng.*, no. 24, pp. 27–34, Jul. 2022, doi: 10.55529/ijitc.24.27.34.