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

C.Deepika [1]
Research Scholar
Vels Institute of Science Technology and Advanced Studies,
Dr. K.Abirami[2]
Assistant professor,
Dept of computer science
Vels Institute of Science Technology and Advanced Studies,

Abstract:

Cyber security is one of the most important topics in the field of information security. Cyber security risk in the 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 cyber security and cyber defense. Resilience. In the context of Cyber security (Cyber security and Emerging Risks), a new conceptual cyber resilience model is presented that encompasses information security and cyber security. The model combines machine learning, natural language processing, behavioral analytics, and deep learning to strengthen cyber security defenses and protect against a wide range of cyber threats, including malware, phishing attacks, and insider threats. This study used a combination of descriptive and analytical techniques to obtain results. This result shows that cyber security is an issue of increasing importance. Businesses are no doubt aware of the dangers and threats hackers pose to their businesses.

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

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 threat, attack, damage, modification, 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 cyber security threats targeting these networks. This blog post delves into the current scenario surrounding VPN cyber security 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.

Cyber Security:

Cyber security is a field aimed at eliminating cybercrime. Cyber security is the backbone of network and information security. Cyber security is the protection of computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Also known as information technology security or electronic information security. Cyber security can be divided into two parts, one is cyber and the other is security. Cyber refers to technology including systems, networks, programs and data. Security is about protecting systems, networks, applications and information. Sometimes referred to as electronic information security or information technology security. Cyber security is about protecting critical systems and sensitive information from digital attacks. Cyber security measures, also known as information technology security (IT security), aim to combat threats to networked systems and applications, regardless of whether the threats come from inside or outside the organization[2].

Figure 1: Cyber Security

Cyber Crime:

Cybercrime is a criminal act involving unauthorized access to a computer system. 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. At the international level, both state and non-state actors are involved in cybercrime, including espionage, financial theft, and other transnational crimes. Cybercrime that transcends national borders and involves the actions of at least one of her states is sometimes referred to as cyberwarfare. Warren Buffett called cybercrime "humanity's greatest problem" and said it "posed a real risk to humanity"[3].

Figure 2: Cyber Crime

Various Cyber Crime:

Email frauds:

Email fraud is another name for phishing attacks. Phishing begins with fraudulent emails and other communications designed to lure victims. The message appears to have come from a trusted sender. 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. In some cases, attackers are content to obtain victims' credit card information and other personal data for financial reasons. Phishing emails may also be sent to obtain employee credentials and other data used in advanced attacks against specific organizations. Cybercriminal attacks such as Advanced Persistent Threats (APT) and ransom ware often startwith phishing[4].

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 cyber bullying, 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.

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, as opposed to bank robbery or bank theft. For this reason, bank fraud is sometimes considered a white-collar crime.

Ransom ware attacks:

Ransom ware is cryptovirological malware that threatens to reveal a victim's personal information or permanently block access to it unless a ransom is paid. While some simple ransom ware can lock down your system without damaging your files, more sophisticated malware uses a technique called crypto-virus extortion. It encrypts victim's files to make them inaccessible and demands ransom payment to decrypt them. With a well-executed crypto currency ransom ware, recovering files without a decryption key is an unsolvable problem, and digital currencies such as Paysafecard and Bit coin are difficult to trace. Ransom ware is harder to find and prosecute as other crypto currencies are used for ransom. perpetrators[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.

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

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. Click jacking 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].

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

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.

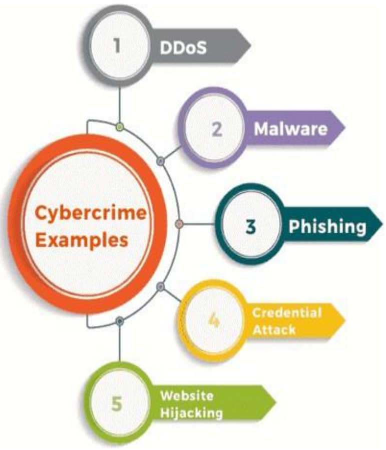


Figure 4: Various Crimes

VPN- Virtual Private Network:

A virtual private network is a mechanism for establishing a secure connection between a computing device and a computer network or between two networks, using an insecure communication medium such as the public Internet. A VPNencrypts your internettraffic and disguises your online identity. This makes it difficult for third parties to track your online activity or steal your data. Encryption happens in real-time.

Figure 5: Virtual Private Networks

VPN is Not Secure:

A VPN is not secure as it exposes the 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.

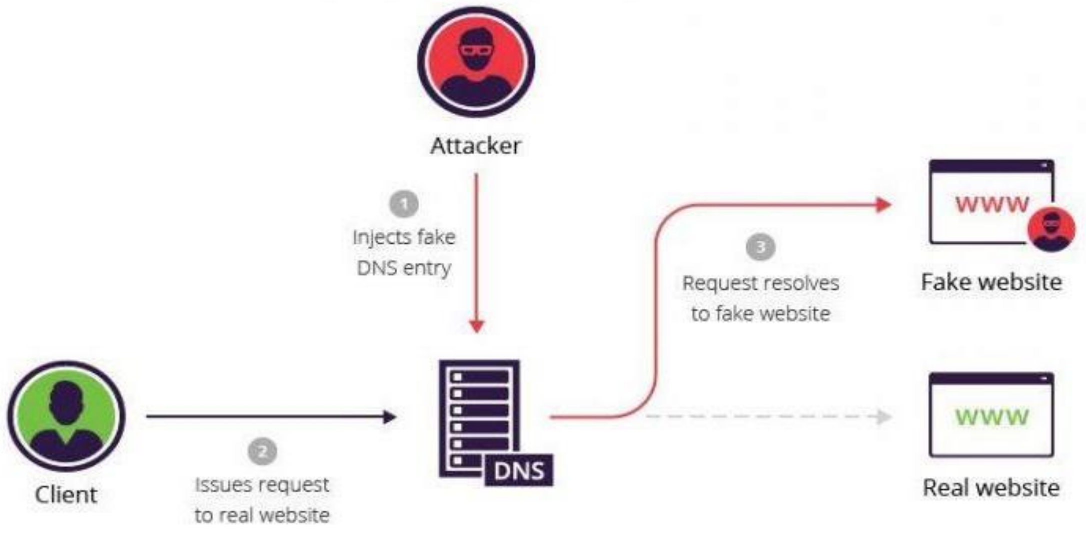


Figure 6: Example of VPN Cyber crimes

VPN Security Vulnerabilities Types:

There are many types of security vulnerabilities are occurs

Operating System Vulnerabilities – Hackers can exploit these to gain access to or damage assets on which operating systems are installed.

Process vulnerabilities – Some vulnerabilities can be caused by specific process controls (or lack thereof).

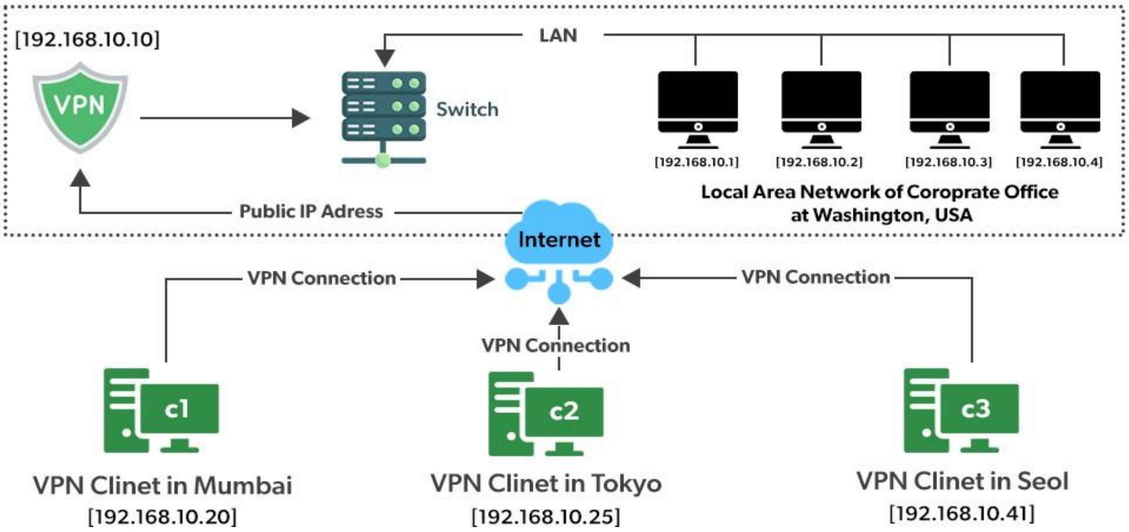


Figure 7: Real time Example of VPN at Washington, USA

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.

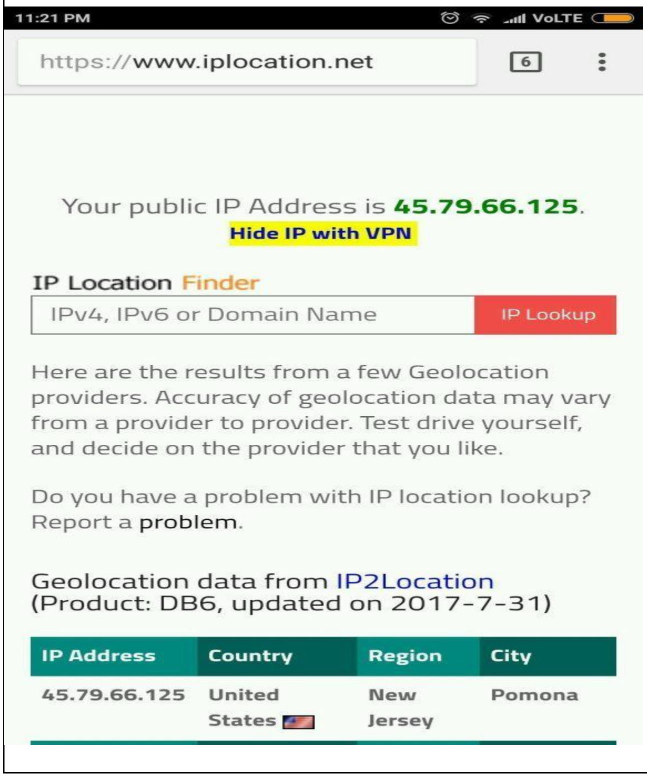
Let’s understand VPN by an example:

Consider a situation where the head office of a bank is in Washington, USA. This office has a local area network of about 100 computers. Assume that the bank has other branches in Mumbai (India) and Tokyo (Japan). The traditional method of establishing a secure connection between headquarters and branch offices was to use dedicated lines between the branch offices and headquarters, which was very expensive and cumbersome. Using a VPN can effectively solve this problem. All 1000 computers at our headquarters in Washington are connected to a VPN server (a properly configured server with a public IP address and a switch to connect all computers residing on our local network (i.e. our US headquarters)). I'm here. A person in the Mumbai office connects to her VPN server through a dial-up window, and the VPN server returns an IP address that belongs to the range of IP addresses that belong to the local area network of the headquarters. As a result, Mumbai branch personnel will be stationed directly at the head office and will be able to exchange information securely over the public Internet. Therefore, it is an intuitive way to extend your local network across geographical borders[7].

VPN with Real Time Example:

Spotify - Swedish music app, not active in India, but we're based in India, so we're fully on it. So how ?? A VPN allows you to obfuscate your geolocation. Suppose your IP address is 101.22.23.3 and you belong to India. Due to this, the device cannot access the Spotify music app. Psiphon app which is an Android app - changes the device's IP address to the IP address of the desired location (e.g. US where Spotify works seamlessly). The IP address is changed using VPN technology. Essentially, your device connects to the VPN server in the country you entered in the Psiphon app location text box and inherits a new IP from that server. I typed in "What is my IP address?" Surprisingly, the IP address was changed to 45.79.66.125 which belongs to the USA. And since Spotify works so well in the US, it is now available in India (effectively in the US). Isn't that good? Very useful. Surprisingly, the IP address was changed to 45.79.66.125 which belongs to the USA. And since Spotify works so well in the US, it is now available in India (effectively in the US). Isn't that good? Very useful.

IP address changed to an IP address belonging to USA



https://www.iplocation.net

Your public IP Address is **45.79.66.125**.

Hide IP with VPN

IP Location Finder

IPv4, IPv6 or Domain Name | IP Lookup

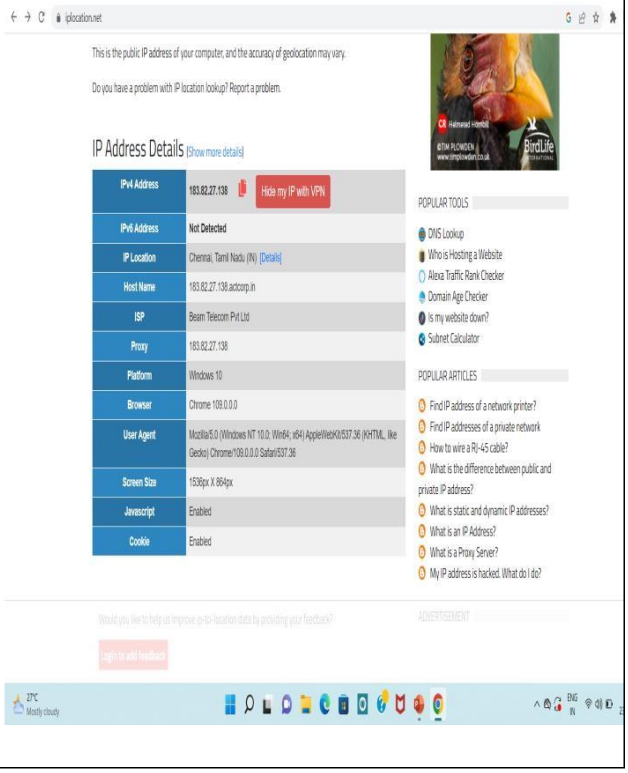
Here are the results from a few Geolocation providers. Accuracy of geolocation data may vary from a provider to provider. Test drive yourself, and decide on the provider that you like.

Do you have a problem with IP location lookup? Report a problem.

Geolocation data from IP2Location (Product: DB6, updated on 2017-7-31)

IP Address	Country	Region	City
45.79.66.125	United States	New Jersey	Pomona

Real Time IP address for Geo location



iplocation.net

This is the public IP address of your computer, and the accuracy of geolocation may vary.

Do you have a problem with IP location lookup? Report a problem.

IP Address Details [Show more details]

IPv4 Address	183.82.27.138 Hide my IP with VPN
IPv6 Address	Not Detected
IP Location	Chennai, Tamil Nadu (IN) [Details]
Host Name	183.82.27.138.actcorp.in
ISP	Beam Telecom Pvt Ltd
Proxy	183.82.27.138
Platform	Windows 10
Browser	Chrome 109.0.0.0
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
Screen Size	1536px X 864px
Javascript	Enabled
Cookie	Enabled

Helmeted Hornbill
©TIM PLOWDEN www.timplowden.co.uk
BirdLife International
POPULAR TOOLS
DNS Lookup
Who is Hosting a Website
Alexa Traffic Rank Checker
Domain Age Checker
Is my website down?
Subnet Calculator
POPULAR ARTICLES
Find IP address of a network printer?
Find IP addresses of a private network
How to wire a RJ-45 cable?
What is the difference between public and private IP address?
What is static and dynamic IP addresses?
What is an IP Address?
What is a Proxy Server?
My IP address is hacked. What do I do?
ADVERTISEMENT

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.

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 integrating research and technical tool, processes with policies and governance structures, which are analyzed against a set of identified challenges[8].

Mahesh et al,The cyber security risks in the emerging DM context assess the impact on manufacturing and identify approaches to secure DM. Case Study 1: Drowned Attack on AM. Case Study 2: Cyberattack on Honda Auto Plant. Case Study 3: Additive Manufacturing Firmware Attack (Attacks, Counter measures and Metrics)[9].

S.Bagui et.al, Our focus is on the classification of encrypted network traffic, tunneled through a VPN, and traffic that is encrypted normally (non-VPN transmission). Our work compares supervised machine-learning techniques for the classification of VPN versus non-VPN traffic. The machine-learning models compared are logistic regression (LR), support vector machine (SVM), Naïve Bayes (NB), k-nearest neighbor (KNN), Gradient Boosting Trees (GBTs), and Random Forest (RF). Supervised machine learning techniques are GBT, KNN, LR, NB, RF and SVM[10].

Al-Turjman Et Al,Mainapplications of smartcities and addresses the major privacy and security issues in the architectureof the smart cities applications. It also reviews some of the current solutionsregarding the security and privacy of information-centric smart cities' applicationsand presents future research challenges that still need to be considered forperformance improvement[11].

A. Razaque et al,Discusses several cybersecurity architectures for the medical domain from the existing literature. The countermeasures from previous papers and architectures that are still weak in terms of resource depletion, attack reduction, applicability, etc. are addressed. (i) Information collection attacks (ii) database attacks, (iii) website attacks and (iv) operation device attacks[12].

DARKO GALINEC, Cyber security encompasses a broad range of practices, tools, and concepts related closely to those of information and operational technology security. Cyber security is distinctive in its inclusion of the offensive use of information technology to attack adversaries. The use of the term cyber security as a key challenge and a synonym for information security or IT security misleads customers and security practitioners and obscures critical differences between these disciplines. The recommendation for security leaders is that they should use the term cyber security to designate only security practices related to defensive actions involving or relying upon information technology and/or operational technology environments and systems. Cyber defense is a computer network defense mechanism that includes the response to actions and critical infrastructure protection and information assurance for organizations, government entities, and other possible networks [3]. In this paper, we investigate how cyber security and cyber defense may lead to cyber resilience with the novel model of cyber resilience designed and presented. Furthermore, within the same model authors investigate actions for cyber security and cyber defense in conditions of increasing challenge of cyber-attacks and the limited capabilities to respond to this threat describing the process of creation, performance, and future of 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,Artificial Intelligence has transformed the cyber security industry by enabling organizations to systematize and enlarge outdated safety procedures. AI can provide more effective threat detection and response capabilities, enhance vulnerability management, and improve compliance and governance. AI technologies such as machine learning, natural language processing, behavioral analytics, and deep learning can enhance cyber security defenses and protect against a wide range of cyber threats, including malware, phishing attacks, and insider threats. Theoretical underpinnings of AI in cyber security, such as machine learning, natural language processing, behavioral analytics, and deep learning, are discussed. The advantages of using AI in cyber security are discussed including speed and accuracy, continuous learning and adaptation, and efficiency and scalability. It’s important to note that AI is not a silver bullet for cyber security and should be used in conjunction with other security measures to provide a comprehensive defense strategy. AI has transformed the way cyber security operates in today’s digital age. By analyzing vast amounts of data quickly and accurately it has become a valuable tool for organizations looking to protect their assets from cyber threats[14].

A. Panneerselvam,Cyber security threats come in a wide variety of forms, including ransomware, phishing, malware attacks, and many others. India is currently ranked 11th in the world in terms of the number of local cyberattacks and it has already experienced 2,399,692 of these incidents in the first three months of 2020. Because cyber security is a topic that is growing more and more essential, businesses are undoubtedly well aware of the hazards and threats that hackers offer to their corporations. However, cybersecurity would continue to be a difficult issue for three reasons: It goes beyond a simple technological issue. Cyberspace operates under a distinct set of regulations than the real world. Law, policy, and practice in the area of cybersecurity are still in their infancy. Every firm requires a security analyst to ensure that their system is secure given the rise in cyber-attacks. These security analysts must secure private company servers; protect the confidential data of governmental organizations, and other cybersecurity-related difficulties. Research indicates that there is a significant need in India for qualified cybersecurity specialists and that this demand will continue to rise soon. Employers anticipate a scarcity of qualified cybersecurity specialists. The goal of the study is to analyze and explain India's cyber security framework and difficulties. The study used a combination of descriptive and analytical methods to draw a result. The Thematic software tool QADMAX was also used in the study to analyze the qualitative data for secondary sources[15].

Conclusion:

Cybersecurity is the backbone of network and information security. Also known as information technology security or electronic information security. Cybercrime is any criminal activity that targets or uses a computer, computer network, or connected device. Most cyber crimes are done by cybercriminals or hackers for money making. spyware, 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 is a mechanism for establishing a secure connection between a computing device and a computer network or between two networks, using an insecure communication medium such as the public Internet. 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.

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.