International Journal of Scientific Research and Management (IJSRM)
||Volume||09||Issue||12||Pages||EC-2021-669-710||2021||
Website: www.ijsrm.in ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v9i12.ec04

A Systematic Literature Review on the Cyber Security

[1]Dr.Yusuf Perwej, [2]Prof. (Dr.) Syed Qamar Abbas, [3]Jai Pratap Dixit, [4]Dr. Nikhat Akhtar, [5]Anurag Kumar Jaiswal

[1]Professor, Department of Computer Science & Engineering, Ambalika Institute of Management and Technology, Lucknow, India
[2]Director General, Ambalika Institute of Management & Technology, Lucknow, India
[3]HOD (CSE, IT), Ambalika Institute of Management & Technology, Lucknow, India
[4]Associate Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India
[5]Assistant Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India

Abstract
In recent years, the Internet has become an integral element of people's everyday lifestyles all across the world. Online criminality, on the other hand, has risen in tandem with the growth of Internet activity. Cyber security has advanced greatly in recent years in order to keep up with the rapid changes that occur in cyberspace. Cyber security refers to the methods that a country or organization can use to safeguard its products and information in cyberspace. Two decades ago, the term "cyber security" was barely recognized by the general public. Cyber security isn't just a problem that affects individuals but it also applies to an organization or a government. Everything has recently been digitized, with cybernetics employing a variety of technologies such as cloud computing, smart phones, and Internet of Things techniques, among others. Cyber-attacks are raising concerns about privacy, security, and financial compensation. Cyber security is a set of technologies, processes, and practices aimed at preventing attacks, damage, and illegal access to networks, computers, programmes, and data. The primary goal of this article is to conduct a thorough examination of cyber security kinds, why cyber security is important, cyber security framework, cyber security tools, and cyber security difficulties. Cyber security safeguards the data and integrity of computing assets that are part of or connected to an organization's network, with the goal of defending such assets from all threat actors throughout the life cycle of a cyber-attack.

Keywords: Cyber Security, Cyber Attacks, Phishing, Cyber Crime, Network Security, Internet of Things (IoT) Security, Cyber Security Frameworks, Malware.

I. Introduction

The Internet is one of the most important inventions of the twenty-first century that has had a significant impact on our lives [1]. Today, the internet has broken down all barriers and transformed the way we communicate, play games, work, shop, make friends, listen to music, watch movies, order meals, pay bills, and greet pals on their birthdays and anniversaries. Our world is becoming increasingly networked, with digitized information underpinning key services and infrastructures [2]. Nation states, organizations, and end users are all concerned about threats to the confidentiality, integrity, and availability of digitized information [3]. In a digital world that is progressively pervading every area of our everyday lives, both public and private, security is a must. The world will fall apart if there is no security. Attacks like WannaCry have wreaked havoc on unprepared citizens, businesses, and organizations, putting their operations in jeopardy [4]. In the sphere of information technology, cyber security plays a critical role. Over the previous few decades, cyber security has progressed [5]. When we come across a fraud, cyber security is the first thing that comes to mind. Protecting our personal data on the internet has become a major concern. The number of [6] connected device has expanded at a rapid rate in recent years, surpassing 50 billion by 2020. The

exponential growth in the number of connected devices increased the complexity of cyber infrastructure, resulting in an increase in the number of vulnerable devices [7].

The world's businesses are being transformed by data science [8]. Because "security is all about data," it is vital for the future of intelligent cyber security systems and services. We analyse security data in the form of files, logs, network packets, and other relevant sources when trying to detect cyber threats [9]. Hackers could possibly acquire easy unauthorised access to information processed using big data [10] technologies unless an emphasis is focused on attaining effective cyber security in big data [11]. As a result, it's evident that big data [12] has both benefits and drawbacks. As a result, cyber security is a concern that affects everyone throughout the world. Hackers are getting smarter all the time, and they're coming up with new ways to create harmful software to abuse the data of individuals, businesses, and governments. Despite adequate security precautions, cyber-attacks [13] are on the rise.

Malicious software, phishing, password attacks, drive-by downloads via hyperlinks, virus attacks, and so on are all examples. In public debates, cyber security [14] is frequently confounded with other ideas such as privacy, information exchange, intelligence collecting, and surveillance. When we encounter cybercrime, we must also consider cyber security. People from various professional backgrounds work in the field of cyber security [15]. As a result, each profession collaborates with others to protect the confidentiality, integrity, and availability of information or data, all of which are critical components of cyber security.

Cyber security will ensure that authorized users have unrestricted access to information and that unauthorized access or hacking of any system is prevented [16]. The core components of confidentiality, integrity, and availability, as outlined above, are frequently used to explain system access. It should be recognized that no system or environment is completely secure, regardless of security procedures, standards, or technology. Cyber security [17] is an ever-expanding field. Every day, new hazards can be found in your company or organization. New technologies are constantly being created to combat hazards, for example. Anyone who has been following the [18] news understands how businesses are dealing with cyber security issues. Until ransom demands are satisfied, files in organizations and institutions all across the world have been encrypted. Cyber security isn't just an issue in the IT world. In fact, it has a fairly broad scope. Everyone nowadays is familiar with the internet. Smart phones are used by even illiterate individuals [19], and they have become indispensable in their daily lives. When someone states that individuals today live on the internet [20], they are not exaggerating. Over time, the internet has evolved into an integral aspect of human life. Using artificial intelligence [21] as an alternative security solution has revealed that leveraging the predictive and defensive capabilities of artificial intelligence and machine learning [22] minimizes the number of additional security solutions needed [23]. This will surely improve system efficiency and raise the pace at which assaults are detected and averted.

This paper offers a comprehensive overview of current research into cyber security. We commence, section 2 provides the cyber security related work, in section 3, by introducing about cyber security. Section 4 outlines the history of cyber security. Section 5 why cyber security is essential, and section 6 cyber security types. In section 7 varieties of cyber threats, section 8 classification of cyber attackers, section 9 cyber security framework, and section 10 cyber security tools. Finally, in section 11 cyber security challenges.

II. Related Work

IT security includes cyber security as a subset. Cyber security protects the digital data on your networks, computers, and devices from unauthorized access, attack, and destruction. While IT security protects both physical and digital data, cyber security protects the digital data on your networks, computers, and devices from unauthorized access, attack, and destruction. In this section, we'll talk about how cyber security works. Brenner [24] describes the first method for identifying measures for assessing crime that originates in cyberspace. Although she acknowledges that designing metrics and scales for cybercrime is extremely difficult, due to ‘apprehension’, scale, and evidence issues, she proposes a simple taxonomy of harms consisting of three main types, namely individual, systemic. Kshetri attempts to define a cost-benefit calculus using a similar methodology to Laube et al. [25], but he focuses on the attacker's point of view He describes the characteristics of cybercriminals, cybercrime victims, and law enforcement officials, arguing

that when these three types of entities interact, they create a vicious cycle of cybercrime. He develops a calculation that analyses an attacker's rewards and costs, as well as arguments for whether or not a cyber-crime will occur. With the use of interruption detection, this paper [26] uses machine learning and information digging approaches for digital inquiry. The crime triangle [27] is sometimes used to define cybercrime, which states that for a cybercrime to occur, three variables must exist: a victim, a motive, and an opportunity. The victim is the person who will be attacked, the motive is what motivates the criminal to perform the crime, and the opportunity is when the crime will be committed (e.g., it can be an innate vulnerability in the system or an unprotected device).

While today's attacks are more sophisticated and targeted to specific victims based on the attacker's goal, such as financial gain, espionage, coercion, or retribution, opportunistic untargeted attacks are still common. "Opportunistic attacks" are defined as attacks that target victims based on their vulnerability to attack [28]. Camellia is a 128-bit block cypher proposed in this publication. Camellia supports 128-bit block sizes and 128-, 192-, and 256-bit keys, i.e. the Advanced Encryption Standard's interface specifications (AES). Camellia is notable for its efficiency on both software and hardware platforms, in addition to its high level of security [29]. Camellia has been proven to give good security against both differential and linear cryptanalysis. Camellia has at least comparable encryption speed in software and hardware to the AES finalists, namely MARS, RC6, Rijndael, Serpent, and Twofish.

The author of this [30] utilized machine learning and sentiment analysis to cyber security in order to establish a way for detecting cyber risks that were previously undetectable by traditional technologies. Greenfield et al. [31] provide a methodology for experimentally assessing harm that includes a number of processes. Functional integrity, material support and amenity, freedom from humiliation, privacy or autonomy, and reputation are the five fundamental dimensions where injury might appear. They also establish five levels of scale for various sorts of harm and investigate the cascading nature of harm by looking at real-world crimes that have generated significant societal impact. Grant et al. coined the term "cyberspace cartography" and applied the concept of "cyber-geography" to military operations. They also suggest that their ontology might be used in research to help solve the attribution problem of being unable to quickly identify hostile actors in cyberspace [32]. Chertoff et al. [33] describe the state of Internet jurisdiction law and the problem of assigning legal authority to a particular forum when a suit traverses multiple states. They present four possible formulations for defining the controlling jurisdiction in situations in a clear and equitable manner. These regulations are based on either the citizenship of the offending information, data, or system's subject, the location where the harm occurred, the citizenship of the data creator, or the citizenship of the data holder or custodian. A high-quality standalone literature review, according to Mathieu and Guy [34], provides reliable information and insights into previous research, allowing other researchers to seek new directions on similar issues of interest. Furthermore, the findings of this study can be utilized as references in related fields or as a basis for future research. Lin [35] compares nuclear and cyber technology and regulation, outlining a slew of contrasts, as well as a few parallels, between the potential difficulties that these two technologies bring, which he categorizes as strategy, operations, acquisition, and arms control. The author of paper [36] claimed that online security attacks have been carried out by hacker-activist organizations with the goal of causing harm to web services in a specific context. On Twitter content, the author demonstrated a sentiment analysis method. The author's strategy was based on a daily collection of tweets from users who utilize the platform to share their opinions on pertinent subjects and to deliver content connected to web security assaults. The information was transformed into data that could be statistically examined to determine whether an attack was likely or not. The latter was accomplished by examining the aggregate sentiment of users and hacktivist groups in response to a worldwide incident. Edwards et al. [37] use a publicly available dataset of data breaches to uncover trends in data breaches using a Bayesian Generalized Linear Model. They conclude that while the amount and frequency of data breaches have remained consistent in recent years, their impact is increasing as threat actors improve their ability to monetize personal information and the quantity of electronic financial transactions grows. A concentrated literature analysis of machine learning and data mining methods for cyber analytics in support of intrusion detection was reported in a survey study [38]. Van Slyke et al. [39] create taxonomy of harms for white-collar crimes by focusing on the victimization aspect of these crimes.

They look at a number of white-collar offences and the costs associated with them. They combine desktop research with victim surveys, focusing on the long-term consequences of damages in specific persons.

The author of paper [40] recommended that timely intelligence on cyber security risks and vulnerabilities is necessary to secure key personal and organizational systems. Overt and covert sources of information regarding these dangers include the National Vulnerability Database, CERT warnings, blog posts, social media, and dark web services. Other initiatives are centered on the evolution of risk frameworks and the modeling of business system resilience [41]. Researchers use these models to try to figure out how disasters can impair global essential services by looking at the interconnection of assets. A threat-based model is developed, with each threat being associated with various processes of destruction, specific vulnerabilities, and different obstacles for system resilience. In order to handle a massive problem like this, some solutions need to be figured out. Even though not everyone is willing to come up with solutions, a few people have stepped in to contribute a possible answer. Kennedy, proposes continuous and timely updates of security [42] software, as well as network and application software for both business and personal devices. The author offers a simulation-based training scenario in which student trainees experience the symptoms and effects of a DDos assault, [43] practice their response in a virtual environment with the purpose of preparing them for real attacks, utilizing a simulator and hacking tools. In paper [44], the author used a semi supervised method to classify cyber security logs into three categories: attack, unsure, and no attack, by first breaking the data into three clusters using Fuzzy K Mean (FKM), then manually labeling a small sample, and finally training the neural network classifier Multi-Layer Perception (MLP) on the manually labeled data. An interesting approach, based on the 'top-down' methodology described in the criminology field, is presented by Nguyen et al. [45]. The authors attempted to elicit 'premiums' that some users would be willing to pay to protect their assets from cyber-incidents. Our current knowledge about cyber security relies heavily on data from commercial threat reporting and news reports. Yet this data provides a partial and biased view of cyber threat activity, because it is often politicized and influenced by the demands of powerful buyers and the interests of capable providers [46].

Cyber-attacks can endanger patient safety by compromising data integrity or affecting medical device operation, for example. Recent examples include the WannaCry and NotPetya ransomware attacks, as well as flaws in [47] Medtronic implantable cardiac device programmers, which have harmed health-care delivery capabilities. It is apparent that cybercrime is here to stay due to its profitable nature [48] and low risk level (since cyber thieves can launch assaults from anywhere on the planet). The author of paper [49] feels that social media is now an important component of people's everyday lives and the livelihood of some. He describes a method for calculating consumer loyalty based on Twitter data. When fighting cyber-crime, it's critical to understand who might be the target of a cyber-attack and why tracking down their perpetrators might be tough. While everyone can theoretically become a victim of a cyber-attack, certain people are far more vulnerable than others. For example, in the past, an elderly person's personal information was particularly vulnerable to being taken by someone looking to make a lot of money. While this circumstance does not necessarily involve hacking, an elderly person can become a victim in other ways. Teenagers and the elderly are seen to be the most vulnerable victims, as they are the ones who are least aware that these attackers exist [50]. Traditional solutions, as well as the use of analytic models, machine learning, [51] and big data, might be improved by giving relevant knowledge to control or restrict the repercussions of threats, according to the author of article.

Cybercrime can manifest itself in the form of cyber bullying and online harassment, which are referred to as cyber enabled crimes, or through security risks that affect the computer itself, such as malware infections, ransomware infections, and theft and misuse of personal data, which are referred to as cyber dependent crimes [52]. An approach for tracking social data that can be used to launch cyber-attacks is presented in paper [53]. The monthly prediction of tweets with content linked to security attacks and the incidents discovered using l1 regularization is their key contribution. Cyber-threats are extremely dangerous for health-care institutions. According to Verizon's 2018 Data Breach Investigation Report, data breaches impacted the health care industry the most, accounting for 24 percent of all investigated breaches across all industries [54].

The investigation in paper [55] was directed at security experts who use machine learning approaches to detect intrusion, malware, and spam. The purpose was twofold: to analyze the current maturity of these systems and to identify the major obstacles that hinder machine learning cyber detection schemes from being adopted immediately. The conclusion was reached after a thorough analysis of the literature and tests on real-world enterprise systems and network traffic. According to a survey of health-care information security professionals, more than 75% of health-care businesses have recently encountered a security issue [56]. A novel approach for sentiment analysis was developed in paper [57] for obtaining opinions from a given data source. The proposed method was tested on one of the world's most important service industries travel. With the application of this approach, an analysis of opinions and sentiments expressed on Twitter about TripAdvisor was done. Cyber-attacks are also present in the world of cryptocurrency. Most cryptocurrency exchanges are done on a Blockchain, where transactions can be conducted in concise manners quickly. 51% of attacks occur when over half of the network of a company is taken over by hackers. The 51 percent assaults work a little differently in the realm of crypto currencies. There, 51% of attacks are carried out in order to obtain control of more than half of a Blockchain, allowing hackers to seize control of it [58]. Cybercrime is defined as the destruction, theft, or unauthorized or illegal use, modification, or copy of information, programmes, services, equipment, or [59] communication network, as well as the destruction, theft, or unauthorized or illegal use, modification, or copy of information, programmes, services, equipment, or [59] communication network.

Cybercrime is defined as the commission of a crime using technology, such as computers, smartphones, or tablets. As a result, this type of criminality has been tremendously costly to the economy, with estimations of $575 billion lost annually worldwide, according to the report. When the Internet first became widely available around the world, China saw it differently than other countries. Because radio and television shows were uploading their recordings to the Internet for anyone to view whenever they wished, China appeared to treat the Internet as a new [60] type of media. Cybercrime, on the other hand, occurs in a different setting than traditional crimes, which may result in different risk factors for both offending and victimization [61]. Traditional offending and victimizations necessitate physical interaction between victims and offenders; however, there is no physical convergence in space or time between offenders and victims in cybercrime. The author of this research offered a framework to help us fight cybercrime no matter where we are by monitoring the actions we undertake on our electronic devices [62]. Scammers take advantage of the fact that cyber criminals are difficult to track down. An in-depth examination of cyber-crime in India has been conducted in this article. According to the author, fraud cases are on the rise, and the majority of victims are between the ages of 20 and 29. Children and women are disproportionately affected. As a result, awareness campaigns are essential in India to prevent or minimize cybercrime [63].

III. About Cyber Security

The growing requirement for computer security, as well as the tendency of cyberization (the sustained use of the Internet or cyberspace by terrorist groups, militias, or other similar groups engaged in conflicts to promote and disseminate their causes), are trademarks of the twenty-first century. The rise in cybercrime, digital currency, and e-governance has been matched by a recent surge in investment in new technology for computer security around the world. The term "cyber security" refers to approaches and procedures for safeguarding digital information. An information system stores, transmits, or uses the data. After all, data is what a criminal seeks. The network, servers, and computers are merely conduits for data. Cyber security that is effective lowers the danger of cyber-attacks and protects companies and individuals against illegal use of systems, networks, and technology.

Cyber security is a set of strategies and processes for defending computers, networks, databases, and applications against assaults, illegal access, modification, or destruction. It can also play a vital role in the development of information technology and Internet services. There are various trends in cyber security, the most prominent of which is Web application. Web applications are now one of the most widely used platforms for delivering information and services via the Internet. Cyber security refers to the technologies, techniques, and procedures that are used to prevent computers, programmes, networks, and data from being hacked, damaged, or accessed without authorization [65]. Specialists in cyber security and forensics are increasingly dealing with a wide range of cyber threats in near-real-time. The capability to detect, analyze,

and defend against such threats in near real-time conditions is not possible without employment of threat intelligence, big data, and machine learning techniques. Cyber security [66] is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.

IV. History of Cyber Security

Worms, viruses, Trojan horses, spyware, and malware were not even mentioned in the common information technology (IT) vernacular seventy years ago. The development of viruses was the catalyst for the creation of cyber security. But how did we end up here in the first place? Jon Von Neumann's "The Theory of Self-Reproducing Automata" was published in 1949. Cybercriminals employ this notion [68] to create self-replicating software, such as viruses. In 1969, UCLA professor Leonard Kleinrock and student Charley Kline sent the first electronic communication from the UCLA SDS Sigma 7 Host computer to Stanford Research Institute programmer Bill Duvall. This is a well-known narrative and a pivotal milestone in the digital world's history. The UCLA sent a message with the term "login" in it. After typing the first two letters "lo" the system crashed.

The first computer "worm" was built in the 1970s by Robert Thomas, a researcher for BBN Technologies in Cambridge, Massachusetts. The Creeper was the name of the creature. "I'M THE CREEPER: CATCH ME IF YOU CAN", said the Creeper, who attacked computers by bouncing from system to system. The first antivirus software was built by Ray Tomlinson, the inventor of email, who created a replicating programme called The Reaper, which would track down Creeper and delete it. Cyber-crime grew more powerful after Creeper and Reaper. As computer software and hardware improves, so do security breaches. With each new breakthrough, hackers discovered a new vulnerability or a means to circumvent security measures. The Russians were the first to use cyber power as a weapon, in 1986. Marcus Hess, a German citizen, gained access to 400 military systems, including Pentagon CPUs. He intended to sell secrets to the KGB, but an American astronomer, Clifford Stoll, caught him before that could happen. In 1988, a man named Robert Morris had an idea: he wanted to test the size of the internet. To do this, he wrote a program that went through networks, invaded UNIX terminals, and copied itself. The Morris worm was extremely aggressive, slowing systems to the point where they were unusable. He subsequently became the first person to be convicted under Computer Fraud and Abuse Act.

The Melissa virus was released in late 1999. This was a macro-virus that was specifically designed to infect email accounts. The virus would get access to these emails with the goal of sending out mass emails. The author was one of the first to be found guilty of creating malware. He was given a five-year term after being accused of causing $80 million in damages. In 2013 and 2014, Yahoo was the target of one of the most serious cyber-attacks [69]. Yahoo accounts belonging to nearly 3 billion people were compromised as a result of the assaults. The attacks took advantage of vulnerabilities that had not yet been addressed. The hackers installed malware on Yahoo's systems using spear phishing techniques, giving them unrestricted backdoor access. They gained access to Yahoo's backup databases and stole sensitive data such as names, emails, passwords, and password recovery questions and answers.

Viruses were becoming more lethal, invasive, and difficult to regulate. We've already seen big cyber-attacks, and the year isn't even halfway through yet. These are only a few examples, but they demonstrate that cyber security is a must-have for both enterprises and small businesses. As shown in the timeline above, cyber security is a never-ending cat and mouse game. Attackers are gaining new talents and employing new methods and techniques as the internet evolves. Defenders, on the other hand, react by playing catch-up. According to Gartner Inc.'s projection [70], global cyber security spending would reach $133.7 billion by 2022. Cyber-attacks are becoming more sophisticated, prompting businesses to invest more in establishing data breach prevention solutions.

V. Why Cyber Security Is Essential

We live in a digital age, which recognizes that our personal data is more susceptible than ever. From internet banking to government infrastructure, we all live in a connected world where data is stored on computers and other devices. A component of that data [71] may contain sensitive information, such as intellectual

property, financial data, personal information, or other sorts of data [72], to which unlawful access or exposure could result in negative effects. One of the most significant difficulties humanity will confront in the next two decades is cyber-criminal activities. Cyber-attacks are the world's fastest-growing crime, and they're getting bigger, more sophisticated, and more expensive. According to Cyber Security Ventures, cybercrime losses will cost the globe $6 trillion per year by 2021, far more than the damage caused by natural catastrophes in a year and far more profitable than the global trade in all major illegal narcotics combined. According to Cisco, Asia-Pacific businesses face six cyber-attacks per minute. Not only are governments and corporations at risk from hackers' acts and intents, but individuals are also at risk. Hackers steal an individual's personal information and sell it for profit, which is known as identity theft [73]. Recognizing that no one is immune to the threat posed by cybercrime, from individuals to major multinational corporations, is a critical step in winning the fight against cybercrime. It will never happen to me,' is one of the worst things you can believe.

Education is a critical component of any cyber-crime plan, and it is critical that everyone in your organisation, from the CEO to the clerical staff, is aware of the hazards associated with using your network and apps [74]. Our youth are one of the most crucial populations to educate about cyber security. While kids may not be banking or shopping online with credit cards, they can make it very easy for cyber criminals to gain access to data by opening insecure personal accounts. Weak passwords and improper email or social media practises make it much easier for others to get into your account and access the information of your friends and family. No one wants to be accountable for cybercrime on their loved ones, whether it's a bank account number [75], and a photo that should be kept secret or complete identity theft. Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber-attack and it is critically important because it helps to preserve the lifestyles we have come to know and enjoy.

VI. Cyber Security Types

It's critical to understand the many types of cyber security in order to be better protected. The procedures used to protect data from being stolen or assaulted are known as cyber security types. Computers, mobile devices [76], networks, servers, and data are all protected from external threats by cyber security, often known as electronic information security. It acts as a security barrier, ensuring that your data and what you save on your devices are not vulnerable to outside attacks [77]. Critical infrastructure security, network security, application security, information security, cloud security, data loss prevention, and end-user education are some of the topics covered. Cyber-attacks are expected to cost the global economy US$6 trillion by 2021, according to estimates.

6.1 Cloud Security

Due to its increased anonymity, cloud-based data storage has become a popular alternative during the previous decade. Even though cloud storage is more secure, you should still protect it with software that monitors activity and can notify you if anything unusual occurs with your cloud accounts. To assist reduce the dangers associated with on-premises attacks, a software-based technology that safeguards and monitors your data in the cloud [78].Hence, Amazon Web Services, Microsoft Azure, and Google Cloud present their customers with a cloud computing platform, where the users can store, and monitor data, by implementing a security tool. Cloud computing security is similar to traditional on-premise data centres, only without the time and costs of maintaining huge data facilities, and the risk of security breaches is minimal.

6.2 Critical Infrastructure Security

Infrastructure is vital. To secure systems with vital infrastructure, cyber security techniques are used. They are systems that societies rely greatly on. Electricity grids, water purification, traffic lights, shopping malls, and hospitals are among them. They are not directly tied to a potential cyber breach, but they can serve as a platform for cyber malware to infect the endpoints to which these systems are connected. Organizations that utilize the critical infrastructure must also evaluate the amount of damage caused due to cyber-attacks. These organizations must have a contingency plan that would help their businesses to bear no brunt of the cyber-attacks. The security and resilience of this critical infrastructure is vital to our society’s safety and well-being.

6.3 Data Loss Prevention (DLP)

Data loss prevention (DLP) ensures that sensitive or vital data is not sent beyond the business network. The word refers to software that allows a network administrator to manage the data that users can send and receive. Develops policies and practises for dealing with and preventing data loss, as well as recovery plans in the case of a cyber-security breach. Setting network permissions and policies [79] for data storage is part of this. Data loss prevention solves three main objectives that are common pain points for many organizations: personal information protection / compliance, intellectual property (IP) protection, and data visibility.

6.4 Application Security

Uses software and hardware to protect against external dangers that may arise during the development of an application. Because apps are increasingly accessible across multiple networks, they are more vulnerable to cyber-attacks. Applications can be protected with cyber-sec antivirus software, firewalls, and encryption services. Companies and organisations can discover sensitive data sets and secure them with specialised applications regarding the datasets using an application security network. Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities. A router that prevents anyone from viewing a computer's IP address from the Internet is a form of hardware application security.

6.5 Information Security

Data encryption, often known as data security, protects data from unwanted access or alteration while it is being stored or sent from one machine to another. Data in whatever form is protected from unauthorised use, disclosure, deletion, or other types of malintent by information security, also known as InfoSec. Mantaps, encryption key management, network intrusion detection systems, password rules, and regulatory compliance are examples of these procedures. Information can be anything from your personal information to your social media profile, cell phone data, biometrics, and so on. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc. During WWI, the Multi-tier Classification System was created with the sensitivity of information in mind. With the outbreak of the Second World War, the classification system was formally aligned. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data. Information Security programs are builds around three objectives, commonly known as CIA Confidentiality, Integrity, and Availability.

6.6 Network Security

While cyber security is concerned with dangers from the outside, network security protects your internal networks from hostile intrusion. Internal network security maintains the safety of internal networks by safeguarding infrastructure and restricting access to it [80]. Users' activities are also recorded because many websites utilise third-party cookies. This can be beneficial to businesses in terms of expanding their operations, but it also exposes clients to fraud and sexual exploitation. As a result, enterprises must implement a security programme to monitor the internal network and infrastructure in order to combat cyber-attacks and viruses linked with the network. Machine learning technology, according to experts, might be used to inform authorities in the event of unusual traffic. Organizations must continue to improve their network security by enacting policies that can protect them from cyber-attacks. Security teams are now employing machine learning to highlight aberrant traffic and alert to dangers in real time, which helps them better manage network security monitoring. Network administrators are continuing to implement policies and procedures to protect the network from unwanted access, modification, and exploitation. Implementing two-factor authentication (2FA) and creating fresh, strong passwords are two examples of network security.

6.7 End User Education

Recognizes that cyber security solutions are only as strong as their weakest connections, which are the people who use them. End user education include instructing users on best practises such as not clicking on unexpected links or opening strange attachments in emails, both of which can lead to the spread of malware and other dangerous software. Teaching users to not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

6.8 Internet of Things (IoT) Security

The Internet of Things is thought to be the next technology revolution's tool. According to a forecast by Bain and Company, the IoT market will grow by 520 billion dollars by 2021. IoT provides the user with a variety of important and non-critical appliances, such as appliances, sensors, printers, and Wi-Fi routers, among other routers, through its secure network [81]. According to Cytelligence, hackers attacked smart home and internet of things (IoT) devices such as smart TVs, voice assistants, [82] connected baby monitors, and cell phones more frequently in 2019. Hackers who obtain access to a connected home's Wi-Fi credentials may also gain access to the users' personal information, such as medical records [83], bank statements, and website login information. According to the survey, one of the most significant barriers to deploying IoT in any firm is the security risk. Organizations get insightful analytics, legacy embedded systems, and a secure network by integrating the system with IoT [84] security.

6.9 Operational Security

During the Vietnam War, the United States military invented the term "actions security" as a result of military operations headed by the Purple Dragon team. Despite North Vietnam's and the Viet Cong's failure to decrypt U.S. communications and the lack of true intelligence collecting assets on the inside, Purple Dragon discovered that America's foes were able to predict their strategy and tactics. Operational security (OPSEC) is a process by which businesses examine and secure public data about themselves that, if properly studied and coupled with other data by a competent adversary, could disclose a larger picture that should remain concealed. Identification of important information, threat analysis, vulnerability analysis, risk assessment, and deployment of effective countermeasures are the five steps in the process.

6.10 Endpoint Security

The majority of security breaches in the past occurred through the network. Today's dangers, on the other hand, are increasingly pouring in through endpoints, implying that centralised network defence is insufficient. Shifting security perimeters that aren't clearly defined necessitate the addition of new levels of security via endpoint protection. To avoid the risks that can come from the use of remote devices, security must maintain better control over access points [86]. This enables businesses to defend their servers, workstations, and mobile devices from cyber-attacks both locally and remotely. The interconnection of devices on a network creates access points for threats and vulnerabilities. By prohibiting efforts to access these entry points, endpoint security effectively safeguards the network. File integrity monitoring, antivirus and anti-malware software, etc. are major techniques used.

6.11 Website Security

This is used to prevent and protect websites from internet cyber security threats. Website security programmes will cover the database, apps, source codes, and files of the website. In recent years, the incidence of data breaches on websites has steadily increased, resulting in identity theft, downtime, financial losses, reputation and brand image damage, and so on. The main reason for this is that many website owners believe their site is safeguarded by their web hosting provider. Thus, leaving them vulnerable to cyber-attacks. Some of the important techniques and tools used for website security are website scanning and malware removal, website application firewall, application security testing, etc.

6.12 Big Data Security

Malware & ransomware attacks, corrupted and vulnerable equipment, and dangerous insider programmes are all examples of cyber security dangers that can be detected using big data analytics technologies [87]. Big data analytics appears to hold the most promise in terms of increasing cyber security in this area. Big data analytics software can assist you in predicting the type and severity of cyber security risks. By accessing data sources and trends, we can assess the complexity of a potential assault [88]. These tools also enable you to analyse current and historical data to determine which trends are acceptable and which are not. Experts can use intelligent Big data analytics [89] to create a predictive model that can send out an alarm as soon as it detects a cyber-security attack entry point.

6.13 Blockchain Security

Blockchain presents itself as a distributed ledger, referring to the way a database is shared among numerous participants on a peer-to-peer network without the involvement of a central authority [90]. The use of Blockchain techniques in content distribution networks. We believe that these networks are a fantastic illustration of how we can utilise Blockchain to add value to existing processes or technology because they are frequently used presently. A Content Delivery Network (CDN) is a network of computers that are connected and contain different versions of the same piece of material. The goal of its design is to optimise the bandwidth available in a service in order to increase the availability [91] and access to data as much as possible. Several assaults have recently been carried out against social media platforms such as Twitter and Facebook. Millions of accounts were breached as a result of these assaults, with user information falling into the wrong hands. If Blockchain technologies are properly deployed in these messaging systems, further cyber-attacks may be avoided. Sensitive data can be protected utilising Blockchain by ensuring a decentralised type of data storage [92]. Hackers would find it more difficult, if not impossible, to breach data storage systems using this mitigating strategy. Many storage service companies are assessing ways Blockchain can protect data from hackers.

VII. Varieties of Cyber Threats

A cyber-attack is any type of hostile activity that uses numerous means to steal, manipulate, or destroy data or information systems and targets computer information systems, infrastructures, computer networks, or personal computer devices.

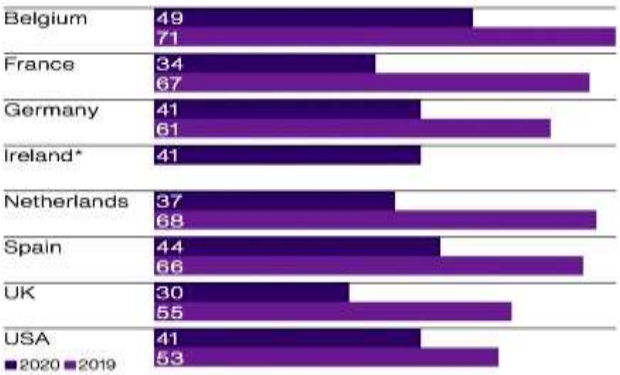

Figure 1: The Cyber Event in 2019 to 2020

Organizations require cyber security experts and specialists to deal with the numerous types [93] of cyber security attacks that come with varying technicalities. Over the past 12 months, the typical cost to businesses of cyber events and breaches increased to $57,000 [94]. This is nearly a six-fold increase over the $10,000 raised the previous year. Hackers are increasingly employing phishing, malware infestations, and DDoS operations. The larger organisations, on average, are the ones who have paid the most for an internet presence. This is unsurprising given that they were also the most extensively targeted. More than half of all businesses with 1,000 or more employees (51%) reported they have had at least one cyber incident. Cybercrime has a significantly higher cost and intensity. Figures 1 and 2 show that cyber thieves are increasingly targeting energy and manufacturing companies, on top of a sector that has been a target for years. Individuals all over the world are affected by numerous forms of cyber security assaults. The most prevalent types of cyber-attacks are discussed in the section below.

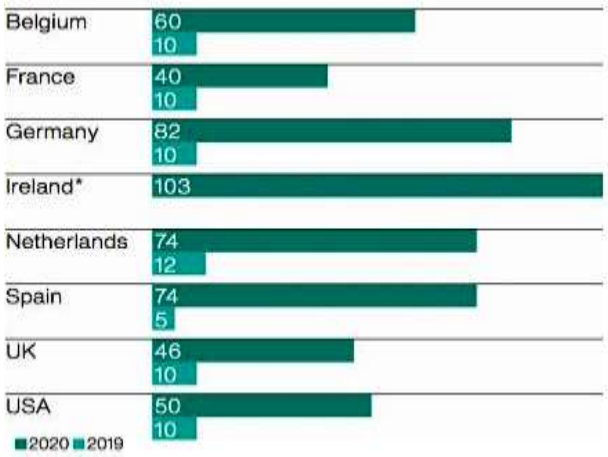

Figure 2: The Incidents and Breaches in 2019 to 2020

7.1 Phishing Attack

One of the most popular sorts of cyber-attacks is phishing. Cyber attackers try to gain personal information or data, such as usernames, passwords, and credit card numbers, by impersonating a trustworthy entity in these circumstances. Phishing is mostly carried out through technological means, such as emails and phone calls. Phishing attacks frequently take the shape of an email purporting to be from a reputable organisation, such as your bank, [95] the tax department, or another trustworthy entity, as seen in figure 3. Now we'll go over the most frequent sorts of phishing assaults in this part.

7.1.1 Spear

Spear phishing is the most popular type of cyber-attack, owing to its ease of execution and startling effectiveness. Spear phishing is a sort of phishing attack that targets a specific group or type of person, such as a company's system administrators. If you go fishing, you might catch an old boot, a tuna, or a flounder, or any other type of fish. When spearfishing, you select a certain fish to pursue, hence the name. The goals are just those goals.

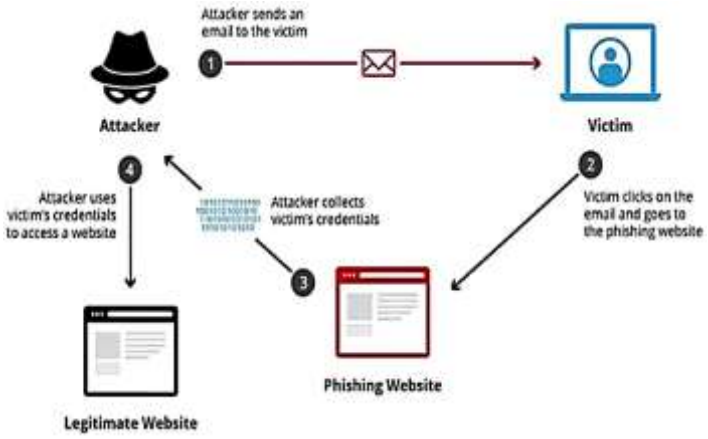

Figure 3: The Phishing Attack

7.1.2 Whaling

Whaling is a sort of phishing that is even more targeted than spear phishing because it targets whales, the big fish. The CEO, CFO, or any Cxx within an industry or even a specific corporation is the target of these attacks. A whaling email can inform them that their company is being sued and that they should click on the link for more information. The link then directs them to a page where they can enter all of their company's important information, such as their Tax ID number and bank account numbers. It's an unfortunate mix-up of nomenclature, because whales aren't fish.

7.1.3 Smishing

Smishing is a type of assault that targets us via text message or SMS. A smishing attack occurs when you receive an SMS message that contains a link to click or a phone number to call. An SMS that appears to be [96] from your bank and informs you that your account has been compromised and that you must contact

your bank immediately is a common occurrence. The attacker will next ask you to verify your bank account number, SSN, and other personal information. The attacker now has complete access of your bank account.

7.1.4 Email Phishing

Since the 1990s, email phishing has arguably been the most popular sort of phishing. These are the emails that a hacker sends to any and all email addresses he or she can get their hands on. The email usually informs the recipient that their account has been hacked and that they must respond promptly by clicking on the 'this' link. Because the English is not always clear, these attacks are frequently easy to notice.

7.1.5 Search Engine Phishing

Hackers use search engine phishing, also known as SEO poisoning or SEO Trojans, to get the top result on Google or other search engines. If they succeed in convincing someone to click on their link, they will be directed to their (hacker) website. They got you when you interacted with it and entered sensitive info. This might be any form of website; excellent choices include banks, PayPal, social networking, and shopping, to mention a few.

7.1.6 Vishing

Vishing is a type of cybercrime that employs the use of a phone to collect personal information from victims. Cyber criminals utilize smart social engineering strategies to persuade victims to act, giving them sensitive information and access to bank accounts. This is known as voice phishing. To deceive consumers into giving critical information, vishings use phoney phone numbers, voice-altering software, SMS messaging, and social engineering. Voice is commonly used by vishing to deceive users.

7.2 Malware

Malware is software that is designed to disrupt the normal operation of any device, including mobile phones, desktop computers, and servers. The user clicks on the malware source, which is usually provided as a script or executable code, and accidentally installs the malware. Some malware strains are aimed to gain persistent network access, while others are designed to spy on the user in order to obtain credentials or other useful information, and still others are just designed to cause disruption. [97] Some malware is designed to extract money from the victim in some way. The most well-known type of malware is ransomware, a programme that encrypts the victim's files and then demands a payment in exchange for the decryption key. The most frequent types of Malware assaults are discussed in this section.

7.2.1 Ransomware

It is a specialized malware distributed to extort money from targets and is one of the most prevalent and known cases of cyber-attacks.

Figure 4: Ransomware

To gain access to the target computer's hard disc, the attacker distributes the malware as a virus. It then encrypts the data and renders the computer and its contents inaccessible until the user pays the ransom demanded by the attacker. It is frequently impossible to decrypt the contents of a file [98] on one's own. WannaCry and Maze ransomware are two recent examples of how malware can cause havoc, compelling many businesses to pay Bitcoins or money to recover their infected equipment and data.

7.2.2 Virus

A virus is a type of self-replicating malware that spreads quickly over the hard disc, including crucial operating system (OS) files, in order to cause maximum harm. It injects itself into existing software/data and spreads with the goal of infecting files. This differs from a Trojan horse, which is designed expressly for a certain application and does not spread itself.

7.2.3 Macro Viruses

These viruses affect Microsoft Word and Excel, among other programmes. Macro viruses attach themselves to the initialization sequence of an application. The virus executes instructions before handing control to the programme when it is opened. The virus replicates and attaches itself to other programmes on the computer system.

7.2.4 Stealth Viruses

To remain undetected, stealth viruses take over system functions. They take over OS files and system processes to avoid being detected by anti-virus software. They hide in boot sectors and partitions and are skilled at evading detection. This means that the infected files/hard disk sectors go undetected. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.

7.2.5 **Boot Record Virus**

They infect the boot loader and attach themselves to the hard drive's master boot record. When the computer starts up, the infector looks for the boot sector, loads into memory, and spreads to other parts of the hard drive. During the days of 3.5-inch floppy discs and MS-DOS, these were fairly ubiquitous. Most viruses have a Terminal Stay Resident component that detects when a disc is inserted and writes to it so that the Master Boot Record is overwritten when the disc is inserted into a new computer.

7.2.6 Trojans

A Trojan, often known as a Trojan horse, is a malicious programme that hides in a useful application. The trojan is a virus delivery technique that cleverly disguises its purpose, hence the term, which is drawn from Greek mythology. It usually [99] lurks in a legitimate programme (such as games, software, or other such items) and creates a back door for attackers to exploit and cause significant damage. As a result, a Trojan horse is a way for attackers to obtain access to a user's device and abuse it further. They do not self-replicate in the same way as viruses do. A Trojan, for example, can be configured to open a high-numbered port so that a hacker can listen and then launch an assault.

7.2.7 Worm

Unlike viruses and Trojans, which are designed for specialised localised attacks, the worm is a special malware designed to propagate from targeted devices to other nodes in the network. These self-contained programmes are frequently distributed as email attachments and are triggered when the user opens them. It is capable of swiftly disseminating itself (by sending emails to contacts and attaching itself as and attachment) and spreading to other systems. Its potential to cause damage is amplified by its complete lack of identification and ability to self-propagate without the attacker's active participation. A worm spreading throughout the internet and overloading email servers can cause denial-of-service attacks against network nodes in addition to undertaking malicious activities.

7.2.8 File Infectors

Viruses that infect executable code, such as.exe files, are known as file infectors. When the code is loaded, the virus is installed. Another variant of a file infector links to a file by producing a virus file with the same name but a.exe extension.
As a result, the viral code will run when the file is opened.

7.2.9 Polymorphic Viruses

These viruses hide their presence through a series of encryption and decryption cycles. A decryption programme first decrypts the encrypted virus and its accompanying mutation engine. The virus then infects a section of code. The virus encrypts the mutation engine and a copy of the virus with an algorithm

corresponding to the new decryption procedure, and the mutation engine produces a new decryption routine. The mutation engine and virus's encrypted package is attached to new code, and the process is repeated. Because of the numerous modifications to their source code, such viruses are difficult to detect but have a high amount of entropy. This characteristic can be used to detect them by anti-virus software or free programmes like Process Hacker.

7.2.10 Logic Bombs

A logic bomb is malicious software that is added to a programme and is activated when a specified event occurs, such as a logical condition or a specific date and time.

7.2.11 Droppers

A dropper is an application that is used to infect computers with viruses. Virus-scanning software may not detect the dropper in many cases since it is not infected with dangerous code. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.

7.2.12 Adware

Advertising banners are displayed while any programme is running, and adware is a software application utilized by businesses for marketing goals. Adware can be downloaded to your system automatically while surfing any website and viewed through pop-up windows or a bar that displays on your computer screen.

7.2.13 Spyware

Spyware is a type of programme that is installed on a user's computer or browser to collect information about them. It secretly records everything you do and delivers the information to a remote user. It can also use the internet to obtain and install additional malicious apps. Spyware is similar to adware in that it is a separate programme that is installed unintentionally when you install another freeware programme.

7. 3 SQL Injection (SQLi)

SQL injection is a sort of attack that targets SQL databases only. SQL statements are used to query data in SQL databases, and these statements are commonly executed through an HTML form on a webpage. If the database permissions are incorrectly specified, the attacker may be able to use the HTML form to run queries that create, read, change, or delete data from the database. The Structured Query Language (SQL) is a database-communications programming language [100]. SQL is frequently used by servers to access and change data between clients and databases. Malicious SQL statements are frequently used by attackers to manipulate computers into executing unwanted and unexpected activities. The attacker can directly access and update the customer's PII from and to databases using the SQL injection (SQLi) approach. SQLi makes the server run malicious code by exploiting known SQL vulnerabilities. By exploiting user interface components such as the search box to dump vital personal information such as login and password directly from the database, attackers are able to bypass all security measures in an application. SQL injection attacks come in a variety of forms.

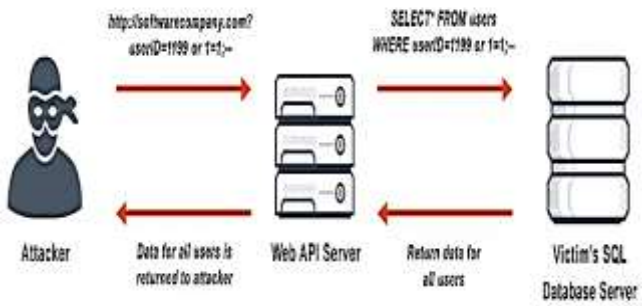

Figure 5: The SQL Injection

7.3.1 Unsanitized Input

It's a form of attack in which the attacker enters user input that hasn't been properly sanitised for characters or validated for expected text. In this situation, the attacker may exploit the flaw by entering character combinations that would cause the database to fetch the entire list of all customer data, which isn't usual database behaviour. This data bounty could then be sold by the attacker on the dark web.

7.3.2 Blind SQL Injection

It does not directly retrieve information from the database, instead relying on a number of parameters that the attacker notices in order to carry out the assault. The attacker can figure out the database setup by looking at the GET String query in HTTP answers, the turnaround time of retrieving information based on a search query, and asking the database a series of true/false questions, among other things [101]. When the web page does not immediately display user data, this is an advanced SQLi attack tactic. The attacker uses Blind SQLi to undertake reconnaissance, collect sensitive information, and change database contents. They are normally carried out by commanding the database to sleep for a certain amount of time and delaying answers during that time period using the SQL sleep() function.

7.3.3 Second Order SQL Injection

These attacks rely on data submitted by users being stored in the database, which the attacker then retrieves and uses in a malicious SQL statement. They use secondary system behaviour to trigger and allow the attacker to control the database.

7. 4 Denial of Service or Distributed Denial of Service Attacks

The perpetrator of a denial-of-service (DoS) attack attempts to prevent intended users from accessing digital assets by disrupting the services of a host connected to the internet. The attack includes inundating the host server with many more requests than it can manage, causing the server to fail. This renders valid user requests unserviceable, depleting resources and bandwidth. When numerous compromised computers (botnets) send requests at the same time, it's called a distributed-denial-of-service (DDoS) assault. Although DoS/DDoS assaults do not directly benefit the attacker in terms of ransom or phishing attempts, the satisfaction of blocking valid requests is enough for some attackers [102]. Attacking a corporate resource with a DoS attack is far more beneficial, as it has a direct influence on customer loyalty and brand trust. In certain circumstances, attackers combine DDoS with other techniques to launch a larger attack, with DDoS serving as a prelude to disconnecting the system from the network. A DDoS assault occurs when an attacker floods a target server with traffic in the hopes of disrupting, if not completely shutting it down. Unlike classic denial-of-service assaults, which are detectable and respondable by most modern firewalls, a DDoS attack can use numerous compromised devices to flood the target with traffic. In this part, we'll go through the various types of DoS and DDoS attacks.

7.4.1 TCP SYN Flood Attack

This involves flooding the system with multiple connection requests and exploits the buffer space during a transmission control protocol (TCP) session initialization handshake.

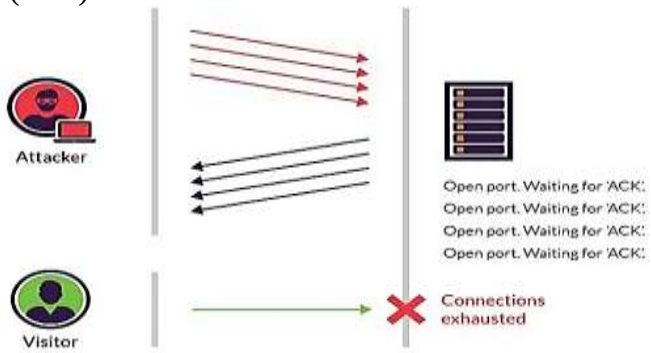

Figure 6: TCP SYN Flood Attack

An attacker uses the buffer space during a Transmission Control Protocol (TCP) session initialization handshake in this attack, as seen in figure 6. The attacker's device sends a torrent of connection requests to the target system's small in-process queue [103], but it does not respond when the target system responds to

those requests. When the connection queue fills up, the target system times out while waiting for a response from the attacker's device, causing the system to crash or become inoperable.

7.4.2 Teardrop Attack

This entails transmitting fragmented data packets to a destination system. TCP/IP fragmentation reassembly flaws (seen in older OS versions) are targeted in this attack, which causes fragmented packets to overlap in the target system depicted in figure 7. Despite the system's best efforts, it fails to rebuild the fragmented packets and crashes. Teardrop assaults are known for their massive payloads. Disable SMBv2 and block ports 139 and 445 if users do not have fixes to protect against this DoS attack.

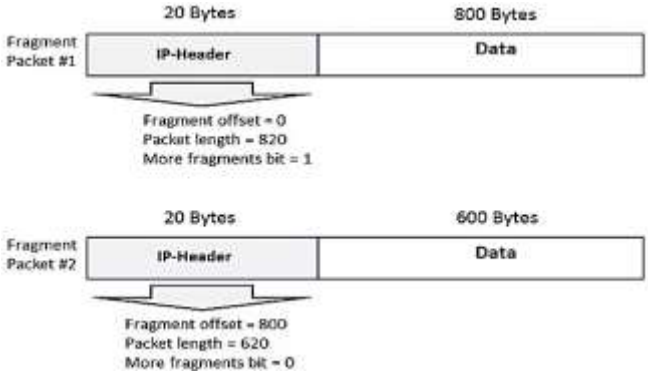

Figure 7: The Teardrop Attack

7.4.3 User Datagram Protocol (UDP) Flood

A network flood, known as a UDP flood, is still one of the most common floods today. The attacker sends UDP packets to a specific target or to random ports, which are usually huge. The attackers usually spoof the SRC IP, which is simple to perform because the UDP protocol is "connectionless" and lacks any kind of handshake process or session. A UDP flood's main goal is to saturate the Internet pipe [104].

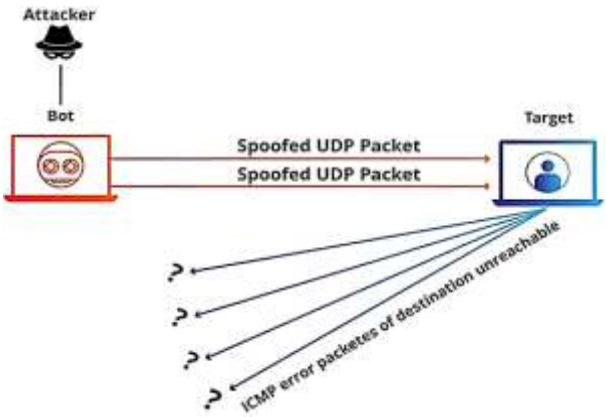

Figure 8: User Datagram Protocol (UDP) Flood

Another effect of this attack is on network and security elements along the path to the target server, particularly firewalls. As a result of UDP flooding, the firewall attached to the server can get overwhelmed, causing the system to shut down, as seen in Figure 8. Firewalls create a state for each UDP packet and are quickly overwhelmed by the influx of connections.

7.4.4 Smurf Attack

To overwhelm a target network with traffic, this attack employs IP spoofing and the ICMP protocol. ICMP echo requests targeted at broadcast IP addresses are used in this attack tactic. These ICMP requests come from a fictitious "victim" address. The attacker would spoof an ICMP echo request from 10.0.0.10 to the broadcast address 10.255.255.255, for example, assuming the intended victim address is 10.0.0.10. This request would go to all IPs in the range, with all the responses going back to 10.0.0.10, overwhelming the

network. This process is repeatable, and can be automated to generate huge amounts of network congestion shown in figure 9.

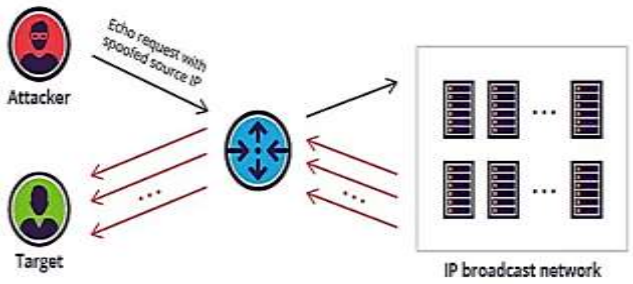

Figure 9: The Smurf Attack

7.4.5 Ping of Death Attack

Pinging a target system with an IP size greater than 65,535 bytes is a form of attack that uses IP packets. Because large IP packets are not permitted, the attacker fragments the IP packet.

Buffer overflows and other crashes can occur once the destination machine reassembles the packet. Ping of death attacks can be prevented by employing a firewall that examines fragmented IP packets for maximum size, as shown in figure 10.

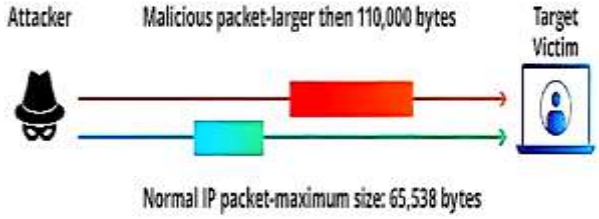

Figure 10: Ping of Death Attack

7.4.6 Botnets

Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks shown in figure 11.

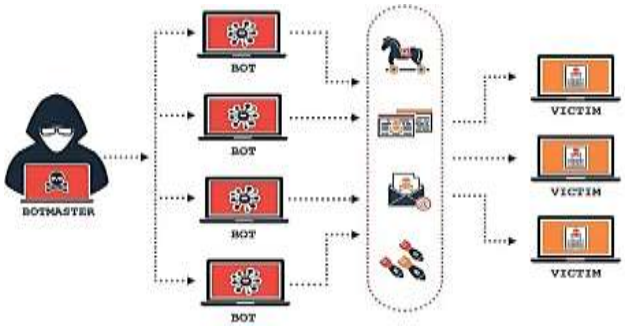

Figure 11: Botnets Attack

These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations.

7.5 Cross Site Scripting (XSS)

Third-party web resources are used in XSS attacks to run scripts in the victim's web browser or scriptable application. The attacker injects a payload containing malicious JavaScript into the database of a website. When the victim requests a page from the website, the website sends the page to the victim's browser, which executes the malicious script depicted in figure 12, which includes the attacker's payload as part of the HTML body. It might, for example, transfer the victim's cookie to the attacker's server, where the attacker can extract it and use it to hijack the victim's session. When XSS is utilized to exploit further vulnerabilities, the most serious effects arise [105]. An attacker can use these flaws to steal cookies as well as track keystrokes, take screenshots, locate and collect network information, and remotely access and manage the victim's machine. While XSS may be used in VBScript, ActiveX, and Flash, JavaScript is the most

commonly exploited, owing to its widespread use on the Internet. What is worse is that neither the website administrator nor the user has any clue about the malicious code put in place, and may result in huge damages if not handled immediately.

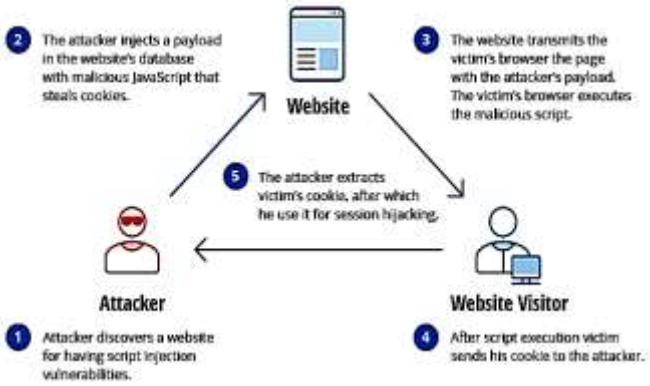

Figure 12: The Cross-Site Scripting (XSS)

7.5.1 Reflected XSS or Non-Persistent XSS Attacks

When an application gets data in an HTTP request but includes the response in an unsafe manner, this sort of attack occurs. The attacker inserts the malicious script into the URL as a query and then publishes it as a link or sends it to the recipient via email (phishing). The script runs when the user clicks on the link. The malicious script injects into the web page that the target system's browser is loading and is executed by the browser displayed in figure 13 since the query has un-sanitized input values. Private information is given to the attacker. In more complex assaults, the attacker can impersonate a user and do any action within the application, including initiating interactions with other users. Others would notice the request originating from the compromised user and become infected as a result.

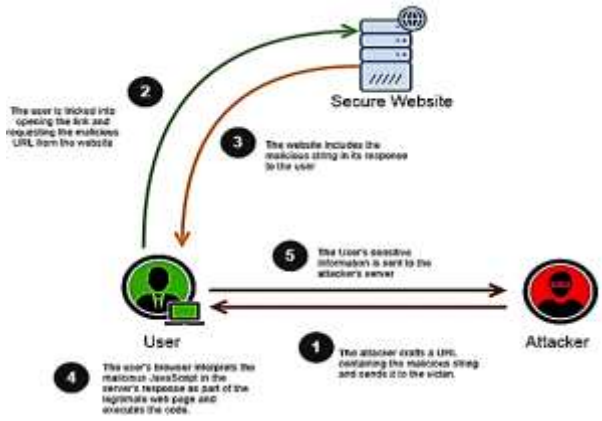

Figure 13: Reflected XSS or Non-Persistent XSS Attacks

7.5.2 Persistent XSS Attacks (also known as Type 2 XSS)

When an attacker keeps user input in the susceptible server without doing adequate validation, this is what happens. In contrast to reflected XSS attacks, the user is compromised simply by browsing the vulnerable web application depicted in figure 14. Other users who visit the hacked [106] website receive the stored inputs and the malicious script is executed in their local browser without having to do anything. They are less common, but they are far more dangerous than their non-persistent equivalent.

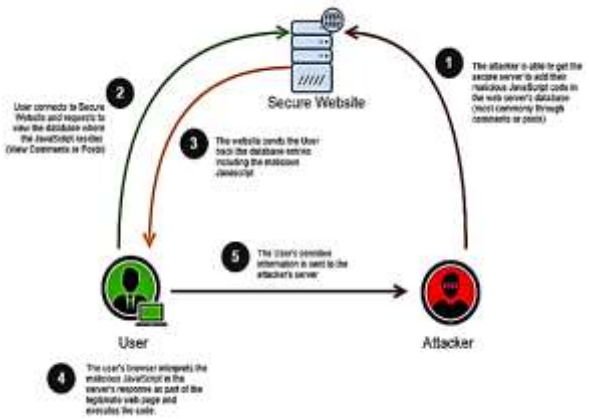

Figure 14: Persistent XSS Attacks (also known as Type 2 XSS)

7.5.3 DOM Based XSS Attack

When a web application publishes data to the Document Object Model without properly sanitizing it, this happens.

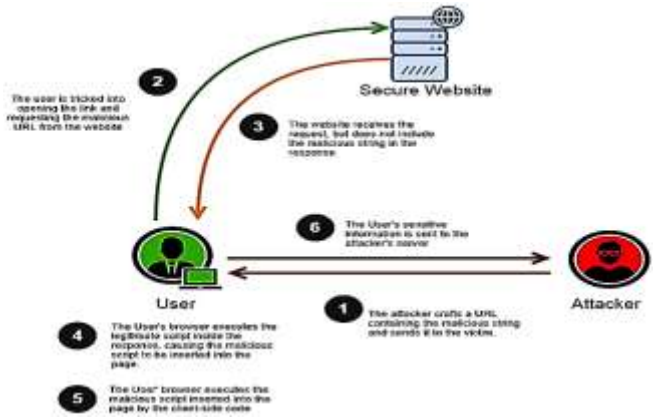

Figure 15: DOM Based XSS Attack

It happens because of flaws in the application's own client-side scripts, not because of any payload provided by the attacker. Figure 15 shows how an attacker can exploit the DOM's various objects to develop XSS attacks. The attacker injects malicious script into the target browser using the vulnerable client-side script.

7.6 Man-in-the-Middle (MiTM) Attack

A man-in-the-middle (MITM) attack occurs when an attacker intercepts communication between two parties with the intent of spying on the victims, stealing personal information or credentials, or altering the dialogue in some way. Most email and chat systems now utilise end-to-end encryption [107], which prohibits third parties from tampering with data transferred across the network, regardless of whether the network is secure or not, as shown in figure 16. IP and DNS spoofing, replay attacks, and session hijacking are all examples of this type of assault. When a hacker gets in between a client and a server's communications, it's called a MitM attack. We'll go over some of the most frequent sorts of man-in-the-middle attacks here.

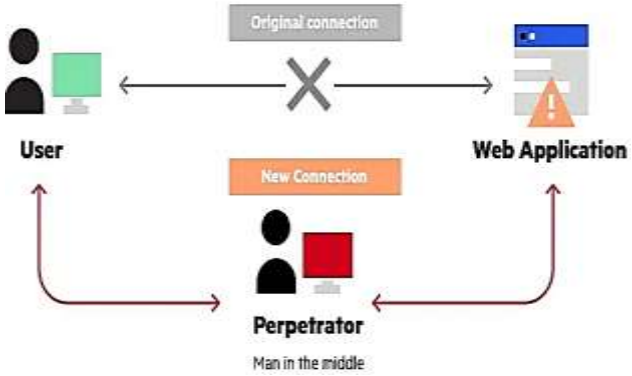

Figure 16: Man-in-the-Middle (MiTM) Attack

7.6.1 Rogue Access Point

The rogue access point is one of the most common wireless security risks, and it's been utilized in a variety of attacks, including DoS and data theft. The rogue access point is an unlawful network node that is nonetheless operational. Assailants may try to get access to adjacent devices using such open wireless access points, as seen in figure 17. They frequently come with no encryption or authentication, in order to connect as many devices as possible. The attacker, thus, compromises the network data.

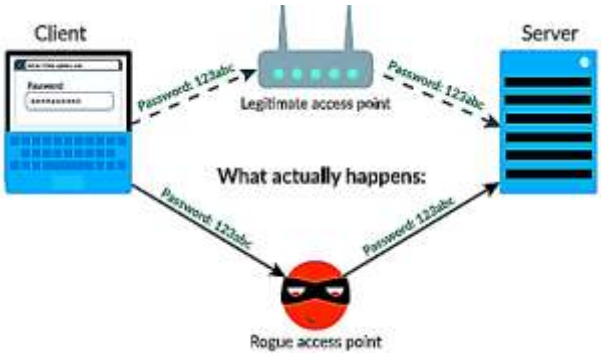

Figure 17: Rogue Access Point

7.6.2 Address Resolution Protocol (ARP)

ARP resolves system IP addresses to physical media access protocol (MAC) addresses in LAN. Two hosts talk to each other by resolving IP addresses to the MAC address by referencing ARP.

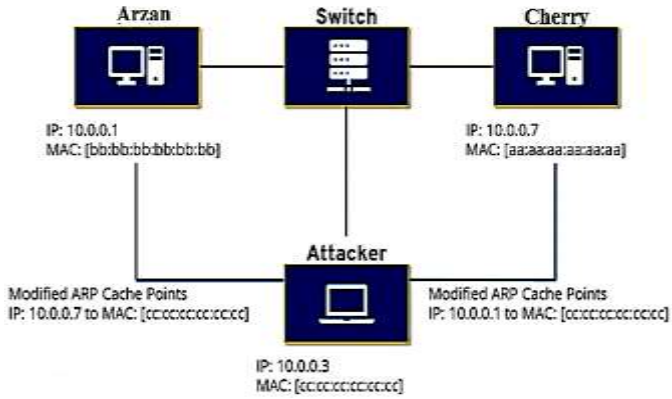

Figure 18: Address Resolution Protocol (ARP)

The attacker transmits false/spoofed ARP messages using ARP spoofing, as demonstrated in Figure 18. As a result, their MAC address corresponds to that of a genuine computer on the network. As a result, the attacker obtains data meant for the original system, intercepting and altering it while in route.

7.6.3 Multicast DNS (mDNS) Attack

MiTM assaults are carried out by the attacker utilising a variety of methods. A DNS query is delivered to all devices in the same broadcast domain on the network. The snooper uses mDNS spoofing on the LAN, similar to ARP spoofing, so that users don't have to remember the addresses to which they connect. The attacker makes a request with bogus data using this protocol's simplification exercise and connects to the system as a trusted network. The attacker's device will appear as a trusted network on the victim's system, allowing the attacker to control the device.

7.6.4 Session Hijacking

The hijacking of a user's session is a common MiTM attack vector. SSL stripping is the process of removing the security layer from HTTPS in order to allow ARP or DNS spoofing.

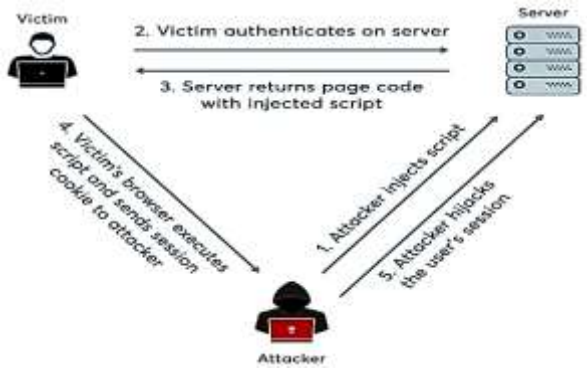

Figure 19: Session Hijacking

Intercepting packets allows attackers to convert secure HTTP requests to non-secure HTTP requests, which convey sensitive data as unencrypted plain [108] text data. An attacker hijacks a session between a trusted client and a network server in this form of MitM attack, as depicted in figure 19. While the server continues the session, believing it is conversing with the trusted client, the attacking machine replaces its IP address for the trusted client.

7.6.5 IP Spoofing

An attacker uses IP spoofing to persuade a system that it is interacting with a known, trusted entity, allowing the attacker to gain access to the system. Instead of sending a packet to a target host with its own IP source address, the attacker sends a packet with the IP source address of a known, trustworthy host. The target host might accept the packet and act upon it.

7.6.6 Replay Attack

A replay attack on data delivered over a network is a sort of security attack. In this assault, a hacker or someone with unauthorised access intercepts traffic and transmits it to its intended destination, impersonating the original sender. The receiver thinks it's an authorised communication, but it's actually the attacker's message. The Replay Attack is distinguished by the fact that the client receives the message twice, hence the name.

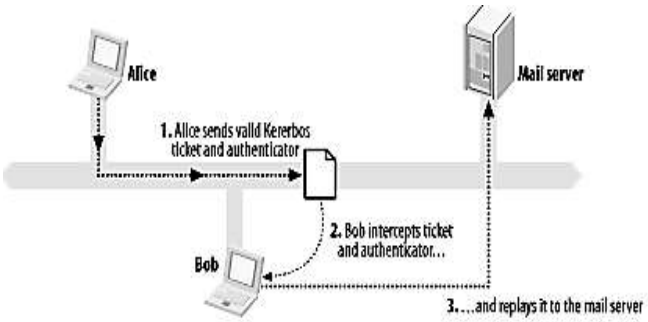

Figure 20: Replay Attack

Figure 20 shows Alice (the unsuspecting end user) obtaining tickets to authenticate to her mail server. Bob, the malicious hacker, is secretly monitoring all network activity between Alice, the mail server, and the Kerberos Key Distribution Centre (KDC). Because the TGT must be decrypted with Alice's password, which Bob does not know, Bob is unable to utilise it immediately in the first stage. However, when Alice sends her encrypted ticket and authenticator, Bob can intercept that message and replay it to impersonate Alice to the mail server.

7.7 Zero Day Attack

A flaw in your programme, hosted application, or even hardware could be the source of the vulnerability. It's usually a bug that escaped the testing team's notice, and as a result, the development team is unaware of it. When a known flaw is discovered, the development team does not have a patch ready to address it before releasing it to the production environment. This exposes weaknesses that can be exploited by an attacker. It

gets its name from the fact that there is a zero-day window between when vulnerability is discovered and when an attack is launched.

7.8 Advanced Persistent Threats (APT)

When an individual or group acquires unauthorised access to a network and goes unnoticed for a long time, attackers may exfiltrate important data[109], obviating the need for the organization's security staff to investigate. APTs are often launched against nation states, huge corporations, or other extremely valuable targets since they require sophisticated attackers and a great amount of work.

7.8.1 Insider Threats

Every day, a large number of cyber-attacks occur, and the most alarming aspect is that most of the time, an insider is involved in the process to assist the Cybercriminals in obtaining information about their firm. Insiders of target businesses are often the ones that carry out these cyber-attacks on a daily basis. They assist external attackers by supplying all essential information, resulting in further consequences. This type of cyber-attack could happen in a business setting. It is also one of the common types of cyber-attacks on banks and types of cyber-attacks on financial institutions.

7.8.2 AI Powered Attacks

Machine learning focuses on teaching a machine to execute several tasks on its own rather than relying on people to do so.

Artificial intelligence being used to launch sophisticated cyber-attacks is a frightening idea because we don't yet know what such attacks will be capable of. Artificial Intelligence [110] is sometimes used to hack into digital systems in order to obtain illicit data. It can also be used to steal confidential financial data. It affects national security and even goes to the extent of harming individuals emotionally.

7.8.3 Birthday Attacks

Birthday attacks are brute force operations that try to stifle contact between customers and various members of a firm, starting with the CEO and ending with the employees. Birthday attacks target hash algorithms, which are used to check the integrity of messages, software, and digital signatures. A message digest (MD) of constant length is produced by a hash function, regardless of the length of the input message; this MD uniquely describes the message. When a hash function is used to process two random messages, the birthday attack refers to the likelihood of discovering two random messages that generate the same MD. If an attacker calculates the same MD for his message as the user, he can securely replace the user's message with his, and even if the receiver compares MDs, he will not be able to detect the replacement.

8. Business Email Compromise (BEC) Attack

In a BEC attack, the attacker targets specific persons, usually employees with the authority to make financial transactions, in order to dupe them into transferring funds to an account controlled by the attacker. In order to be successful, BEC assaults normally necessitate extensive planning and study. Any information about the target organization's executives, workers, customers, business partners, and potential business partners, for example, will aid the attacker in persuading the employee to hand over the funds depicted in figure 21. BEC assaults are one of the most expensive types of cyber-attacks.

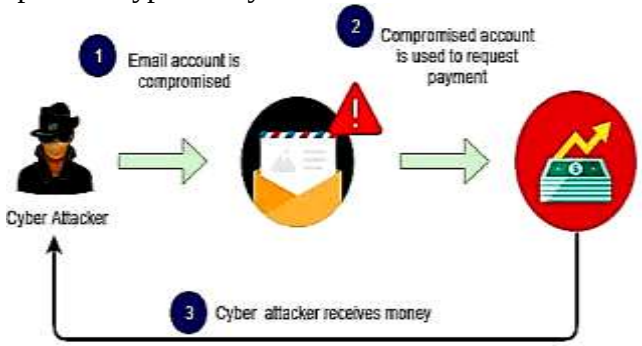

Figure 21: Business Email Compromise (BEC) Attack

9. Cryptojacking

Cryptojacking is when hackers get access to a user's computer or device and use it to mine cryptocurrency like Bitcoin. Although crypto jacking is less well-known than other attack vectors, it should not be overlooked, as demonstrated in figure 22. When it comes to this form of assault, organisations don't have a lot of visibility, which means a hacker may be mining crypto currencies using valuable network resources without the organization's knowledge. The draining resources from a company's network are significantly less troublesome than stealing sensitive information.

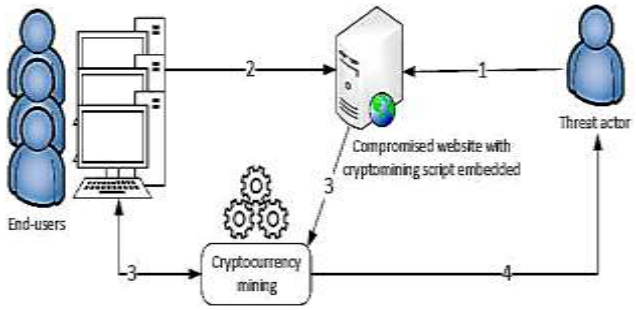

Figure 22: The Cryptojacking Attack

10. Drive-by Attack

A 'drive-by-download' assault occurs when an unwitting victim accesses a website that then infects their computer with malware. The website in question could be one that the attacker controls directly or one that has been hacked. Malware is sometimes embedded in content such as banners and adverts. These days exploit kits are available which allow novice hackers to easily setup malicious websites or distribute malicious content through other means.

11. Password Attack

As you may have guessed, a password attack is a form of cyber-attack in which an attacker attempts to guess, or "crack," a user's password. Although a description of these numerous ways is beyond the scope of this article, there are many distinct techniques for cracking a user's password. The Brute-Force assault, Dictionary attack, Rainbow Table attack, Credential Stuffing, Password Spraying, and Key logger attack are only a few examples. Of course, attackers will attempt to get a user's password via Phishing tactics.

12. Eavesdropping Attack

An eavesdropping attack, sometimes known as "snooping" or "sniffing", occurs when an attacker searches for unsecured network connections to intercept and access data being transferred across the network [111]. Employees are required to use a VPN when accessing the company network from an insecure public Wi-Fi hotspot for this reason. Interception of network communication is used in eavesdropping attacks. Passwords, credit card numbers, and other personal information that a user may be sending over the network can be obtained by eavesdropping. Eavesdropping can be done in two ways: passively or actively. The hacker identifies the information by listening to the network message transmission in passive eavesdropping. In active eavesdropping, a hacker disguises himself as a friendly unit and sends inquiries to transmitters to obtain information. Probing, scanning, or meddling is all terms for the same thing.

13. IoT Based Attacks

As things stand, IoT devices are less secure than most modern operating systems, and hackers are eager to take advantage of these flaws. The internet of things, like AI, is still a relatively new idea, thus we have yet to see what tactics cybercriminals will employ to attack IoT devices [112], and for what purposes. Hackers might go after medical equipment, security systems, and smart thermometers, or they could try to exploit IoT devices to conduct large-scale DDoS attacks.

14. Whaling Attack

A whaling attack is a strategy used by cybercriminals to impersonate a key player in a company and directly target senior or other important employees with the goal of stealing money or sensitive information, or gaining access to their computer systems for illicit purposes. Also known as CEO fraud, whaling is similar

to phishing in that it uses methods such as email and website spoofing to trick a target into performing specific actions, such as revealing sensitive data or transferring money.

VIII. Classification of Cyber Attackers

We now live in the digital age. The majority of individuals nowadays utilise computers and the internet. Because of our reliance on digital devices, unlawful computer activity is on the rise and changing much like any other sort of crime. Despite the fact that the goal of a cyber-attack is always malevolent, the hacker may utilise a variety of tools and strategies to carry it out [113]. An exploitation of computer systems and networks is referred to as a cyber-attack. It employs harmful code to change computer code, logic, or data, resulting in criminality such as data and identity theft. The following are the different types of cyber-attacks.

8.1 Cyber Criminals

This is the most well-known and active type of assailant. They are individuals or groups of individuals who seek to monetize company information, customer data, or other sensitive data on the dark web [114]. They use sophisticated tools and procedures, as well as computer/mobile devices, to carry out intelligent, difficult-to-detect harmful cyber-attacks.

8.2 Hacktivists

They want to spread a non-financial message. They may carry out an attack in order to strengthen their belief system, which could be a political agenda, social ideology, religious ideology, or a cause that they want to be known for through their online misbehaviour. Hacktivism is a form of digital disobedience, according to Dan Lohrmann, chief security officer for Security Mentor, a national security training firm that works with states. It's hacking for a cause. Hacktivists are not like cybercriminals who hack computer networks to steal data for the cash. Depending on the political beliefs they hold, they can be described as progressive, ethical, or plain disruptions among other categories.

8.3 State Sponsored Attackers

They use the assistance of their home country to launch cyber assaults against a specific country in order to undermine its social, economic, or military government. The attackers in this category are not in a rush. The government [115] employs highly competent hackers who specialise in finding and exploiting flaws before they are patched. Due to the immense resources at their disposal, defeating these attackers is extremely difficult. They could even carry out lone wolf attacks to demonstrate their support to a specific state.

8.4 Insider Threats

The insider threat is a threat to a company's security or data that originates from within the company. They are difficult to identify and avoid because of the trust aspect involved. They come from workers, contractors, and third-party affiliates of a business. These attacks could be malevolent, unintentional, or the result of carelessness. Insider threats are classified as follows.

8.4.1 Malicious

Insider threats are attempts by an insider to gain access to an organization's data, systems, or IT infrastructure with the intent of causing harm. Insider threats are frequently attributed to disgruntled employees or ex-employees who believe the organisation has wronged them in some way and believe they are justified in seeking retaliation. When malevolent outsiders use financial incentives or extortion to masquerade insiders, they can pose a threat.

8.4.2 Accidental

Insider threats are threats that are made by mistake by insider employees. In this type of hazard, an employee may accidently delete critical files or share confidential information with a business partner in violation of corporate policy or legal requirements.

8.4.3 Negligent

These are dangers in which employees attempt to circumvent the policies set in place by a company to protect endpoints and valuable data. Employees may try to share work on public cloud services so that they can work from home if their employers have tight regulations for external file sharing. Although there is nothing wrong with these actions, they can expose you to serious hazards. Furthermore, based on the attack's end-point, cyber-attacks are divided into two categories.

8.5 Web Based Attacks

These are the types of assaults that take place on a website or a web application. To harvest credentials, skim visitor payment details, or infect computers with malware or ransomware, web-based attacks use browsers and their extensions, websites, content management systems, and IT components of web services [116] and applications. Malicious JavaScript code was injected into both British Airways and Ticketmaster's websites, resulting in recent data breaches.

8.6 System Based Attacks

If the goal of the assault is to compromise node(s) & system(s) in a network, it is a system-based cyber-attack.

IX. Cyber Security Framework

Because data is the most valuable asset, data security has become a worldwide priority. Data breaches and security flaws might jeopardise the global economy. The development of a cyber-security framework to help mitigate cyber hazards is required for national and economic security [117]. Security of vital systems and data is currently an issue for businesses of all sizes, industries, and business contexts. An organisation needs a strategic, well-thought-out cyber security plan to protect its critical infrastructure and information systems in order to address these problems. As a result, businesses should seek help from cyber security frameworks. When used correctly, a cyber-security framework allows IT security directors to more effectively manage their companies' cyber threats. A company might use an existing cyber security framework or create one from scratch to match its specific demands. Various cyber security groups (including some government bodies) produce these frameworks to serve as guidance for organisations looking to improve their cyber security. A cyber security framework is a set of documents that define an organization's best practises for managing cyber security risk. Such frameworks lower a company's vulnerability exposure. Any cyber security framework will outline how to implement a five-step cyber security approach in detail. The Cyber Security Framework (CSF) is a set of rules that private sector firms can use to detect, identify, and respond to cyber threats. Cyber security frameworks have the potential to become instruments for enforcing government security legislation [118]. The framework also contains guidance to assist businesses in preventing and recovering from cyber-attacks. Even those designed by governments, most cyber security regimes are not mandated. NIST's cyber security Framework, version 1.1 of which was issued in April of 2018, is one of the most popular of these. This paradigm has been mandated for use within US federal agencies and is gaining traction worldwide, including voluntary adoption [119] by banks, energy businesses, defence contractors, and communications firms. Now we'll go through the five primary roles of the cyber security framework, which are depicted in figure 23.

Figure 23: The Five Main Functions of Cyber Security Framework

- **Identify:** To manage cyber security risk to systems, assets, data, and capabilities, companies must first understand their environments.

- **Detect:** Organizations must put in place the necessary procedures to detect cyber security incidents as quickly as feasible.

- **Protect:** Organizations must create and put in place suitable controls to limit or contain the consequences of potential cyber security incidents.

- **Respond:** Businesses must be able to build reaction plans to mitigate the effects of cyber-attacks.

- **Recover:** Businesses must devise and implement effective strategies for restoring capabilities or services that have been harmed as a result of cyber security incidents.

The cyber security Framework is intended for businesses of all sizes, divisions, and stages of development. The framework was created with flexibility in mind. The framework can be customised to be utilised by any organisation thanks to the built-in customisation option.

9.1 Components of Cyber Security Framework

The cyber security Framework consists of three main components shown in figure 24.

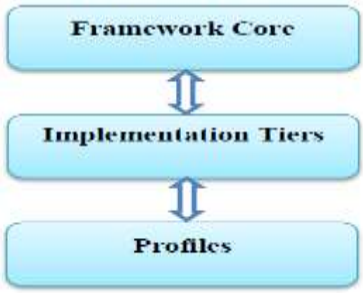

Figure 24: The Cyber Security Framework Components

9.1.1 Framework Core

It provides a list of needed cyber security exercises as well as their outcomes in plain English. The Core helps organisations manage and reduce their cyber security risks in a way that complements their existing cyber security and risk management processes. The core is a collection of desirable cyber security activities and outputs that have been categorised into categories and linked to informative references [120]. The framework core is intended to be intuitive and to serve as a translation layer, allowing multidisciplinary teams to communicate using simple, non-technical language. Functions, Categories, and Subcategories are the three sections of the core.

9.1.2 Implementation Tiers

It assists organisations by defining how they approach cyber security risk management. The tiers assist organisations in determining the appropriate amount of detail for their cyber security programme and are frequently used as a specialised tool to discuss risk appetite, mission necessity, and budget. Tiers show how well an organization's cyber security risk management processes adhere to the Framework's criteria. Tiers vary from Partial (Tier 1) to Adaptive (Tier 4) and define an increasing level of rigour, as well as how well cyber security risk judgments [121] are integrated into broader risk decisions and the extent to which the company provides and receives cyber security information from third parties. Tiers do not always correspond to maturity levels. Organizations should define the intended Tier, ensuring that it satisfies business goals, minimises cyber security risk to acceptable levels, and is fiscally and logistically practical to implement.

9.1.3 Profiles

Profiles are an organization's unique arrangement of organisational requirements, goals, and assets in relation to the Framework Core's desired outcomes. Profiles are primarily used to identify and categorise

open doors for improving an organization's cyber security. Profiles are the unique alignment of an organization's organisational goals and objectives, risk appetite, and resources with the Framework Core's desired outcomes. By comparing a "Current" Profile to a "Target" Profile, a "Current" Profile can be utilised to discover possibilities for strengthening cyber security posture. The goal of profiles is to improve the cyber security framework so that it can best serve the enterprise.

X. Cyber Security Tools

Protecting hardware, software, and data from hackers is referred to as cyber security. It guards against cyber-attacks such as gaining access to, altering, or destroying sensitive data. Cyber-attacks have the capacity to bring an entire country to its knees. As a result, protecting these networks is not an option, but a requirement [122]. It is critical that every firm be informed of the potentially dangerous security attacks and that they be kept secure. Many various components of cyber protection may need to be taken into account. Many cyber security technologies exist that can do a privacy audit on all software, as well as discover and remove the most recent risks [123]. These cyber security solutions assist you in controlling file access and performing forensic investigation. Here are six critical technologies and services that every company should consider to provide the best possible cyber protection.

10.1 Firewalls

The firewall, as we all know, is at the heart of security technologies, and it has evolved into one of the most critical security tools. Its job is to keep unauthorised users from accessing or leaving a private network. It can take the form of hardware, software, or a hybrid of the two. Unauthorized internet users are prevented from accessing private networks connected to the Internet via firewalls [124]. The firewall filters all messages entering and leaving the intranet. Each message is examined by the firewall, and those that do not fit the set security standards are blocked.

10.2 Antivirus Software

Antivirus software is a programme that prevents, detects, and removes viruses and other malware from personal computers, networks, and IT systems. Trojan horses, worms, keyloggers, browser hijackers, rootkits, spyware, botnets, adware, and ransomware are among the threats and viruses that it protects our machines and networks from. Most antivirus software includes an auto-update capability that allows the system to scan for new viruses and threats on a regular basis. It also offers other services like email scanning to ensure that emails are free of harmful attachments and web links.

10.3 PKI Services

Public Key Infrastructure (PKI) is an acronym for Public Key Infrastructure. This programme allows you to distribute and identify public encryption keys. It allows individuals and computers to securely communicate data over the internet while also verifying the other party's identity. We can also exchange sensitive information without PKI, but in that case, there would be no assurance of the authentication of the other party. The people associate [125] PKI with SSL or TLS. It is the technology which encrypts the server communication and is responsible for HTTPS and padlock that we can see in our browser address bar. PKI solve many numbers of cyber security problems and deserves a place in the organization security suite.

10.4 Cyber Security Software Tool

Without a solid cyber security staff, no firm can avoid cyber dangers and security challenges nowadays. Hackers are constantly on the lookout for security flaws in order to exploit them and put companies in jeopardy. India is ranked third among the top ten countries most frequently attacked by cyber criminals. When it comes to the safeguarding of sensitive and private data held by enterprises and individuals, cyber security software plays a critical role. Table 1 summarises the main types of cyber security software tools discussed in this section.

Table 1: Type of Cyber Security Software Tool

Software	Our Ratings	Best For	Category	Features	Free Trial	Price
SolarWinds Security Event Manager	5 Stars	Small to large businesses.	Cloud based tool for SIEM.	Threat Intelligence, SIEM Security & Monitoring, Log correlation & Analysis, Network & Host Intrusion Detection, etc.	Available for 14 days.	It starts at $4500.
Indeni	4.5 Stars	Small to large businesses	Behavioral Analytics, Incident Management	Indeni is an automated crowd-sourced cybersecurity platform for network and security infrastructure.	Free for 90 days	Get a quote
Intruder	5 Stars	Small to large businesses.	Cloud-based Vulnerability Scanner	Over 9,000 security vulnerabilities, Checks for web application flaws, Emerging threat notifications, Smart Recon, Network view, PCI ASV scans available.	Available for 30 days.	Get a quote
LifeLock	5 Stars	Small to large business.	Identity Theft Protection	Block cyber threats, detect & alert, restore & reimburse.	Available for 30 days.	It starts at $7.99/month.
Bitdefender Total Security	5 Stars	Small to large businesses	Cybersecurity software	Multi-layer ransomware protection, Network threat protection, etc.	Available for 30 days	$24.99/year for 5 devices, Bitdefender Total Security: $42.99
Malware bytes	4.5 Stars	Small to large businesses & personal use.	Cybersecurity for home and business.	Multi-layered protection, Prevention of threats in real-time, etc.	Available on request.	Personal: Starts at $399.99/year & Business Starts at $119.97/year.
Mimecast	5 Stars	Small to large businesses.	Email Security & Compliance Platform.	Cyber Resilience for Email, Email Security Web Security, Cyber security Training, etc.	No	Get a quote
CIS	5 Stars	Small to large businesses.	Cybersecurity tools	Securing Organization, Securing a specific platform, & Tracking specific threats.	No	Free as well as paid subscription tools.
SiteLock	5 Stars	Small & Medium-sized businesses	Simply Powerful Website Security	Web threat management, two-factor authentication, enhances security testing for the websites and accelerates the performance	No	$149.99 per site/year
Snort	5 Stars	Small & Medium-sized businesses.	Network intrusion prevention system.	Real-time packet analysis, Packet logging.	No	Free
Wireshark	5 Stars	Commercial & non-profit enterprises, government agencies, & educational institutions.	Network protocol analyzer.	Decryption of various protocols, Output in XML, PostScript, CSV, or Plain Text, Inspection of hundreds of platforms, etc.	No	Free
Webroot	4.5 stars	Businesses and Home use.	Cybersecurity for endpoints, networks, PCs, mobile devices.	Real-time protection, Multi-vector protection, Predictive threat intelligence.	Available	Antivirus: $29.99/device/ year.
Cyber Control	4 stars	Small & Medium-sized businesses	Vulnerability Scanning	Fraud detection reporting suite, and file security review for data privacy and GDPR	Free trial available	Annual License – £29.99

10.5 Network Security Monitoring Tools

Network security monitoring solutions make network administration and monitoring easier while also assisting in security compliance auditing. Anti-virus applications, firewalls, and intrusion detection systems are examples of network security solutions that sit on the network's edge and collaborate to help assure its

safety and security. There are also network security utility tools used in penetration testing, such as network mappers, packet analyser's, and port scanners, which allow system administrators and security professionals to identify the vulnerabilities threat actors can use to exploit your network with DDoS attacks and more.

10.6 Managed Detection and Response Service (MDR)

To break an organization's security, today's cybercriminals and hackers employ more modern techniques and tools. As a result, it is necessary for all firms to employ more powerful cyber security defences. Threat hunting, threat intelligence, security monitoring, incident analysis, and incident response are all part of MDR's advanced security solution. It's a service that was created to help organisations (with limited resources) become more aware of hazards and increase their ability to recognise and respond to threats. MDR also employs AI and machine learning to research, auto-detect dangers, and orchestrate responses in order to achieve faster results.

10.7 Penetration Testing

Penetration testing, often known as pen-testing, is a method of evaluating a company's security systems and the security of its IT infrastructure by safely exploiting weaknesses. These flaws can be found in operating systems, services, and applications, as well as in incorrect setups and unsafe end-user behaviour. Cyber security pros will conduct penetration testing using the same tools and processes used by criminal hackers to look for potential dangers and flaws [126]. A pen test simulates the kind of attacks that criminal hackers might launch against a company, such as password cracking, code injection, and phishing. A simulated real-world attack on a network or application is involved. This test can examine servers, online applications, network devices, endpoints, wireless networks, mobile devices, and other potential points of vulnerability using manual or automated technologies. Once the pen test has been completed successfully, the testers will present us with their results and may be able to assist us by recommending system adjustments.

10.8 Web Vulnerability Scanning Tools

Vulnerability on the Internet Scanning tools are automated programmes that analyse your organization's web applications for security flaws including SQL injection, command injection, path traversal, cross-site scripting, and unsecured server setup. Your Web Vulnerability Scanning tools should provide you with a detailed report after the scan which includes a list of vulnerabilities, detailed explanations of risks and vulnerabilities, and recommendations for remediation.

10.9 Staff Training

Staff training is not a "cyber security instrument," but it is one of the most effective kinds of defence against cyber-attacks to have knowledgeable personnel who understand cyber security. There are numerous training options available now that may teach employees about the finest cyber security procedures. Every company can use these training tools to teach its employees about cyber security and their role in it. We all know that cyber thieves are constantly improving their methods and level of expertise in order to break into firms' security. It has become critical for businesses to invest in training tools and services. If they fail to do so, they risk putting the company in a situation where hackers can simply target their security system. As a result, the cost of investing in these training tools may provide a long-term payback for the corporate organisation in terms of security and safety.

XI. Cyber Security Challenges

Cyber security is becoming a critical part of the country's overall national and economic security plans. The key to overcoming cyber security difficulties is to remain ahead of the game by adopting proactive measures before adversaries [126] exploit the system. It serves a crucial role in protecting our privacy in this day of digitization, when hackers are becoming increasingly sophisticated. We hear about threats like ransomware, phishing, vulnerability exploitation, IoT-based attacks, and so on every day. Cloud infrastructure is going online with the help of the internet, making it vulnerable to a variety of attacks and data breaches. Easy Jet is the most prominent case, with hackers gaining access to the travel records of 9 million customers. Client phone numbers email addresses, personal correspondence, contracts, and non-disclosure agreements with advertising and modelling firms are all said to have been obtained by the hackers. So, it's not just a matter of reputation or [127] monetary loss; there's also the possibility that enterprises would go bankrupt after paying

the fines. As a result, security analysts face numerous issues linked to cyber security, such as securing government classified data, securing private company servers, and so on. Ransomware, phishing assaults, malware attacks, and other cyber security concerns [128] arise in a variety of forms. India is ranked 11th in the world in terms of local cyber-attacks, with 2,299,682 instances reported in the first quarter of 2020. The most recent significant cyber security challenges are discussed in the section below.

11.1 IoT Threats

The Internet of Things (IoT) is a term that refers to a network of connected devices. It is a network of interconnected physical devices that may be accessed over the internet. The connected physical devices are given a unique identification (UID) and can communicate data over a network without the need for human-to-human or human-to-computer contact. Consumers and organisations are especially vulnerable to cyber-attacks due to the firmware and software that runs on IoT devices. By 2021, IoT [129] Analytics predicts that there will be 11.6 billion IoT devices on the market. IoT devices are computational, digital, and mechanical devices that can send data over the internet on their own. Desktops, laptops, mobile phones, smart security devices, and other IoT devices are examples. As the popularity of IoT devices grows at an unprecedented rate, so are the cyber security challenges. When IoT devices are built, they are not designed with cyber security and commercial reasons in mind. To assist manage the risk, every firm should collaborate with cyber security experts [130] to ensure the security of their password rules, session handling, user verification, multifactor authentication, and security procedures. The compromise of sensitive user data can occur when IoT devices are attacked. Safeguarding IoT devices is one of the biggest challenges in Cyber Security, as gaining access to these devices can open the doors for other malicious attacks.

11.2 Ransomware Evolution

Ransomware is a sort of software that encrypts data on a victim's computer and demands payment before the data may be freed. The victim's access rights were restored after a successful payment. Cyber security, data experts, IT, and executives all fear ransomware [131]. Ransomware attacks have grown in popularity in recent years, and in 2020, they will be one of India's most significant Cyber Security threats. Ransomware attacks are dangerous for individual users, but they're much more dangerous for organisations that can't access the data they need to conduct their day-to-day operations. In most ransomware assaults, however, the attackers refuse to release the data even after payment is received, instead attempting to extort more money. With DRaaS solutions, we can back up our files automatically, simply identify which backup is clean, and initiate a fail-over with a single button press when malicious attacks harm our data.

11.3 Blockchain and Cryptocurrency Attacks

The most important invention in the computing era is Blockchain technology. We now have a truly native digital medium for peer-to-peer value exchange for the first time in human history. The Blockchain is a technology that allows for the creation of cryptocurrency such as Bitcoin. The Blockchain [91] is a massive worldwide platform that allows two or more parties to conduct business or conduct transactions without the requirement for a third party to create trust. It's difficult to say what Blockchain technologies will bring to the table in terms of cyber security. Professionals in the field of cyber security can make educated estimates about Blockchain. As Blockchain applications and value in the context of cyber-security [132] develops, there will be a healthy tension, as well as complimentary synergies with existing, proven cyber-security measures. As a result, various attacks have occurred, including DDOS, Sybil, and Eclipse, to mention a few. Organizations need to be aware of the security challenges [92] that accompany these technologies and ensure that no gap is left open for intruders to invade and exploit.

11.4 Server less Apps Vulnerability

Server less architecture and apps are applications that rely on third-party cloud infrastructure or a back-end service like Google Cloud Functions, Amazon Web Services Lambda, and other similar services. Because users access the application locally or off-server on their device, server less apps encourage cyber criminals to quickly distribute threats on their system. As a result, while utilising a server less application, it is the user's obligation to take security precautions. The servers less apps do nothing to deter attackers from accessing our information. If an attacker acquires access to our data through vulnerability such as leaked credentials, a compromised insider, or any other means other than server less, the server less application will

not help. We can use software in conjunction with an application to give us the best chance of defeating cybercriminals. The size of server less apps is often tiny. It enables developers to quickly and simply start their applications. They don't need to worry about the underlying infrastructure. The web-services and data processing tools are examples of the most common server less apps.

11.5 Artificial Intelligence & Machine Learning Expansion

Machine Learning and Artificial Intelligence technologies have shown to be extremely advantageous for significant progress in a variety of fields [133], but they also have flaws. It is a branch of computer science concerned with the building of intelligent machines that function and react in the same way as humans do. Speech recognition, learning, planning, problem-solving, and other artificial intelligence operations are only a few examples. The ability to protect and defend an environment when a malicious attack begins, thus mitigating the impact, is one of the key benefits of incorporating artificial intelligence into our cyber security strategy. Unlawful individuals can use these technologies to carry out cyber-attacks and represent a threat to enterprises. These algorithms can be used to find high-value targets in a vast dataset. Attacks on machine learning and artificial intelligence are also a major worry in India. Due to our country's lack of Cyber Security knowledge, a sophisticated attack may prove too difficult to handle. Artificial intelligence responds quickly to hostile attacks when they threaten a company's operations. After a lot of research and modelling, artificial intelligence may identify anomalies in behaviour patterns that can be used as a defensive tool, but regrettably, hackers, phishers, and thieves can use the same techniques to carry out a cyber-attack.

11.6 BYOD Policies

For its employees, most companies offer a Bring-Your-Own-Device policy. Having such systems creates a slew of problems in terms of cyber security. To begin with, if the gadget is running an out-of-date or pirated version of the software, it is already a prime target for hackers. Hackers can readily obtain confidential corporate data because the method is utilized for both personal and professional purposes. Second, if their security is hacked, these devices make it easier to gain access to your private network. Thus, organizations should let go of BYOD policies and provide secure devices to the employees, as such systems possess enormous challenges of Computer Security and network compromise.

11.7 Cloud Risks

Cloud services are used by the majority of people nowadays for both personal and professional purposes. Due to the flexibility and costs associated with older data centers, businesses are migrating their critical data [64] to the cloud. Moving data to the cloud necessitates adequate configuration and security procedures, or else you risk slipping into a trap.

Cloud service providers only secure their platform; protecting a company's infrastructure against theft and destruction in the cloud is the responsibility of the firm. Firewalls, multi-factor authentication, Virtual Private Networks (VPNs), and other cloud security solutions are available. In summary, the organization must implement procedures and technology to protect itself from both external and internal dangers.

11.8 Technical Skills Gap

When thieves can simply clone identities for any fraud and hackers may exploit any weakness in 2020, the problem will only get worse unless there are an equal amount of resources with the proper capabilities to deal with it. Companies must invest in existing staff training and acquire new resources to assess network dangers in order to avert cyber-attacks. Companies will lose millions of dollars if this does not happen. For navigating threats, education and experience are essential. The IT manager's job is to provide instructional training to enable employees comprehend the security posture of the firm. Describe your company's strengths and weaknesses, as well as how you're actively addressing security flaws. This training should emphasis the roles of your employees in your company's security policy. Companies are investing extensively in making the system more secure, but deploying these new advanced technologies need access to highly qualified technical resources with hands-on experience.

11.9 Out-Dated Hardware

Not all cyber security threats take the form of software attacks.

As software developers become more aware of the dangers of software vulnerabilities, they provide regular updates. However, these new updates might not be compatible with the hardware of the device. This is what leads to outdated hardware, wherein the hardware isn't advanced enough to run the latest software versions. This leaves such devices on an older version of the software, making them highly susceptible to cyber-attacks.

11.10 Biometric Authentication

Biometric authentication is becoming increasingly used as a cutting-edge cyber security solution. While some see biometrics as a novel and effective tool to improve company security, others see it as a potential threat. Biometric identification can take numerous forms, from simple fingertip scanning to more advanced voice, iris, or facial recognition [134]. Many people feel that biometric systems are nearly impossible to hack because the data is impossible to guess and is unique to each user. As a result, it appears to be a better single-factor authentication solution and a fantastic addition to a multi-factor authentication system. Biometric systems, on the other hand, have disadvantages. Biometric information, like a user's login and password, can still be stolen or duplicated, which is a serious issue. In contrast to a password, the user cannot modify their iris scans or obtain a new face. This creates new challenges for cyber security professionals in the future.

11.11 5G Technology

The benefits of 5G technology will be enormous, including improved performance and speed, decreased latency, and increased efficiency. One of the most likely and well-known benefits of 5G technology is that it will enable even more IoT devices to connect to the internet and support more connections between them [135]. This would allow consumers to connect to or monitor their IoT devices remotely over the internet, implying that cyber-attacks are possible. As a result, IoT devices and sensors will require increasingly complex authentication in order to prevent unwanted access. It will, however, come with hazards. To avoid widespread service disruptions, malicious exploitation of IoT devices, and millions, if not billions, of dollars in losses, it is now unavoidable to address the 5G security issue. The 5G standard will result in greater 5G security risks and a wider, diverse attack surface due to the massive number of devices and the impending use of virtualization and the cloud. To comprehend a healthy and strong communications future, the industry needs to preserve a laser focus on 5G security.

11.12 Mobile App Risks

Mobile app development has become a critical component of any company's success. As mobile apps have become more popular among consumers, it's become even more vital for developers to make app security as important as the app's functions. Security is critical in mobile apps, as the data included within the app may be jeopardised if suitable security precautions are not implemented throughout app development. Furthermore, the rising use of mobile applications has resulted in increased susceptibility. Hackers nowadays are interested in obtaining personal information from consumers for their own gain. As a result, when developing apps for the Android and iOS platforms, developers must exercise greater caution. There are various app development platforms available, but none of them can guarantee complete virus security for your app. More Android apps have been discovered to be infested with malware or having flawed code that thieves might exploit. App developers have been known to skip or undertake minimal testing on their apps. A lack of testing, on the other hand, can lead to a data breach. The source code of a mobile app may incorporate code from third-party libraries. Use any library only after thoroughly testing it, as some libraries may be dangerous. Without decryption, we can change the transmitted data into a form that no one else can read. Hackers frequently infect a mobile app through vulnerable source code. Hence, it is important to implement mobile app security best practices when writing code.

11.13 Bluetooth Evolution

People have been using Bluetooth technology to connect their devices and transfer data in a simple manner. Bluetooth has a number of advantages and benefits, but they do not come without risk. Authorization, authentication, and optional encryption are all part of Bluetooth security. The act of verifying the identity of one Bluetooth-enabled device to another is known as authentication. The giving or refusing of Bluetooth connection access to resources or services from the requesting device is known as authorization. Encryption

is the process of converting data into a secret code that cannot be read by eavesdroppers. Bluetooth [136] connections, like any other internet connections, have significant flaws. This is especially true these days, when data hackers are lurking around every corner, waiting to prey on unwary Smartphone users. Blue bugging is a technique in which a hacker gains access to your Bluetooth-enabled phone and uses it to make unwanted calls and send text messages without your awareness. In Blue jacking hackers using your phone to create a malicious phonebook contact and then using that contact to send harmful text messages to your phone. And because the contact is already trusted by your phone, the messages will be opened up automatically, stealing your data in the process. Currently viruses and worms is very common these days for Smartphone users to unknowingly download apps that contain malware and other damaging files. Sometimes you will simply mistype a URL and you end up in a phishing site or download an app and it brings along a harmful malware. These viruses can open up your Bluetooth and attack your shared files. In Bluesnarfing hacker gains access to your Smartphone by connecting to your network, then proceed to copy personal data from your phone applications.

11.14 Recommendation Systems Evolution

Users are increasingly using recommendation systems to expose themselves to the entire digital world via the lens of their experiences, behaviours, preferences, and interests [137]. A recommendation engine is a system that, based on data analysis, proposes products, services, and information to users. The recommendation might be based on a number of criteria, including the user's history and the behaviour of similar users. To arrive at a [138] recommendation, collaborative filtering leverages data from the client and other users who share similar characteristics. Filtering based on the content or attributes of the products you prefer is known as content-based filtering. The goal behind content-based filtering is to classify products with specific keywords, learn what the customer likes, look up those terms in the database, and then recommend similar things. When service providers collect more and more personal information, the public's privacy is jeopardised [139]. Malicious users who seek to skew the suggestions could target the service providers. Commercial recommender systems are frequently required to process large amounts of data in real time nowadays. Using cryptographic techniques to ensure privacy will be a huge issue. [140] has taken things a step further by relying heavily on a user's friends to generate recommendations. However, this will necessitate the service provider creating/maintaining a social network for all of its customers, which may not be a simple task [141]. The other issue is the flawed security models that are typically based on semi-honest attackers. For example, [142] demonstrated that [143] offline recommendation mechanism is subject to key recovery attacks. To acquire these functionalities in reality, service providers must track user behaviour. The bulk of existing solutions are only concerned with protecting the [144] rating vectors for users. Existing privacy-protection technologies, such as anti-tracking techniques, may be integrated to give consumers with more privacy protection. Regrettably, it may not be so simple.

Finally, we may take basic steps to protect our devices and data against cyber threats [145] by using the most up-to-date hardware and software for our digital needs. We'll also need to take more advanced precautions, such as setting up a firewall to add an extra layer of security.

XII. Conclusion

With the rapid advancement of technology, our lives are becoming increasingly digitalized. People now live in a cyber-world where all data and information is stored digitally and online. Whether it's for business, education, shopping, or banking, practically everything is now done online. The focus on cyber security is frequently on attempting to characterize the problem and determine the genuine threat level. All individuals, professionals, legislators, and, more broadly, all decision makers are concerned about cyber security. Cyber security is critical to the advancement of both information technology and Internet services. Cyber-attacks will be on the rise in 2021-22, and not just from the solitary hackers we've come to associate with them, but also from nation-state actors looking to steal data from governments and organizations. Because cyberspace has no borders, a nation's cyberspace is a component of the global cyberspace and cannot be isolated to define its bounds. It has never been easy to maintain cyber security. And, because assaults are becoming more innovative every day, it's vital to define cyber security and determine what constitutes excellent cyber security. Cyber security is a technology that was designed to protect data and information systems kept on computers. This paper comprehensive review covers cyber security, its history, and many types of cyber

security. Explores the various forms of cyber dangers and discusses how cyber attackers are classified once more. The state or process of safeguarding and recovering networks, devices, and programmes from any sort of cyber-attack is known as cyber security.

References

1. Barry M. Leiner at. al., "A Brief History of the Internet," ACM SIGCOMM Computer Communication Review, Volume 39, Number 5, October 2009
2. M. Gallaher, A. Link and B. Rowe, Cyber Security: Economic Strategies and Public Policy Alternatives, Edward Elgar Publishing, 2008
3. T. Rid and B. Buchanan, "Attributing cyber-attacks", Journal of Strate St., vol. 38, no. 1-2, pp. 4-37, 2015
4. B. Zhu, A. Joseph and S. Sastry, "A taxonomy of cyber-attacks on SCADA systems", 2011 International conference on internet of things and 4th international conference on cyber physical and social computing, pp. 380-388, 2011
5. Lillian Ablon, Martin C. Libicki and Andrea A. Golay, Markets for Cybercnme Tools and Stolen Data: Hackers' Bazaar, pp. 1-85, 2014
6. Dawson, J. and Thomson, R., "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance", Frontiers in Psychology, 9(JUN), pp. 1–12, 2018, doi: 10.3389/fpsyg.2018.0074
7. C. L. Philip, Q. Chen and C. Y. Zhang, "Data-intensive applications challenges techniques and technologies: A survey on big data", Information Sciences, vol. 275, pp. 314-347, 2014
8. Yusuf Perwej, "An Experiential Study of the Big Data", International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Science and Education Publishing, Volume 4, No. 1, Pages 14-25, 2017, DOI: 10.12691/iteces-4-1-3
9. Yusuf Perwej ," The Hadoop Security in Big Data: A Technological Viewpoint and Analysis ", International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE) , E-ISSN: 2320-7639, Volume 7, Issue 3, Pages 1- 14, June 2019, DOI: 10.26438/ijsrcse/v7i3.1014
10. Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, "A Perusal of Big Data Classification and Hadoop Technology", International Transaction of Electrical and Computer Engineers System (ITECES), USA, Volume 4, No. 1, Pages 26-38, 2017 , DOI: 10.12691/iteces-4-1-4
11. Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "A Close-Up View About Spark in Big Data Jurisdiction", International Journal of Engineering Research and Application (IJERA), ISSN : 2248-9622, Volume 8, Issue 1, (Part -I1), Pages 26-41, January 2018, DOI: 10.9790/9622-0801022641
12. Cagri B Aslan, Rahime Belen Saglam and Shujun Li, "Automatic Detection of Cyber Security Related Accounts on Online Social Networks: Twitter as an example", SMSociety, July 2018.
13. Igor Skrjanc, Seiichi Ozawa, Tao Ban and Dejan Dovzan, "Large-scale cyber-attacks monitoring using Evolving CauchyPossibilistic Clustering" in Applied Soft Computing, Elsevier, vol. 62, pp. 592-601, 2018
14. Praveen Paliwal, "Cyber Crime", Nations Congress on the Prevention of Crime and Treatment of Offenders, March 2016
15. M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors", Comput. Secur., vol. 25, no. 7, pp. 522-538, 200
16. M. A. Faysel and S. S. Haque, "Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 10, no. 7, 2010
17. Le Compte, D. Elizondo and T. Watson, "A renewed approach to serious games for cyber security", 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, pp. 203-216, 2015
18. N. Virvilis, A. Mylonas, N. Tsalis and D. Gritzalis, "Security Busters: Web browser security vs. rogue sites", Comput. Secur., vol. 52, pp. 90-105, 2015
19. P. Chen, L. Desmet and C. Huygens, "A study on advanced persistent threats" in Communications and Multimedia Security, Springer, pp. 63-72, 2014
20. Yusuf Perwej, "An Evaluation of Deep Learning Miniature Concerning in Soft Computing", International Journal of Advanced Research in Computer and Communication Engineering, ISSN Volume 4, Issue 2, Pages 10 - 16, February 2015 DOI: 10.17148/IJARCCE.2015.4203

21. B. M. Thuraisingham, "Can AI be for Good in the Midst of Security Attacks and Privacy Violations?", Proceedings ACM CODASPY, 2020
22. Yusuf Perwej , “Recurrent Neural Network Method in Arabic Words Recognition System”, International Journal of Computer Science and Telecommunications (IJCST), Sysbase Solution (Ltd), UK, London, ISSN 2047-3338, Volume 3, Issue 11, Pages 43-48, November 2012.
23. Brenner SW. Cybercrime metrics: old wine, new bottles? Va. JL & Tech, 9:13–13, 2004
24. Kshetri N. The simple economics of cybercrimes, IEEE Secur Priv, 4, pp. 33–39, 2006
25. Maloof, M. A. (Ed.), Machine learning and data mining for computer security: methods and applications. Springer Science Business Media, 2006
26. M. Cross and D. L. Shinder, Scene of the cybercrime.Syngress Pub., 2008
27. N. Dhanjani, B. Rios, and B. Hardin, Hacking: The Next Generation: The Next Generation. O’Reilly Media, Inc., 2009
28. Y Perwej, K Haq, U Jaleel, F Parwej, “Block ciphering in KSA, A major breakthrough in cryptography analysis in wireless networks”, International Transactions in Mathematical Sciences and Computer, India, ISSN-0974-5068, Volume 2, No. 2, Pages 369-385, July-December 2009
29. Fink, E., Sharifi, M., & Carbonell, J. G. “Application of machine learning and crowdsourcing to detection of cybersecurity threats”, In Proceedings of the US Department of Homeland Security Science Conference–Fifth Annual University Network Summit, Washington, DC., 2011
30. Greenfield VA, Pa. L. A framework to assess the harm of crim. Br J Crimi., vol. 53, pp. 864–885, 2013
31. T. Grant and S. Liles, On the military geography of cyberspace," Proc. Int. Conf. Inf. Warfa, p. 66, 2014
32. M. Chertoff and P. Rosenzweig. (Mar. 1, 2015). A Primer on Globally Harmonizing Internet Jurisdiction and Regulations, accessed on oct. 15, 2015.
33. Mathieu, T. & Guy, P., “A Framework for Guiding and Evaluating Literature reviews”, Communications of the Association for Inf. System, 37(6), pp 6, 2015
34. H. Lin. (May 15, 2015). Thinking About Nuclear and Cyber Con_ict: Same Questions, Different Answers, accessed on Oct. 15, 2015.
35. Hernández, A., Sanchez, V., Sánchez, G., Pérez, H., Olivares, J., Toscano, K., & Martinez, V. (2016, March). Security attack prediction based on user sentiment analysis of Twitter data. In 2016 IEEE international conference on industrial technology (ICIT) (pp. 610-617). IEEE.
36. Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: a closer look at data breaches. J Cyber secur 2016;2:3–14
37. Buczak, A. L., & Guven, E ,”A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), pp. 1153-1176, 2016
38. Van Slyke SR, Van Slyke S, Benson ML. The Oxford Handbook of White Collar Crime. Oxford University Press, 2016
39. Mittal, S., Das, P. K., Mulwad, V., Joshi, A., & Finin, T. ,”Cyber twitter: Using twitter to generate alerts for cyber security threats and vulnerabilities”, Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 860-867, 2016
40. Punter A, Coburn A, Ralph D. Evolving risk frameworks: modelling resilient business systems as interconnected networks. Centre for Risk Studies, University of Cambridge, 2016
41. Kennedy, Mike. ‘Equifax hack shows we need more regulation.’ Daily Herald. Infotrac Newsstand, 2017
42. Kemal Hajdarevic,Adna Kozic and Indira Avdgic,”Training Network Managers in Ethical Hacking Techniques to Manage Resource Starvation Attacks using GNS3 Simulator”, International Conference on Information, Communication and Automation Technologies (ICAT) , Sarajevo, Bosnia-Herzegovina , pp. 1-6 , Oct 26- 28, 2017
43. Teoh, T. T., Zhang, Y., Nguwi, Y. Y., Elovici, Y., & Ng, W. L. “Analyst intuition inspired high velocity big data analysis using PCA ranked fuzzy k-means clustering with multi-layer perception (MLP) to obviate cyber security risk ”, 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 1790-1793, IEEE, 2017
44. Nguyen KD, Rosoff H, Richard SJ. Valuing information security from a phishing attack. In: International Conference on Applied Human Factors and Ergonomics. Cham: Springer, 2017

45. Lindsay, J. R. “Restrained by design: The political economy of cybersecurity”, Digital Policy, Regulation and Governance, 19, 493–514, 2017
46. Furnell S, Emm D. “The ABC of ransomware protection”, Comp. Fraud & Sec. (10), pp. 5-11, 2017
47. M. McGuire, Understanding the Growth of Cybercrime Economy. Bromium, 2018
48. Khan, R., & Urolagin, S. “Airline Sentiment Visualization, Consumer Loyalty Measurement and Prediction using Twitter Data”, International journal of advanced computer science and applications, 9(6), 380-388, 2018
49. Xingan Li. “Crucial Elements in Law Enforcement against Cybercrime.” Inte. Journal of Information Security Sci. , vol. 7, no. 3, pp. 140–158, 2018
50. Foroughi, F., & Luksch, P. “Data Science Methodology for Cybersecurity Projects”, arXiv preprint arXiv:1803.04219., 2018
51. Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. ,”Cyber-Dependent Crime Victimization: The Same Risk for Everyone? Cyberpsychology, Behavior, and Social Networking, 21(2), 84–90, 2018
52. Hernandez-Suarez, At al.., Social sentiment sensor in Twitter for predicting cyber-attacks using ℓ1 regularization. Sensors, 18(5), 1380, 2018
53. Verizon Enterprise.. Data Breach Investigations Report, 2018
54. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. “On the effectiveness of machine and deep learning for cyber security”, 10th International Conference on Cyber Conflict (CyCon) pp. 371-390. IEEE, 2018
55. Healthcare Information and Management Systems Society.,HIMSS Cybersecurity Survey, 2018
56. Bhardwaj, P., Gautam, S., & Pahwa, P. “A novel approach to analyze the sentiments of tweets related to TripAdvisor”, Journal of Information and Optimization Sciences, 39(2), 591-605, 2018
57. Sarwar Sayeed, and Hector Marco-Gisbert. “Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack.” Applied Sciences , no. 9, p. 1788, 2019
58. Catherine D. at. al.“Handbook on Crime and Deviance. Handbooks of Sociology and Social Research, 2019
59. Ying-Yu Lin. “China Cyber Warfare and Cyber Force.” Tamkang Journal of InternationalmAffairs , vol. 22, no. 3, pp. 119–161, 2019
60. Kranenbarg, M. W., Holt, T. J. & van Gelder J.L. , “Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap, Deviant Behavior,40:1, pp. 40-55, 2019
61. Grace Odette Boussi,” A Proposed Framework for Controlling Cyber- Crime”, 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),IEEE, India, 2020
62. Priyanka Datta at. al.,” A Technical Review Report on Cyber Crimes in India”, International Conference on Emerging Smart Computing and Informatics (ESCI),IEEE, India, 2020
63. Altair, "Cyber security attacks on smart cities and associated mobile technologies", Procedia Computer Science, vol. 109, pp. 1086-1091, 2017
64. Nikhat Akhtar, Bedine Kerim, Yusuf Perwej, Anurag Tiwari, Sheeba Praveen,“A Comprehensive Overview of Privacy and Data Security for Cloud Storage”, International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Volume 08, Issue 5, Pages 113-152, September- October 2021, DOI: 10.32628/IJSRSET21852
65. C. S. Kruse, B. Frederick, T. Jacobson and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends", Tech. and Health Care, vol. 25, no. 1, pp. 1-10, 2017
66. L. Y. Chang and N. Coppel, "Building cyber security awareness in a developing country: lessons from Myanmar", Computers & Security, vol. 97, pp. 101959, 2020
67. Yusuf Perwej, Firoj Parwej, Mumdouh Mirghani Mohamed Hassan, Nikhat Akhtar, “The Internet-of-Things (IoT) Security: A Technological Perspective and Review” , International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSRCSEIT), Volume 5, Issue 1, Pages 462-482, February 2019, DOI: 10.32628/CSEIT195193
68. L. J. Janczewski and A. M. Colarik, Cyber warfare and cyber terrorism, Hershey:Information Science Reference, 2008

69. N. Choucri and D. Goldsmith, "Lost in cyberspace: harnessing the Internet international relations and global security", Bulletin of the Atomic Scientists, vol. 68, no. 2, pp. 70-77
70. Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "A Close-Up View About Spark in Big Data Jurisdiction", International Journal of Engineering Research and Application (IJERA), Volume 8, Issue 1, (Part -I1), Pages 26-41, January 2018, DOI: 10.9790/9622-0801022641
71. Yusuf Perwej, Md. Husamuddin, Majzoob K.Omer, Bedine Kerim, "A Comprehend the Apache Flink in Big Data Environments" , IOSR Journal of Computer Engineering (IOSR-JCE), USA, Volume 20, Issue 1, Ver. IV, Pages 48-58, 2018, DOI: 10.9790/0661-2001044858
72. C.M. Williams, R. Chaturvedi and K. Chakravarthy, "Cybersecurity Risks in a Pandemic", Journal of Medical Internet Res., vol. 22, no. 9, pp. 23692, 2020
73. Asif Perwej "The Impact of Pandemic Covid-19 On The Indian Banking System", International Journal Of Recent Scientific Research (IJRSR), ISSN 0976 –3031, Volume. 11, Issue 10 (B), Pages 39873-39883, 28th October, 2020
74. S. Wu, Y. Chen, M. Li, X. Luo, Z. Liu and L. Liu, "Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools", EEE/ACM Transactions on Networking, vol. 28, no. 2, pp. 874-887, 2020
75. S. Aftergood, "Cybersecurity. The Cold war online", Nature, vol. 547, no. 7661, pp. 30, 2017
76. Yusuf Perwej, Shaikh Abdul Hannan, Firoj Parwej, Nikhat Akhtar , "A Posteriori Perusal of Mobile Computing", International Journal of Computer Applications Technology and Research (IJCATR), , Volume 3, Issue 9, Pages 569 - 578, September 2014, DOI: 10.7753/IJCATR0309.1008
77. M. Schwenk Jensen, J. Gruschka and N. Iacono, "On technical security issues in Cloud", IEEE International Conference on Cloud Computing, pp. 109-16, 2009
78. Yuya Jeremy Ong, Mu Qiao, Ramani Routray and Roger Raphael, "Context-Aware Data Loss Prevention for Cloud Storage Services", 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), 2017
79. X. Jin, W. Sun, Y. Liang, J. Guo and Z. Xie, "Design and implementation of intranet safety monitoring platform for Power secondary system", Automation of Electric Power System, pp. 99-104, Aug. 2011
80. Yusuf Perwej, Kashiful Haq, Firoj Parwej, M. M. Mohamed Hassan ," The Internet of Things (IoT) and its Application Domains", International Journal of Computer Applications (IJCA) ,USA , ISSN 0975 – 8887, Volume 182, No.49, Pages 36- 49, April 2019,DOI: 10.5120/ijca2019918763
81. Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "An Empirical Analysis of Web of Things (WoT)", International Journal of Advanced Research in Computer Science (IJARCS), Volume 10, No. 3, Pages 32-40, 2019, DOI: 10.26483/ijarcs.v10i3.6434
82. Nikhat Akhtar, Yusuf Perwej, "The Internet of Nano Things (IoNT) Existing State and Future Prospects", for published in the GSC Advanced Research and Reviews (GSCARR), e-ISSN: 2582-4597, Volume 5, Issue 2, Pages 131-150, November 2020, DOI: 10.30574/gscarr.2020.5.2.0110
83. Nikhat Akhtar, Saima Rahman, Halima Sadia, Yusuf Perwej, "A Holistic Analysis of Medical Internet of Things (MIoT)", Journal of Information and Computational Science (JOICS), ISSN: 1548 - 7741, Volume 11, Issue 4, Pages 209 - 222, April 2021, DOI: 10.12733/JICS.2021/V11I3.535569.31023
84. S. Kowtha, L. A. Nolan and R. A. Daley, "Cyber security operations center characterization model and analysis", Proc. IEEE Conf. Technol. Homeland Secur. (HST), pp. 470-475, Nov. 2012
85. Lital Asher-Dothan, Seven essential elements of modern endpoin t security, March 2018, [online] Available: https://www.cybereason.com/blog/7-elements-of-modern-endpoint-security
86. Yusuf Perwej, "The Ambient Scrutinize of Scheduling Algorithms in Big Data Territory", International Journal of Advanced Research (IJAR), ISSN 2320-5407, Volume 6,Issue 3, Pages 241-258, March 2018, DOI: 10.21474/IJAR01/6672
87. F. Pasqualetti, F. Dorfler and F. Bullo, "Attack detection and identification in cyber-physical systems", IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013
88. Yusuf Perwej, Bedine Kerim, Mohmed Sirelkhtem Adrees, Osama E. Sheta, "An Empirical Exploration of the Yarn in Big Data", International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868, Foundation of Computer Science FCS, New York, USA, Volume 12, No.9, Pages 19-29, December 2017, DOI: 10.5120/ijais2017451730

89. Yusuf Perwej, Nikhat Akhtar, Firoj Parwej, “A Technological Perspective of Blockchain Security”, International Journal of Recent Scientific Research (IJRSR), ISSN: 0976-3031, Volume 9, Issue 11, (A), Pages 29472 – 29493, November 2018, DOI: 10.24327/ijrsr.2018.0911.2869
90. Asif Perwej, Dr. Kashiful Haq, Dr. Yusuf Perwej, “Blockchain and its Influence on Market”, International Journal of Computer Science Trends and Technology (IJCST), ISSN 2347 – 8578, Volume 7, Issue 5, Pages 82- 91, Sep – Oct 2019, DOI: 10.33144/23478578/IJCST-V7I5P10
91. Yusuf Perwej, “A Pervasive Review of Blockchain Technology and Its Potential Applications”, Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA, Volume 5, No. 4, Pages 30 - 43, October, 2018
92. D. Grpoup, Cyber Crime: New Challenge to Mankind Society Introduction to the Nature of Cyber Crime and its Investigation Process, January 2011
93. K. K. R. Choo, "The cyber threat landscape", Challenges and future research directions. Computers & Security, vol. 30, no. 8, pp. 719-731, 2011
94. Mahmoud Khonji, Youssef Iraqi and Andrew Jones, "Literature Review on Phishing Detection", Institute of Electrical and Electronics Engineers Communication Surveys and Tutorials, vol. 15, no. 04, 2013
95. Lee, K. Kim, H. Lee and M. Jun, "A study on realtime detecting smishing on cloud computing environments" in Advanced Multimedia and Ubiquitous Engineering, Berlin, Heidelberg:Springer, pp. 495-501, 2016
96. N. Thamsirarak, T. Seethongchuen and P. Ratanaworabhan, "A Case for Malware that Make Antivirus Irrelevant" in , Thailand:IEEE, 2015
97. Ali, "Ransomware: A research and a personal case study of dealing with this nasty malware", Issues in Informing Science and Information Technology Education, vol. 14, pp. 87-99, 2017
98. M. Tehranipoor and R. Koushanfar, "A survey of hardware Trojan taxonomy and detection", IEEE design & test of computers, vol. 27, no. 1, 2010
99. M. Choraś, R. Kozik, D. Puchalski , W. Hołubowicz, "Correlation approach for sql injection attacks detection", Inte. Joint Confe. CISIS’12-ICEUTE´ 12-SOCO´ Special Sessions, pp. 177-185, 2013
100. Y. Shin, L. Williams and T. Xie, "Sqlunitgen: Sql injection testing using static and dynamic analysis", The 17th IEEE International Symposium on Software Reliability Engineering (ISSRE 2006), 2006
101. S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046-2069
102. Bin Xiao, Wei chen, Yanxiang He, Edwin Hsing and Mean Sha, "An Active Detecting Method against SYN Flooding attack", proceedings of the 11th International conference on Parallel and Distributed Systems ICPADS2005, pp. 709-715, July 2005
103. Raymond, D.R. and S.F. Midkiff, Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. Pervasive Computing, IEEE, 2008. 7(1): p. 74-81
104. Abdalla Wasef Marashdih and Zarul Fitri Zaaba, "Cross Site Scripting: Detection Approaches in Web Application", International Journel of Advanced Computer Science and appl., vol. 7, no. 10, 2016
105. Huajie Xu, Xiaoming Hu and Dongdong Zhang, "A XSS defensive scheme based on behavior certification", Applied Mechanics and Materials, vol. 241–244, pp. 2365-2369, 2013
106. M. Conti, N. Dragoni and V. Lesyk, "A survey of man in the middle attacks", IEEE Communications Surveys & Tut., vol. 18, no. 3, pp. 2027-2051, 2016
107. K. Zeng, D. Wu, A. Chan and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks", INFOCOM 2010 Proceedings IEEE, pp. 1-9, 2010
108. Prof. Kameswara Rao Poranki, Dr. Yusuf Perwej, Dr. Asif Perwej, ”The Level of Customer Satisfaction related to GSM in India “, published by The TIJ's Research Journal of Science & IT Management RJSITM, International Journal's-Research Journal of Science & IT Management of Singapore, Singapore, Volume 04,Number: 03, Pages 29-36 , 2015
109. Yusuf Perwej , Firoj Parwej, “A Neuroplasticity (Brain Plasticity) Approach to Use in Artificial Neural Network”, International Journal of Scientific & Engineering Research (IJSER), France , ISSN 2229 – 5518, Volume 3, Issue 6, Pages 1- 9, June 2012, DOI: 10.13140/2.1.1693.2808

110. X. Li, H. Wang, H.-N. Dai, Y. Wang and Q. Zhao, "An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things", Mobile Information Systems, vol. 2016, 2016
111. Yusuf Perwej, Majzoob K. Omer, Osama E. Sheta, Hani Ali M. Harb, Mohmed S. Adrees, "The Future of Internet of Things (IoT) and Its Empowering Technology" , International Journal of Engineering Science and Computing (IJESC), Volume 9, Issue No.3, Pages 20192– 20203, March 2019
112. Adnan Amin at. Al. ," Classification of cyber-attacks based on rough set theory", First International Conference on Anti-Cybercrime (ICACC), IEEE, Saudi Arabia 2015
113. R. Sabillon, J. Cano, V. Cavaller and J. Serra, "Cybercrime and Cybercriminals: A Comprehensive Study", International Journal of Computer Networks and Comm. Security, vol. 4, no. 6, pp. 165-176, 2016
114. Al-Mushayt O., Haq Kashiful, Yusuf Perwej, "Electronic-Government in Saudi Arabia", a Positive Revolution in the Peninsula", International Transactions in Applied Sciences, India, ISSN-0974-7273, Volume 1, Number 1, Pages 87-98, July-December 2009
115. Raymond Wu and Masayuki Hisada, "Static and Dynamic Analysis for Web Security in industry Applications", International Journal of Electronic Security and Digital forensics Inder Science, vol. 3, no. 2, pp. 138-150, 2010
116. Zhu Huafei, "Towards a Theory of Cyber Security Assessment in the Universal Composable Framework", Information Science and Engineering (ISISE) 2009 Second International Symposium on, pp. 203-207, 26–28 Dec. 2009
117. T. Chmielecki, P. Cholda, P. Pacyna, P. Potrawka, N. Rapacz, R. Stankiewicz, et al., "Enterprise-oriented cybersecurity management", Computer Science and Information Systems (FedCSIS) 2014 Federated Conference on, pp. 863-870, 7–10 Sept. 2014
118. Bela Genge, Piroska Haller and Istvan Kiss, "A framework for designing resilient distributed intrusion detection systems for critical infrastructures", International Journal of Critical Infrastructure Protection, vol. 15, pp. 3-11, 2016,
119. F. Setiadi, P. H. Putra, Y. G. Sucahyo and Z. A. Hasibuan, "Determining components of national cyber security framework using Grounded Theory", Second Int. Conf. Informatics Comput., pp. 1-6, 2017
120. Y. Nugraha, S. Member and I. A. N. Brown, "An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements", IEEE Transactions On Emerging Topics in Computing, vol. 4, no. 1, pp. 47-59, 2016
121. Z. A. Soomro, M. H. Shah and J. Ahmed, "Information security management needs more holistie approach: A literature review", International Journal of Information Management, vol. 36, no. 2, pp. 215-225, 2016
122. Z. Trabelsi, K. Hayawi, A. Braiki and S. Mathew, Network Attacks and Defenses: A Hands-on Approach, Boca Raton, Florida:CRC Press, 2013
123. Brian Komar, Ronald Beekelaar and Joern Wettern, Firewalls for Dummies, pp. 10, August 2001
124. Imran Ijaz, "Design and Implementation of PKI (For Multi Domain Environment)," Inter. Journal of Com. Theory and Eng. vol. 4, no. 4, pp. 505-509, 2012
125. C. Weissman, "Security penetration testing guideline" in , US:Handbook for the Computer Security Certification of Trusted Systems, Center for Secure Information Technology, Naval Research Laboratory (NRL), pp. 1-66, 1993
126. Roumen Trifonov, Georgi Manolov, Radoslav Yoshinov and Galya Pavlova, "A survey of artificial intelligence for enhancing the information security", International Journal of Development Research, vol. 7, no. 11, pp. 16866-16872, 2017
127. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues", Internet Technology Letter (Wiley), pp. 1-6, 2020
128. Yusuf Perwej, Majzoob K. Omer, Osama E. Sheta, Hani Ali M. Harb, Mohmed S. Adrees, "The Future of Internet of Things (IoT) and Its Empowering Technology", International Journal of Engineering Science and Computing (IJESC), ISSN : 2321- 3361, Volume 9, Issue No.3, Pages 20192– 20203, 2019
129. R. Doshi, N. Apthorpe and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices", 2018 IEEE Security and Privacy Workshops (SPW), pp. 29-35, 2018

130. N. Scaife, P. Traynor K. Butler, "Making sense of the ransomware mess planning a sensible path forward)", IEEE Potentials, vol. 36, no. 6, pp. 28-31, 2017
131. Bag, S. Ruj and K. Sakurai, "Bitcoin block withholding attack: Analysis and mitigation", IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1967-1978, 2017
132. Yusuf Perwej, Ashish Chaturvedi, "Machine Recognition of Hand Written Characters using Neural Networks", International Journal of Computer Applications (IJCA), USA, ISSN 0975 – 8887, Volume 14, No. 2, Pages 6- 9, January 2011, DOI: 10.5120/1819-2380
133. Biometric Systems: Technology Design and Performance Evaluation, Springer Verlag, 2005
134. Tudzarov , T. Janevski, "Design of 5G Mobile Architecture" International Journal of Communication Networks and Information Security, Vol. 3, No. 2, August 2011
135. Yusuf Perwej, Kashiful Haq, Uruj Jaleel, Sharad Saxena, "Some Drastic Improvements Found in the Analysis of Routing Protocol for the Bluetooth Technology Using Scatternet", Special Issue on The International Conference on Computing, Communications and Information Technology Applications (CCITA-2010), Ubiquitous Computing and Communication Journal (UBICC), Seoul, South Korea, ISSN Online: 1992-8424, Volume CCITA-2010, Number 5 , Pages 86-95, 2010
136. Nikhat Akhtar, Devendera Agarwal, "A Literature Review of Empirical Studies of Recommendation Systems", International Journal of Applied Information Systems (IJAIS), ISSN: 2249-0868, Foundation of Computer Science FCS, New York, USA, Volume 10, No.2, Pages 6 – 14, December 2015, DOI: 10.5120/ijais2015451467
137. Nikhat Akhtar, Devendera Agarwal, "An Influential Recommendation System Usage for General Users", Communications on Applied Electronics (CAE), ISSN : 2394-4714, Foundation of Computer Science, New York, USA, Vol. 5, No.7, Pages 5 – 9, 2016, DOI: 10.5120/cae2016652315
138. Nikhat Akhtar, Devendra Agarwal, "A Survey of Imperfection of Existing Recommender System for Academic Fraternity", IOSR Journal of Computer Engineering (IOSR-JCE), p-ISSN: 2278-8727 , Volume 20 , Issue 3, Pages 08-15, Ver.III(May – June. 2018), DOI: 10.9790/0661-2003030815
139. Qiang Tang and Jun Wang. "Privacy preserving context-aware recommender systems: Analysis and new solutions", In G. Pernul, P. Y. A. Ryan, and E. R. Weippl, editors, Computer Security ESORICS 2015, volume 9327, pages 101–119. Springer, 2015
140. Nikhat Akhtar, "A Model Based Research Material Recommendation System For Individual Users", Transactions on Machine Learning and Artificial Intelligence (TMLAI), Society for Science and Education, United Kingdom (UK), ISSN 2054-7390, Vol. 5, Issue 2, Pages 1 - 8, March 2017, DOI: 10.14738/tmlai.52.2842
141. Arjan Jeckmans, Andreas Peter, and Pieter Hartel. "Efficient privacy-enhanced familiarity based recommender system", In Computer Security–ESORICS 2013, pages 400–417. Springer, 2013
142. Nikhat Akhtar, Devendera Agarwal, "An Efficient Mining for Recommendation System for Academics", International Journal of Recent Technology and Engineering (IJRTE), ISSN 2277-3878 (online), SCOPUS, Volume-8, Issue-5, Pages 1619-1626, 2020, DOI: 10.35940/ijrte.E5924.018520
143. Nikhat Akhtar, "Perceptual Evolution for Software Project Cost Estimation using Ant Colony System", International Journal of Computer Applications (IJCA) USA, Volume 81, No.14, Pages 23 – 30, 2013, DOI: 10.5120/14185-2385
144. ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends, 2019, [online] Available: https://doi.org/10.2824/