A Systematic Literature Review on the Cyber Security

Dr.Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, Anurag Kumar Jaiswal

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.

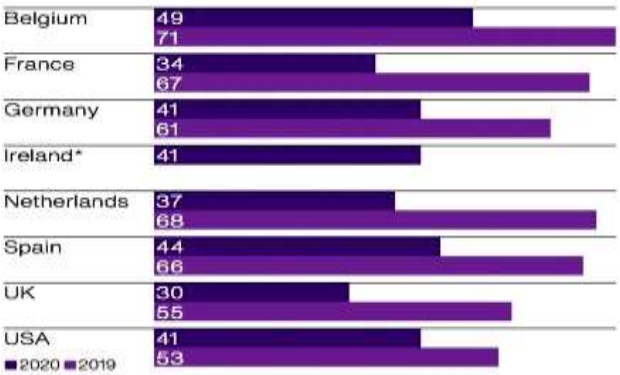

Figure 1: The Cyber Event in 2019 to 2020

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.

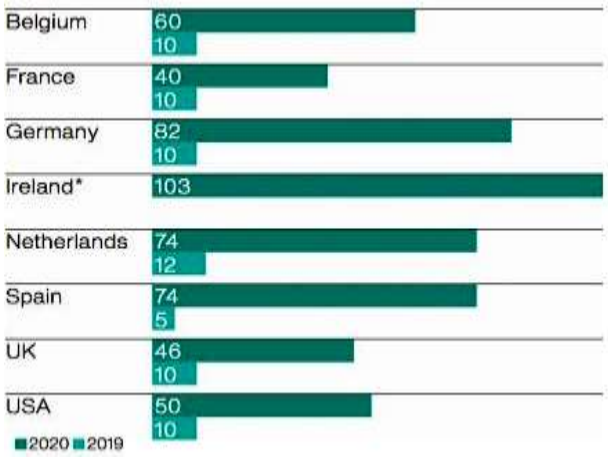

Figure 2: The Incidents and Breaches in 2019 to 2020

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.

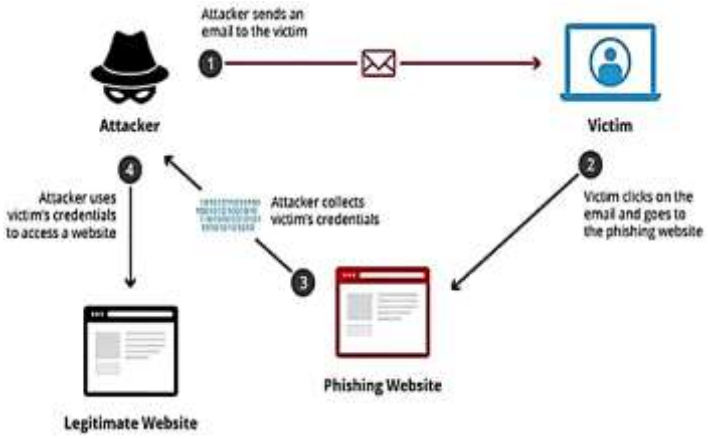

Figure 3: The Phishing Attack

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.

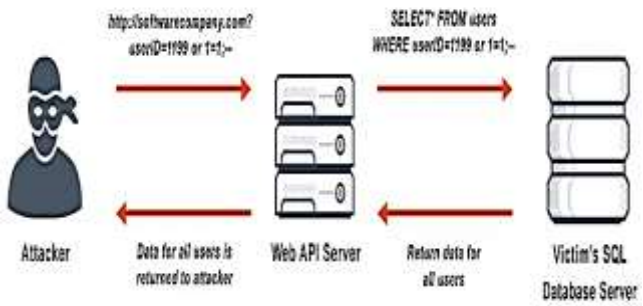

Figure 5: The SQL Injection

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.

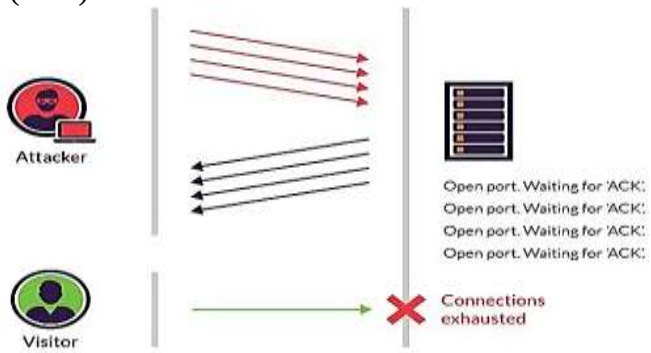

Figure 6: TCP SYN Flood Attack

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.

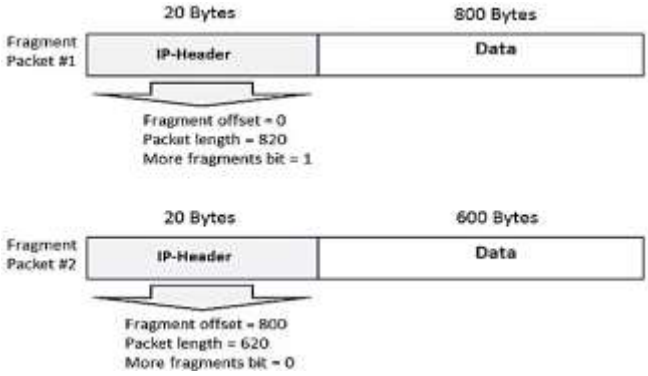

Figure 7: The Teardrop Attack

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].

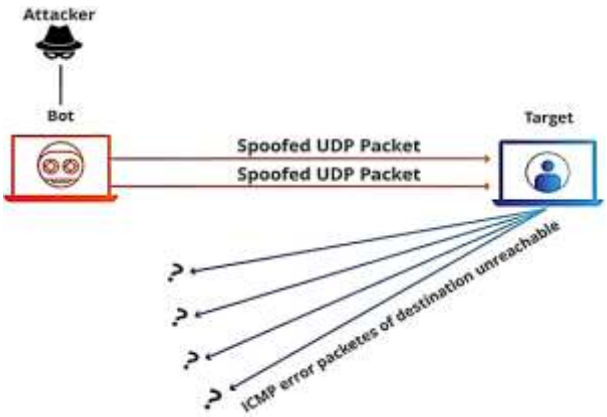

Figure 8: User Datagram Protocol (UDP) Flood

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.

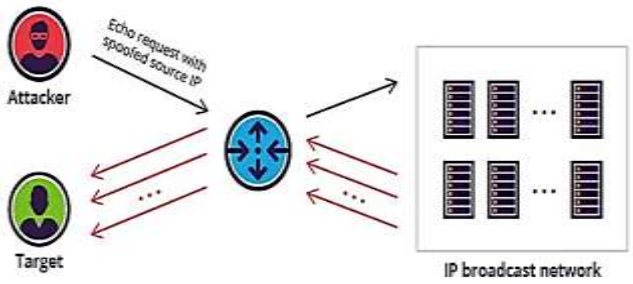

Figure 9: The Smurf Attack

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.

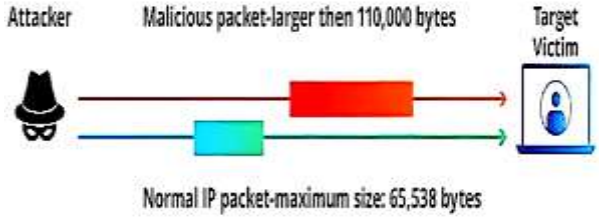

Figure 10: Ping of Death Attack

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.

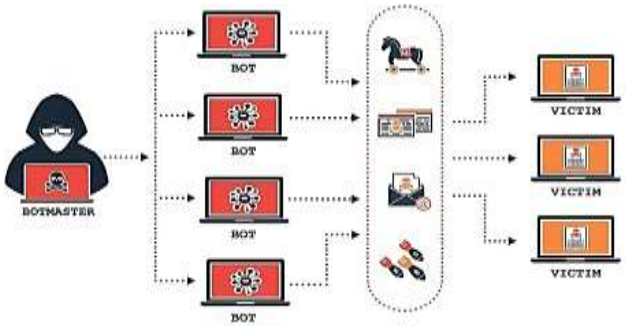

Figure 11: Botnets Attack

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.

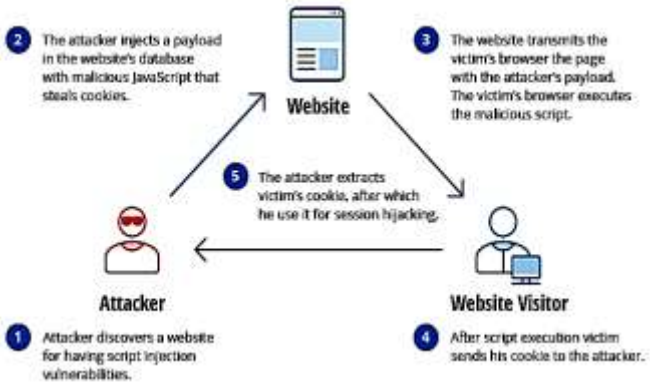

Figure 12: The Cross-Site Scripting (XSS)

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.

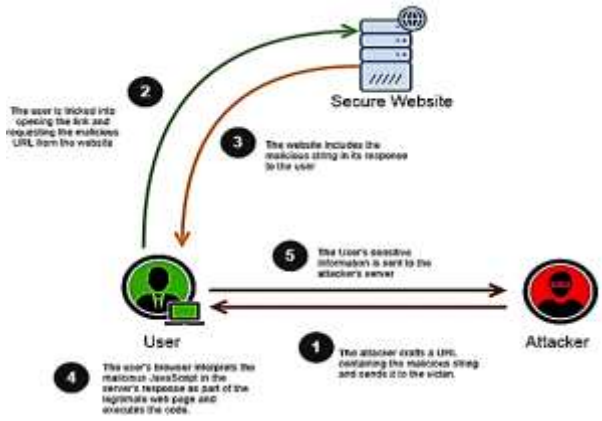

Figure 13: Reflected XSS or Non-Persistent XSS Attacks

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.

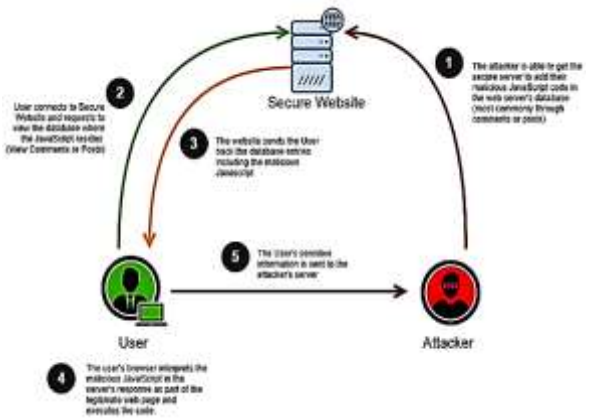

Figure 14: Persistent XSS Attacks (also known as Type 2 XSS)

7.5.3 DOM Based XSS Attack

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

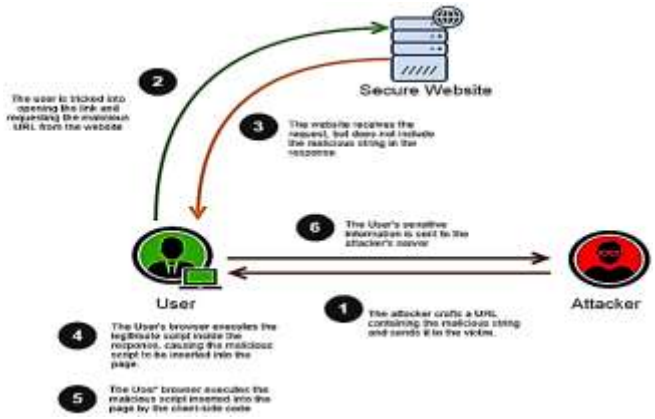

Figure 15: DOM Based XSS Attack

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.

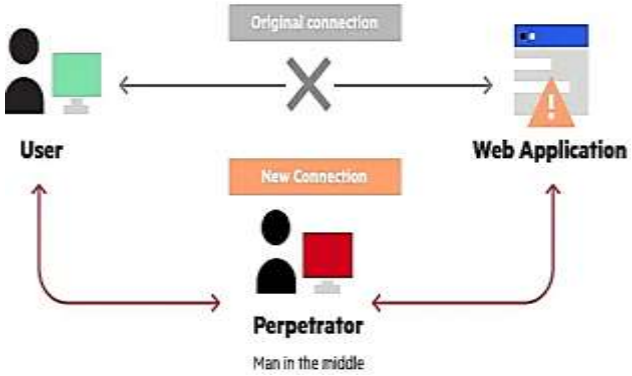

Figure 16: Man-in-the-Middle (MiTM) Attack

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.

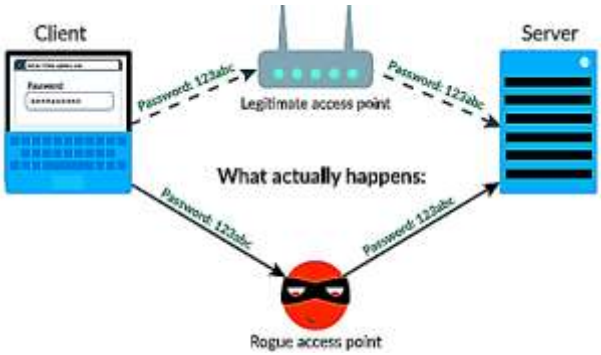

Figure 17: Rogue Access Point

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.

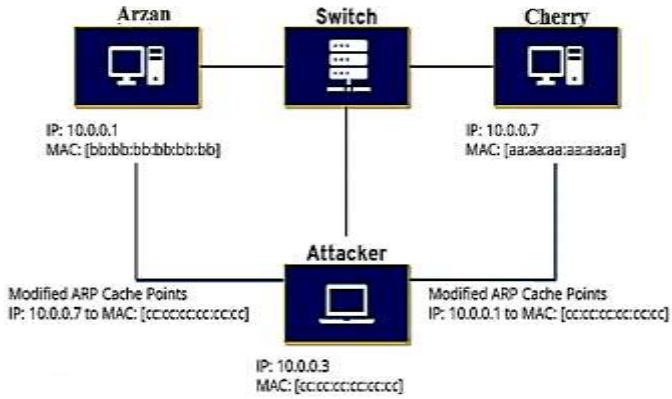

Figure 18: Address Resolution Protocol (ARP)

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.

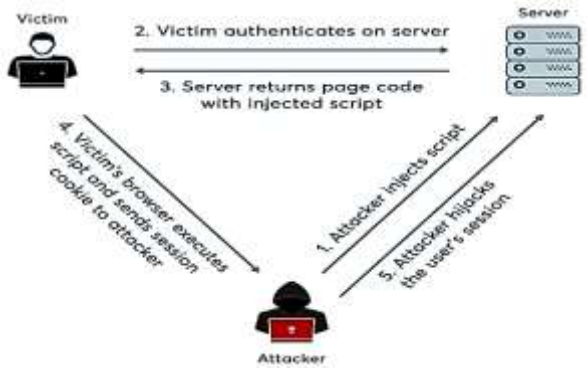

Figure 19: Session Hijacking

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.

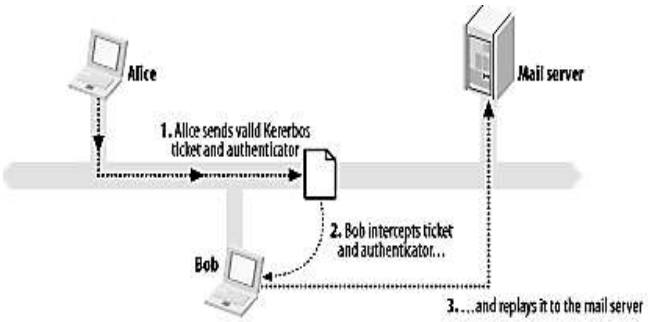

Figure 20: Replay Attack

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.

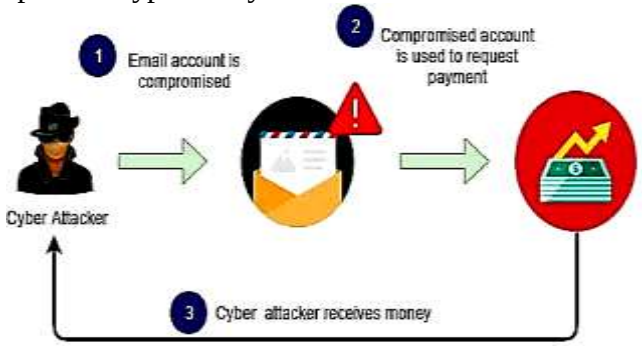

Figure 21: Business Email Compromise (BEC) Attack

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.

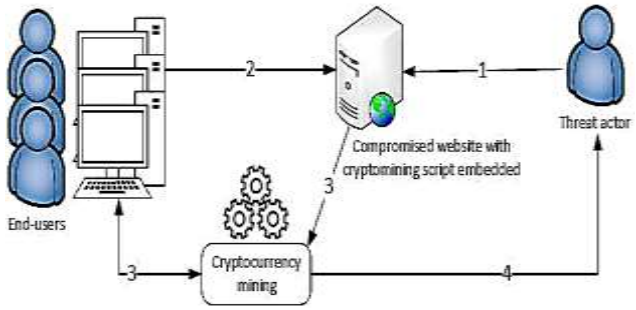

Figure 22: The Cryptojacking Attack

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.

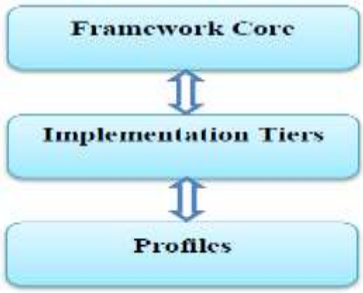

Figure 24: The Cyber Security Framework Components

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/

sensors

IMPACT FACTOR 3.4

Indexed in: PubMed

CITESCORE 7.3

Review

Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations

Saqib Saeed, Salha A. Altamimi, Norah A. Alkayyal, Ebtisam Alshehri and Dina A. Alabbad

Special Issue

Industry 5.0: How Intelligent Sensors and Its Applications Accelerate Customized Digital Transformation for Industry

Edited by

Prof. Dr. Jiann-Shing Shieh and Prof. Dr. Maysam Abbod

MDPI

https://doi.org/10.3390/s23156666

sensors

MDPI

Review

Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations

Saqib Saeed [1,*], Salha A. Altamimi [2], Norah A. Alkayyal [2], Ebtisam Alshehri [2] and Dina A. Alabbad [3]

[1] Saudi Aramco Cybersecurity Chair, Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
[2] Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; 2230500089@iau.edu.sa (N.A.A.)
[3] Saudi Aramco Cybersecurity Chair, Department of Computer Engineering, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
* Correspondence: sbsaed@iau.edu.sa

Abstract: This systematic literature review explores the digital transformation (DT) and cybersecurity implications for achieving business resilience. DT involves transitioning organizational processes to IT solutions, which can result in significant changes across various aspects of an organization. However, emerging technologies such as artificial intelligence, big data and analytics, blockchain, and cloud computing drive digital transformation worldwide while increasing cybersecurity risks for businesses undergoing this process. This literature survey article highlights the importance of comprehensive knowledge of cybersecurity threats during DT implementation to prevent interruptions due to malicious activities or unauthorized access by attackers aiming at sensitive information alteration, destruction, or extortion from users. Cybersecurity is essential to DT as it protects digital assets from cyber threats. We conducted a systematic literature review using the PRISMA methodology in this research. Our literature review found that DT has increased efficiency and productivity but poses new challenges related to cybersecurity risks, such as data breaches and cyber-attacks. We conclude by discussing future vulnerabilities associated with DT implementation and provide recommendations on how organizations can mitigate these risks through effective cybersecurity measures. The paper recommends a staged cybersecurity readiness framework for business organizations to be prepared to pursue digital transformation.

Keywords: digital transformation; cybersecurity; information technology

Citation: Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors* **2023**, *23*, 6666. https://doi.org/10.3390/s23156666

Academic Editors: Maysam Abbod and Jiann-Shing Shieh

Received: 2 July 2023
Revised: 17 July 2023
Accepted: 19 July 2023
Published: 25 July 2023

1. Introduction

Digital transformation refers to adopting digital solutions in the business processes of organizations, which can result in significant changes in their business operations. Such modification can impact various aspects of an organization, for instance, user experience, business processes, target markets, customers, customer relationships, and even diverse cultural implications. The accelerated technology adoption by business organizations during the COVID-19 pandemic also resulted in many abrupt challenges [1]. Emerging technologies such as artificial intelligence, big data and analytics, blockchain, cloud computing, the Internet of Things, and the industrial Internet of Things are critical enablers for digital transformation. Due to extensive benefits, businesses are accelerating the digital transformation drive. Still, cybersecurity has grown into a significant challenge for companies, and to gain business continuity, organizations need to secure their digital transformation tools and artifacts. Therefore, it is crucial for organizations undergoing DT adoption to prioritize cybersecurity measures and ensure that their systems are secure from potential threats [2,3].

Cybercriminals may take advantage of vulnerabilities in digital technologies; therefore, organizations must ensure that technological solutions are secure from digital attacks. Cybersecurity can be achieved by implementing encryption, authentication, and access control measures to protect data and networks from unauthorized access or malicious activities. Additionally, organizations should consider investing in cyber insurance policies that can provide financial protection against losses due to a successful attack on their systems. Another critical issue is to raise awareness among employees regarding cybersecurity attacks, as higher awareness results in dependable information security behavior [4,5]. Cyber-attacks have drastically escalated; therefore, business organizations must understand cybersecurity threats and how best to mitigate them comprehensively. These attacks usually aim to assess, change, or destroy sensitive information; extort monetary benefits from users; or interrupt normal business processes. Cybersecurity involves techniques to protect computers and networks from unauthorized access and malicious activities such as data theft and destruction.

Cybersecurity costs and cybercrimes are exhibiting an increasing trend globally [6]. Haislip et al. [7] highlighted that the economic cost of cybersecurity breaches is underestimated, as it is not only limited to the targeted form; they spill over to the industry concerned through negative returns and higher insurance costs. Garg [8] has highlighted seven critical benefits of investing in cybersecurity to motivate organizations in making cybersecurity investments. These include protecting intellectual property, better meeting customer requirements, minimizing customer turnover, branding secure products, joining secure vendors in an integrated network, company reputation, and minimizing collateral damage in the industry. Lee [9] has presented a risk management framework focusing on continuously improving cybersecurity practices and cost–benefit analysis for cybersecurity investments. Many organizations use the National Institute for Standards and Technology (NIST) Cybersecurity Framework for cybersecurity risk management; however, the standard lacks a cost–benefit analysis. The Gordon–Loeb model has been proposed to identify which tier of NIST is more effective for a particular organization in terms of cost–benefit study [10]. Krutilla et al. [11] enhanced the Gordon–Loeb model by considering the depreciation cost of cybersecurity assets, which can impact the cost–benefit analysis of cybersecurity initiatives. Simon and Omar [12] highlighted that companies may be affected by cybersecurity risks via cybersecurity attacks on their supply chain partners, so they maintain that cybersecurity investments need to consider both coordinated and uncoordinated attacks. Uddin et al. [13] highlighted that cybersecurity weaknesses impact organizational growth and performance, and, especially for the banking sector, operational risks have increased due to cybersecurity threats. Curti et al. [14] highlighted that cybersecurity attacks are on the rise in the governmental sector, and to mitigate these threats, governments are increasing governmental operating costs and overall financing costs.

In this paper, we have conducted a systematic literature review that documents how digital transformation has changed the business sector and the implications of cybersecurity for digital transformation. We have investigated the papers published during 2019–2023 using PRISMA guidelines for conducting a literature review. We have proposed a cybersecurity readiness framework for business organizations pursuing digital transformation. The findings of this paper will help business organizations, practitioners, and researchers to grasp the state of the art in this domain and will form the basis for further research.

This paper is organized as follows: Section 2 outlines the methodology adopted to conduct the survey, and Section 3 discusses the literature in detail. Section 4 provides a discussion, and a conclusion is offered in Section 5.

2. Materials and Methods

In this section, we explain the methodology. We did a systematic literature review using the PRISMA guidelines [15]. As shown in Figure 1, we used the Google Scholar database. Primary studies were extracted using specific keywords in search criteria. Keywords were chosen to facilitate the generation of research articles relevant to our topic. The

search terms used were (business transformation) AND (security), (digital transformation) AND (cybersecurity), (digital transformation) AND (cyber security), (digital transformation) AND (protection), and (digitization) AND (security). To refine our search results, we used the following inclusion criteria:

- The paper should be relevant to digital business and cybersecurity.
- The paper is published between 2019–2023.

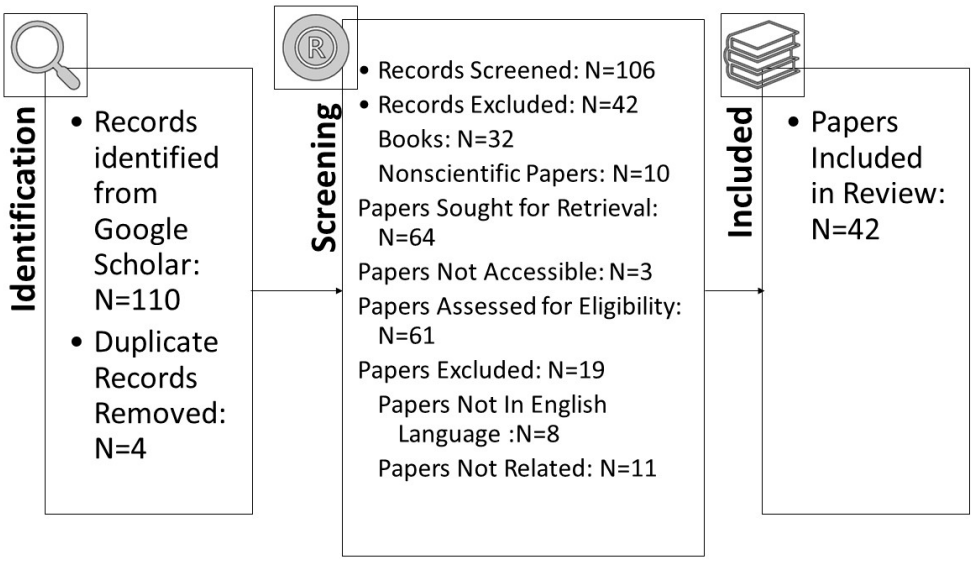

Figure 1. Prisma diagram for our systematic literature review.

Additionally, the following exclusion criteria were applied to search results:

- The papers are not written in the English language.
- The paper is not related to cybersecurity and digital transformation.
- The paper is a review paper.

All Google Scholar results were checked for compliance with these criteria. The process of identifying the extracted studies went through the quality assessment stage, starting with a quick scan of the title and the language of the paper (English or not). Secondly, it was also ensured that these papers are related to and relevant to our research. Figure 1 shows the number of final papers that were selected after going through these stages.

As highlighted in Figure 1, digital transformation and cybersecurity are widely researched, and our final analysis included forty-two papers. Figure 2 highlights the year-wise publication history.

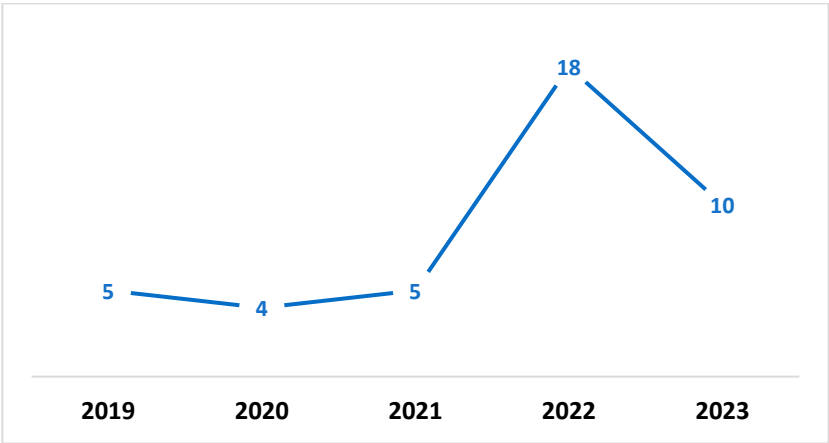

Figure 2. Year-wise publication history.

3. Results

In this section, we highlight the findings of downloaded papers.

3.1. Financial Sector

The financial sector is a critical component of an economy, and there have been many empirical studies in different geographical contexts. For example, Al-Alawi and Al-Bassam conducted empirical research in Bahrain and found that financial institutions are exposed to online identity theft, computer system damage, and hacking attempts resulting in operational disturbances [16]. Similarly, Hasan and Al-Ramadan [17] conducted an empirical study with bank customers in Iraq and found that although banks adopt significant security measures, some customers are still skeptical about online banking. In another study, Joveda et al. [18] investigated the banking sector in Bangladesh. They highlighted developing a cybersecurity system for identifying money laundering transactions that negatively impact economic development. There is a vast potential in modern technologies to support the financial sector. Almudaires and Almaiah [19] outlined major threats to credit card companies and associated solutions for credit card companies to improve their cybersecurity implementation. Smith and Dhillon [20] highlighted that blockchain is a crucial technology to minimize security threats in financial transactions; however, there is a need for rigorous analysis of blockchain implementation in the financial sector. Similarly, Kuzmenko et al. [21] used machine learning models to analyze large volumes of financial data to identify potential threats at an early stage.

Rodrigues et al. [22] developed a decision-support model for incorporating artificial intelligence (AI), digital transformation, and cybersecurity into the banking sector while ensuring data security is not compromised. The authors found that traditional banks are under pressure from their stakeholders to adapt to new technologies, and they also need to ensure that any potential data breaches or other security issues do not compromise their reputation. The authors used cognitive mapping and the decision-making trial and evaluation laboratory method to address this complex issue with an expert panel in group sessions. This resulted in a realistic framework for making decisions regarding AI implementation in the banking industry while ensuring data security is not compromised. The study developed a multi-stakeholder cognition-driven framework using cognitive mapping combined with DEMATEL methodology. This approach allowed them to identify critical factors affecting AI adoption within banks, such as customer trust toward technology-based services offered by banks; regulatory compliance requirements; and availability of a skilled workforce, which were then ranked based on their relative importance using DEMATEL analysis.

Similarly, Fedorov et al. [23] highlighted how cognitive technologies could ensure data security when using biometric identification technology in remote banking transactions. The article discussed how digital transformation and biometric identification would impact financial services in Russia. It emphasized that advanced security measures are necessary for protecting sensitive customer data during these transactions. The proposed solution is through cognitive technologies focused on human intellectual abilities as one direction for ensuring information security within this context.

Another research study by Patil and Bharath [24] investigated technological advancements in the financial sector. The study's findings showed that Fintech has improved businesses, and investors have more confidence in the technology. They also presented new technologies adopted by Fintech and their associated issues. The effect of financial technology was positive on the factors of trust and business authorization. Traditional finance has noticed the most important critical issues, such as the risks of fraud and low performance, and differences and limitations have been encountered. The research was conducted on a limited sample of approximately 160.

Moreover, Rãƒdulescu et al. [25] explained the risks associated with digitalization regarding economic development and ensuring social and information security. They highlighted that digitalization significantly impacts economic growth, social inclusion, and

sustainable development. However, it also introduces new vulnerabilities that can lead to cyber-attacks and require smart controls to prevent them. The authors suggested that technology experts and other stakeholders should be involved in assessing these risks as they can grow and become more complex over time. Risk managers must develop a comprehensive strategy that includes mitigation and risk transfer solutions, prioritizing which IT security options best mitigate the organization's risk.

Moreover, international cooperation is essential to combat cybercrime due to the evolving global crime and terrorist threats associated with digital transformation. Finally, it highlighted the growing importance of information technology in business development, human relations, and communication between people and governments. Digital risk management should therefore be a priority for all involved stakeholders.

3.2. Health Sector

Cybersecurity in the health sector deals with patient data privacy [26] and the security of medical devices [27–30]. A secure digital transformation drive can help improve health organizations' organizational governance [31–33]. Garcia-Perez et al. [34] discussed how the digital transformation of healthcare systems must be managed effectively from a cybersecurity perspective. This paper analyzed data from higher management in the UK during the COVID-19 pandemic. According to their findings, a balanced foundation that considers cybersecurity knowledge development, uncertainty management, and the sector's high systematic and organizational interdependence that has implications for research and management practices is essential for digital resilience and sustainability efforts in the health sector.

On the other hand, Paul et al. [35] discussed the use of digital technology in the healthcare sector and highlighted privacy and security issues related to these technologies. This study examined how digitization is transforming the healthcare sector, its impact on patient care, and opportunities for new business models with Industry 4.0 and business intelligence approaches. The rise in chronic diseases and the current pandemic have increased the need for person-centered care that encourages individuals to be involved in their health care. Digital solutions such as biosensors and software are being introduced to meet the growing need for on-demand healthcare services. Big data analytics have also significantly impacted healthcare organizations by providing access to decades of stored data, which serves as evidence-based medicine for better decision-making when treating patients while ensuring patient privacy remains protected. There are many ways to address security and privacy concerns related to digitalization in healthcare. It covers various solutions such as mutual authentication, key agreement, lightweight cryptography, blockchain-based solutions, etc., which can help ensure the secure handling of medical data. The authors also suggest developing management programs for medical equipment and investigating how patient engagement can impact privacy and security measures. Finally, they recommend further research on regulations regarding privacy and security in the healthcare sector and exploring the role of artificial intelligence (AI) and blockchain technology in improving healthcare outcomes while maintaining data safety. The adoption of cloud-based technology is also discussed as a potential solution for better patient data archiving and usage, lower storage costs, quicker innovation cycles, more straightforward collaboration, and increased telemedicine possibilities.

Nwaiwu and Mbelu [36] highlighted that the General Data Protection Regulation GDPR is essential for businesses and governments to comply with to track and monitor people's health, develop business models, and discover market opportunities. Statistics show that Europe has recorded 1.92 million confirmed COVID-19 cases and contact tracing with personal data is necessary to limit and contain the spread of the virus.

Maleh and Mellal [37] provided insights into how digital transformation and cybersecurity are impacted by COVID-19 proliferation. The author discussed how COVID-19 has accelerated digital transformation trends such as cloud computing, the IoTs explosion, and big data accumulation while also increasing cyber-attacks related to personal data

protection. The three main categories of challenges faced by cybersecurity departments during and after the pandemic are resilience against cyber attackers exploiting crises such as phishing or ransomware; recovery by ensuring secure pre-COVID-19 working methods upon return to the office; and adapting a technology roadmap for new realities while meeting business needs and customer expectations in digital transformation projects.

3.3. Governmental Sector

Digital transformation in governmental organizations is adopted all over the world, such as in Bahrain [38], the UK [39], and Saudi Arabia [40]; however, the adoption speed is not uniform. Al Shobaki et al. [41] investigated how digital transformation affects cybersecurity practices within the Ministry of Interior and National Security in Palestine. The researchers used a descriptive-analytical approach with a questionnaire as their primary research tool. They found a statistically significant correlation between all digital transformation dimensions and the ministry's cybersecurity practices. Additionally, certain organizational factors were found to have a powerful impact on these practices. For example, effective data exchange among different departments was identified as crucial for maintaining robust cybersecurity measures across all areas of operation. Overall results showed that there is indeed an impact of digital transformation on cybersecurity in this context, specifically in Gaza governorates, where it had an impact coefficient (0.897). Based on these findings, recommendations were made for improving electronic services offered by government agencies while also addressing gaps in worker performance related to technology use or knowledge gaps around best practices when dealing with sensitive information online. In conclusion: this paper provides valuable insights into how businesses can adapt their cybersecurity strategies when undergoing significant changes due to technological advancements such as those associated with "digital transformations", identifying key organizational factors impacting cybersecurity measures across organizations like ministries.

Another study by Al Najjar et al. [42] aimed to identify the reality of digital transformation in the Palestinian Ministry of Interior and National Security from the point of view of workers in computer and information technology units. The study used a comprehensive survey method, distributing questionnaires among workers, with 61 retrieved (representing an 87.1% response rate). Several dimensions related to digital transformation were measured through these questionnaires, including senior management support, strategic directions, technical infrastructure necessary for digital transformation, human resources coordination, data privacy and security, organizational structure, and job description. The results showed that most dimensions related to digital transformation are available within the ministry to a large extent. However, there is still room for improvement, such as providing more funds for electronic services development or innovation spending. Senior management support received a high approval degree along with strategic directions. At the same time, the technical infrastructure necessary for digital transformation also achieved a large approval degree, followed by human resources coordination, which scored lower than other dimensions but still had significant relative weight. In conclusion, this paper highlights how important it is for organizations seeking competitive advantage through improved efficiency or low-cost electronic service growth opportunities that exploit technological revolution possibilities offered at all levels, internally or externally, with various partner institutions, to consider investing in their efforts toward achieving successful digital transformation initiatives.

In another study, Fjord and Schmidt [43] examined the potential and challenges of using digital tools to simplify tax assessment and collection and enhance transparency. Practical experiences in Denmark showed that states had made progress in making tax processes more efficient but needed to take measures to ensure legality and transparency through cybersecurity.

Mijwil et al. [44] highlighted the importance of cybersecurity governance in digital transformation for public services provided by companies or institutions. The paper argued

that changes in cybersecurity must be considered as it constitutes a large part of priorities for nations and companies undergoing digital transformation. The conclusion summarizes the importance of establishing straightforward programs and strategies to develop trustworthy cybersecurity governance without hacking or tampering with data/information while undergoing digital transformation. It also provided recommendations on how businesses can ensure secure operations while improving efficiency and effectiveness when providing public services through electronic means.

Maglaras et al. [45] focused on protecting critical infrastructure vital for public safety and national security. They proposed a methodology to protect critical national infrastructure based on fileless attacks versus Advanced Persistent Threat (APT) group techniques used in such attacks. The study using this methodology aimed to quantify and score cyber-attacks from an offensive cybersecurity perspective.

3.4. Business Sector

Business organizations are very heterogeneous, resulting in the technological systems deployed in the organizations. Modern-day technologies like the Internet of Everything can help organizations improve cybersecurity [46]. Gonchar [47] developed theoretical and practical recommendations for improving economic security in the digital economy. The researchers conducted a study on the impact of digital technologies on entrepreneurial activity in Ukraine, finding that businesses are increasingly using information and communication technologies. Still, there were differences based on size and sector. The paper proposed a methodology for assessing a country's level of digital transformation within this context, which could help unify the study of conditions related to entrepreneurship and innovation. However, the paper found no significant relationship between the performance levels of the companies studied and their degree of digitization due to low staff involvement in these projects. The conclusion drawn from this research is that while businesses are adopting more technology across all sectors, including banking, as it increases flexibility and sales opportunities while decreasing costs incurred internally, such as time spent retraining employees who may not be familiarized yet or lack sufficient skills necessary at present given the rapid changes happening globally, there needs to be greater employee involvement in these projects if they are going to have an impact on business performance levels. Therefore, activities should focus not only on supporting enterprise resilience against risks associated with cybersecurity threats but also on promoting better employee qualifications required by more complex tasks resulting from business process automation through technology adoption across all sectors, including banking, where it increases flexibility and sales opportunities while decreasing costs incurred internally such as time spent retraining employees.

In another paper, Kuzior et al. [48] described the convergence of digitization processes across countries based on factors such as internet use, infrastructure metrics, and access to ICT. This study used the coefficient of variation to determine sigma convergence. It developed an econometric model that described the impact of national cybersecurity levels, ease of doing business, and anti-money laundering indices on digital development. This study aimed to understand the key determinants shaping risk in using financial instruments for money laundering and terrorist financing concerning global digitalization trends.

Moreover, another paper by Putri et al. [49] presented an example using the change from directory to digitization in Indonesia. Qualitative research approaches were used such as examining and describing events via interactions with others, mental images, and perceptions. These were drawn based on opinion from general public to encourage the use of digitization in public business and services and to follow trends observed from related parties as well as to encourage the government sector to develop services and evaluate the effectiveness of concepts using the six-ware cyber security framework (SWCSF) and Electronic-Based Government System (SPBE) that many government agencies have used.

Furthermore, another study by Shitta-Bey [50] showed the impact of digital transformation through cloud computing on business transformation depending on the requirements

factors chosen by organizations to publish or other models that differ from each other. The model and the scope of control were defined between cloud service providers and companion consumers. Therefore, there were security risks and broad threats associated with it, as well as an increase in the amount of confidential data in different cloud environments, and this is a significant concern for companies considering business transformation using a qualitative method to gain a thorough grasp of cloud computing service trends and practices. Among these threats to the cloud environment, whether from the inside or the outside, such as data penetration, loss, or leakage, dangers may also include weaknesses in the infrastructure or secure access, or they may be other destinations that are dead using the application programming interface. Eighteen threats were identified in this study of complete cloud migration. To deal with these security risks and take measures to reduce them and create strategies using appropriate equipment and recording procedures to monitor risks, suitable measures must be adopted during the migration or transition to the cloud. Protocols are included in the strategic plan that define the scope of migration and identify the basic parameters and indicators of performance.

E-commerce is an important application where digital transformation has transformed the business sector. Trung et al. [51] analyzed the applications of digital transformation, AI, IoTs, and blockchain in managing commerce secrets from a SWOT perspective. The authors used qualitative analysis, synthesis, inductive methods, and statistical data to conduct their research. They found that these technologies offer several benefits, such as increased efficiency, transparency, and security for businesses that adopt them. However, there are also challenges associated with their implementation, such as high costs and technical complexity, which need to be addressed by organizations before they can fully realize the potential benefits. In conclusion, the paper highlighted how mathematical solutions could be applied for industrial uses through a SWOT analysis of blockchain technology. It emphasized how businesses should consider adopting these technologies while being aware of their advantages and limitations to make informed decisions about implementing them into their operations effectively while minimizing cybersecurity risks in the industry 4.0 era or beyond.

Gul et al. [52] investigated Saudi E-commerce websites to understand the customers' security perceptions using trustworthiness, credit card usage concerns, and consumer ratings as primary criteria. The authors found that Saudi E-commerce websites lack customers' trust in the context of security, and there is a need to enhance the security features of Saudi websites. Similarly, Saeed [5] explored the user behavior of E-commerce customers in Pakistan using protection motivation theory as a theoretical model. The results highlighted that customer feelings, trustworthiness, motivation factors, and credit card concerns impact customer trust during online shopping.

3.5. Industrial Sector

Industry 5.0 advocates for establishing intelligent manufacturing systems, which require the Internet of Things based on technological implementation. There are many technological advancements to secure industrial organizations, such as automated attack detection [53,54], automated control rooms [55–57], zero trust architecture [58], and digital twins [59]. Osak and Buzina [60] explored ways to evaluate the flexibility and security of power systems under new conditions brought about by digital transformation and changes in industry practices, such as an increase in renewable energy sources and electric cars. The authors discussed principles for automatic control of power systems during digital transformation while considering differences between various electrical installations.

In another study, Mayhuasca and Sotelo [61] summarized how quantum technologies could revolutionize various industries by improving data processing capabilities and enhancing security against cyber threats. However, the authors acknowledged that further research is needed before these technologies can become widely adopted due to their complexity and the high cost currently associated with them. Overall, the authors suggested that continued exploration into quantum technology will likely lead to innovations

that could transform our society even further than what we have seen with traditional computing systems.

In another study, Raza et al. [62] explored how organizations balance preventing security issues with responding to them in digital transformation projects. This research likely presents original insights into how organizations approach managing IS security compliance during digital transformation initiatives. This paper focused on Robotic Process Automation (RPA) in digital transformation and its impact on Information Security Compliance. Similarly, Trung et al. [63] explored how IoTs, machine learning (ML), AI, and digital transformation impact service industries such as education, medicine-hospitals, tourism, and manufacturing sectors. The authors found that in the education sector, ML and IoTs have affected teaching methods by evaluating students' performance, which can help teachers choose suitable career development paths for learners. In the health sector, public health data processing is faster with big data due to ML technology being applied. Based on their empirical research findings, the authors proposed implications for future studies on applications of machine learning in each specific sector. They also highlighted cybersecurity risks associated with implementing these technologies that need management solutions. This study showed how emerging technologies like IoTs, machine learning (ML), and AI transform industries. Still, at the same time, it highlighted potential security risks associated with them, which need attention from researchers and practitioners who implement these systems into their organizations or businesses.

3.6. Diverse Organizational Contexts

In a study, Di et al. [64] proposed a networked organizational structure for enterprise information security management based on genetic algorithms and analyzed its benefits compared to traditional approaches. The authors identified the challenges enterprises face in managing their information security during digital transformation efforts, such as risks from cyber-attacks and data breaches. They proposed a new genetic algorithm approach to improve work efficiency, reduce costs, and maintain strong information security. Their experiments comparing traditional network organization structures with those based on genetic algorithms found that the latter was much more efficient in terms of work efficiency. Additionally, they provided data showing advantages such as cost savings and room for growth when implementing this approach within enterprises. Overall, the results suggested that using a networked organizational structure for enterprise information security management based on digital transformation and genetic algorithms can effectively maintain strong information security while improving work efficiency within businesses undergoing technological change.

Alenezi [65] examined the role of software engineering in digital transformation and its importance for secure development practices. The authors argued that software engineering has become essential in ensuring efficient functioning as organizations increasingly adopt digital solutions to improve their operations. They also highlighted that security concerns are critical during this process due to increased cyber threats. Analyzing trends in software engineering and examining case studies from various industries, such as healthcare and finance, they conclude that all digital systems rely on software for efficient performance while emphasizing how secure development practices can mitigate risks associated with adopting new technologies.

Moreover, in another paper, Marelli [66] discussed how digitization and new technologies are becoming increasingly crucial in humanitarian operations, making organizations vulnerable to cyber-attacks that can impact their ability to protect and assist those affected by armed conflict and violence.

In another study, Dvojmoč and Verboten [67] emphasized that employers have certain obligations to ensure employee information security, such as using appropriate hardware and software, configuring firewalls, and implementing antivirus programs. Furthermore, they highlighted the need for companies to comply with international instruments such as

the GDPR when dealing with personal data protection issues related to new technologies being implemented.

On the other hand, in the environmental sector, Mukhlynina et al. [68] examined the problem of introducing digital technologies into the system of environmental safety and protection in Russia. The authors focused on the role and specific steps currently being taken by state authorities at the federal level. They also highlighted legal problems that exist in this context. The detailed findings suggested several challenges associated with implementing digital transformation efforts related to environmental safety in Russia. These included a lack of clear regulatory frameworks, insufficient funding for research and development activities, inadequate infrastructure support, and limited public awareness about these issues. In terms of results, based on their analysis using the factor analysis method, they identified vital factors affecting digitization efforts, such as technological readiness, availability of a skilled workforce, government policies and regulations, etc., which can be used by policymakers while designing strategies toward achieving sustainable environmental goals through digitization. Furthermore, Halabi et al. advocated for green cybersecurity practices to save energy consumption [69].

Voskresenskaya [70] investigated the current state of digital transformation in governance, economy, and social sectors as a factor for development and security. The researchers found that digitalization has become an integral part of modern society. They identified vital attributes such as the mechanism for transforming economic cooperation into information/telecommunication space, active introduction/application of e-money/smart contracts into civil transactions, and development of e-governance. They also noted that problems within these areas could affect compatibility with other economies due to lagging data processing capabilities or the inability to use digital resources effectively. Based on their analysis using both qualitative (laws/regulations) and quantitative (statistical/comparative) methods at national/international levels, they concluded that there are significant benefits associated with embracing digitization across various sectors, including increased efficiency/productivity in service delivery processes, which ultimately leads toward sustainable growth/security.

In conclusion, it was recommended that governments prioritize investment in infrastructure necessary for the effective implementation/adoption of new technologies while ensuring that adequate regulation/policy frameworks exist to support innovation without compromising citizens' privacy/data protection rights. Additionally, given the rapid pace of change, businesses must adapt quickly to remain competitive. In another study, Kuchumov et al. [71] suggested that while there are potential benefits from digitization initiatives, such as increased efficiency and productivity gains, significant risks are involved, such as cybersecurity threats or job displacement due to automation. Furthermore, the impact of these initiatives varies depending on regional policies toward digitization. In conclusion, this paper highlighted that it is essential that policymakers in Russia's regions consider potential benefits and carefully evaluate possible negative impacts when implementing digital transformation strategies. By doing so, they can develop adequate public policies based on systemic analyses that take into account both positive effects along with serious risk factors affecting further development within each region individually rather than applying one-size-fits-all solutions across all areas indiscriminately without considering local conditions or needs specificities, which could lead to unintended consequences if not adequately addressed beforehand through careful planning processes involving stakeholders at different levels (local communities/businesses/government agencies).

Alahmadi et al. [72] highlighted that digital agriculture has helped automate labor-intensive jobs. However, many threats and vulnerabilities are associated with digital agriculture. They highlighted the potential side-channel attacks relevant to digital transformation. Similarly, Song et al. [73] highlighted that the Internet of Things and 5G networks have resulted in massive growth of digital agriculture. However, publishing a large volume of data is prone to security concerns. As a result, the authors have proposed a privacy-preserving data aggregation scheme that is more secure and flexible.

Gonçalves [74] highlighted that digital transformation in the accounting sector of small- and medium-scale enterprises is in its early stages; however, the benefits are widely recognized. Data protection and cybersecurity threats are vital challenges that need to be handled by accounting professionals. In another study, Tiron-Tudor et al. [75] highlighted that artificial intelligence, blockchain, and GPS technologies can help companies' accounting departments implement real-time auditing systems. However, companies must allocate substantial resources to mitigate cybersecurity risks associated with advanced technologies.

Rodríguez-Abitia and Bribiesca-Correa [76] highlighted the fact that technological advancements, such as artificial intelligence, the Internet of Things, blockchain, 3D printing, and secure technical infrastructure, will also change universities. Everyone may adopt a new role, such as content producer, influencer, etc., to contribute to the education sector. Similarly, Pavlova [77] highlighted that the culture is typically based on free and open knowledge sharing in an educational setting. However, security threats demand a balance between openness and security mechanisms. Table 1 provides a summary of all the literature discussed.

Power systems are complex infrastructures in modern society and are vulnerable to cybersecurity threats [78,79]. Dagoumas [80] has used IEEE RTS 96 power system, and the author highlighted that a combination of operating conditions and cyber-attacks should be used to evaluate system stability. Diaba et al. [81] highlighted that power system communication protocols are prone to cyber-attacks by hackers. The authors have proposed an algorithm outperforming conventional deep learning approaches using SVM, ANN, and CNN. Similarly, Presekal et al. [82] developed a hybrid machine learning model using Graph Convolutional Long Short-Term Memory (GC-LSTM) and a deep convolutional network for anomaly detection in electrical power grids.

Kechagias et al. [83] highlighted that cybersecurity in the maritime industry has become very important. The authors have presented a detailed case of how a maritime company adopted a systematic approach to review its cybersecurity strategic policies, found loopholes, and subsequently performed risk mitigation.

Table 1. Key findings of literature.

Paper	Publication Year	Application Domain	Key Technologies/Theories	Key Findings
[22]	2022	Financial sector	Artificial intelligence, cognitive mapping, DEMATEL techniques	Provision of a decision-support model by combining the decision-making trial and evaluation laboratory (DEMATEL) method and cognitive mapping.
[23]	2023	Financial sector	Cognitive technologies	Provided directions to use cognitive technologies in the digital transformation of the Russian economy.
[24]	2022	Financial sector	Artificial intelligence, blockchain, voice-based technology, or natural language processing	Higher trust in Fintech by stakeholders in the financial sector.
[25]	2019	Public institutions, financial institutions, banking institutions, industry, transportation, and agriculture	Different technologies related to digitalization	Highlighting the need for information security in different application domains.
[34]	2023	Healthcare sector	No specific technology was mentioned	Sustainability of digital transformation in the healthcare sector requires cybersecurity skills, uncertainty management, and the healthcare sector's interdependence.

Table 1. *Cont.*

Paper	Publication Year	Application Domain	Key Technologies/Theories	Key Findings
[35]	2023	Healthcare sector	Electronic health records, remote patient monitoring, artificial intelligence, telemedicine, and federated learning	Privacy and security recommendations for the healthcare sector.
[36]	2020	Healthcare sector	Smartphone apps and wearable tech products enable data sharing	Need for data privacy of patients in healthcare applications.
[37]	2021	Healthcare sector	No specific technology was mentioned	Need for enhanced cybersecurity in post-COVID-19 digital transformation.
[41]	2022	Government sector	No specific technology was mentioned	Recommendation to use a secure network by the ministry in Palestine.
[42]	2022	Government sector	No specific technology was mentioned	Establishment of clear data exchange policies and clear job descriptions for IT employees.
[43]	2023	Government tax payments	Full-service mobile apps and e-payment channel	Need for actions to make the process transparent and legal in Danish tax payment.
[44]	2023	Governmental and other public services	AI and other leading technologies	Emphasizes cybersecurity governance.
[45]	2021	Government critical infrastructure	No specific technology was mentioned	Emphasizes cybersecurity of critical infrastructure.
[47]	2022	Business sector	No specific technology was mentioned.	Emphasizes state regulations for the transformation of economic clusters at the international level.
[48]	2022	Business sector	Advanced encryption and data analytics are essential for cybersecurity and AML efficiency	Analyzed digital transformation and cybersecurity situations across different countries.
[49]	2022	Business sector	Business sector advanced encryption and data analytics are essential for cybersecurity and AML efficiency	Digital transformation in Indonesia and six-ware cyber security framework.
[50]	2023	Business sector	IT security and data protection, cloud migration, cloud computing	Security concerns for cloud transformation of business.
[51]	2021	Business sector	Blockchain, IoTs, AI, and other emerging technologies	SWOT analysis of blockchain and other technologies.
[52]	2022	E-commerce	Trustworthiness, credit card usage concerns, consumer rating	User information security perception in Saudi Arabian E-commerce applications.
[5]	2023	E-commerce	Protection Motivation Theory	User information security perception of E-commerce in Pakistan.
[60]	2023	Industrial sector	No specific technology was mentioned	Security implication of small power plants.

Table 1. *Cont.*

Paper	Publication Year	Application Domain	Key Technologies/Theories	Key Findings
[61]	2022	Industrial sector	Quantum computing, cryptography, optical fiber, and related technologies are discussed	Information security implications in quantum technologies.
[62]	2019	Industrial sector	Robotic Process Automation (RPA)	Information system security compliance and response implications.
[63]	2019	Service industry	IoTs, machine learning, AI, and digital transformation	Cybersecurity implications of IoTs, machine learning, and digital transformation.
[64]	2022	Networked organizational structure	Genetic algorithms	Factors affecting quality in manufacturing settings.
[65]	2021	Work environment	Cloud computing	Emphasizes the importance of secure software development in digital transformation.
[66]	2020	Enterprises	Mobile devices, cloud computing, social media platforms	Cybersecurity implications for the digital transformation of humanitarian organizations.
[67]	2022	Work environment	Firewalls, encryption software, intrusion detection systems	Emphasizes data security of employee data in organizations.
[68]	2022	Environment	No specific technology focused on	Digital transformation and environmental security in Russia.
[69]	2022	Environment	IoTs	Green IoTs and adaptive cybersecurity implications.
[70]	2019	Governance, economy, and social sectors	No specific technology was mentioned	Digital transformation and security in Russia.
[71]	2020	Economy	No specific technology was mentioned	Economic security and digital transformation in Russia.
[72]	2022	Digital agriculture	Smart sensors, Internet of Things, machine learning	Side-channel attacks in digital agriculture.
[73]	2020	Digital agriculture	Internet of Things, 5G networks	Privacy-preserving data aggregation scheme.
[74]	2022	Digital accounting	Robotics, enterprise resource planning, artificial intelligence, optical character recognition	Digital transformation and future of accounting.
[75]	2022	Digital accounting	AI, blockchain, cloud computing	Emphasis on benefits for accounting firms in digital transformation.
[76]	2021	Education	Artificial intelligence, Internet of Things, blockchain, 3D printing, cybersecurity, big data	Futuristic universities in the era of digital transformation.
[77]	2022	Education	No specific technology focused on	Emphasis on cybersecurity culture in universities.

Table 1. *Cont.*

Paper	Publication Year	Application Domain	Key Technologies/Theories	Key Findings
[80]	2019	Power systems	IEEE RTS 96	Emphasizes the impact of cybersecurity attacks on power systems.
[81]	2023	Power systems	Artificial neural networks, convolutional neural networks, and support vector machines	Meta-heuristic and deep learning algorithms for cybersecurity in power systems.
[82]	2023	Power systems	Graph Convolutional Long Short-Term Memory (GC-LSTM) and a deep convolutional network	Model for situational awareness in online cyber-attack.
[83]	2022	Maritime	No specific technology focused on	Cybersecurity implications for maritime industry.

4. Discussion

Table 1 highlights that advanced technologies such as the IoTs [51,53], blockchain [63,74], and 5G [84,85] networks can facilitate organizations in securing business processes and making them efficient [1,2]. Furthermore, machine learning approaches [63,72,86] can help identify malicious traffic in the network, which can help in identifying cyber threats proactively. However, such technological interventions should be well thought out and appropriately designed [9]. While new technologies can increase efficiency and competitiveness of businesses, they also bring unknown risks, such as cyber-attacks [3]. This leaves them vulnerable to cyber threats, which could have significant economic consequences. Therefore, raising awareness about these risks among industry professionals is essential. Additionally, there should be reasonable security measures to secure technological infrastructures from cyber-attacks [87]. A fundamental security strategy could help organizations from recurring cyber-attacks [88]. Therefore, it is important to analyze cybersecurity risks during the transition to the digital economy [89]. Governments have an extensive role in developing and implementing national-level policy. For instance, establishing a national cybersecurity strategy has helped Greece pursue digital transformation [90]. It should also be considered that while aiming for digital transformation, human factors should also be considered. Human performance degradation is a critical factor in cybersecurity attacks [91]. As shown in the taxonomy of the literature in Figure 3, every sector of the economy is benefiting from the advances in digital transformation and trying to minimize cybersecurity risks.

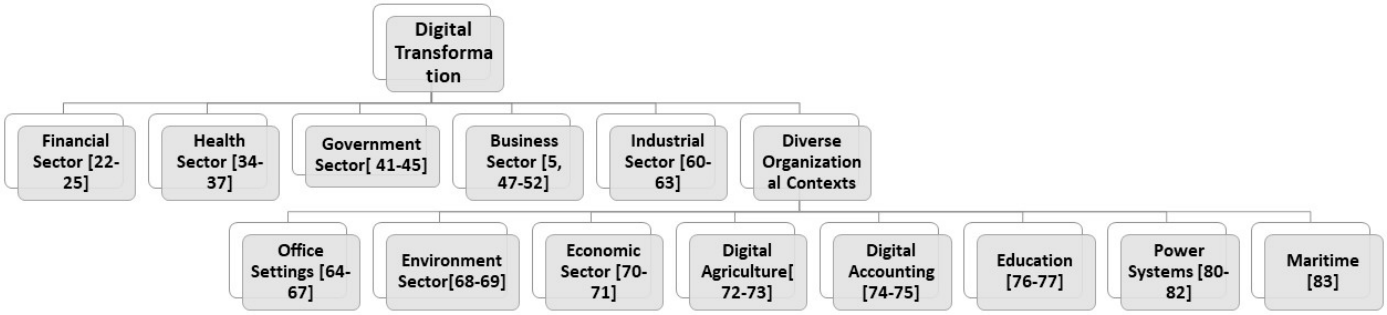

Figure 3. Taxonomy of the literature.

In the literature, some review articles have focused on digital transformation, such as an article by Metawa et al. [92], which investigated the role of information in digital transformation in the context of Egyptian small- and medium-scale enterprises. Similarly, Özsungur [93] researched business strategy for cybersecurity in digital transformation, and

Nguyen Duc [94] documented security risk from an engineering perspective. Furthermore, Hai et al. [1] highlighted the opportunities and challenges for emerging countries regarding digital transformation, and Kour's work [95] focused on cybersecurity implications in the railway domain. Despite these surveys within the literature, no survey has presented a domain taxonomy and looked into cybersecurity implications in diverse industries, as has been explored in this paper. Based on our review, we propose a cybersecurity readiness framework for business organizations pursuing digital transformation. As shown in Figure 4, this framework has four levels.

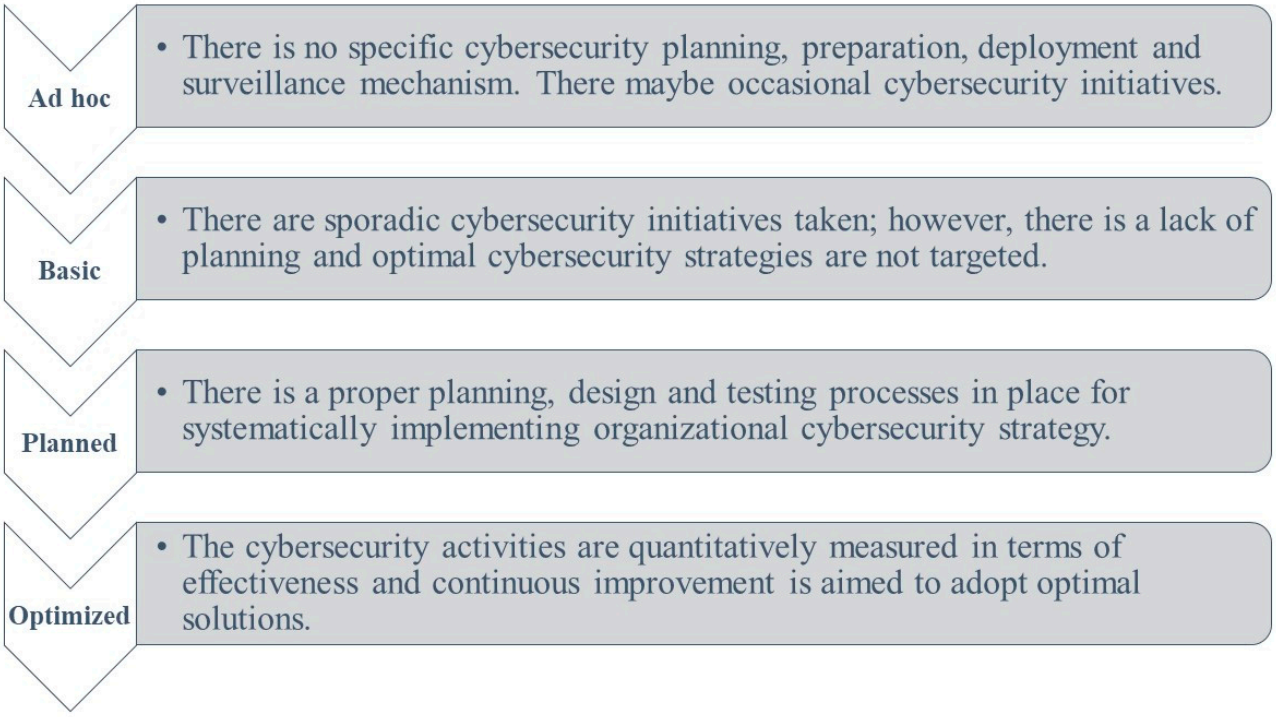

Figure 4. Cybersecurity readiness framework for business organizations.

At the ad hoc level, organizations do not have planning, preparation, deployment, and surveillance mechanisms to respond to cybersecurity threats. Cybersecurity resilience is dependent on the personal initiatives of employees. Emerging technologies such as artificial intelligence, big data and analytics, blockchain, cloud computing, and services drive digital transformation worldwide while increasing cybersecurity risks for businesses undergoing this process. Therefore, it is crucial to analyze cybersecurity measures during implementation in pursuit of digital transformation, but the organizations at this level do not focus on these aspects.

At the basic level of our framework, organizations have essential cybersecurity planning, preparation, deployment, and surveillance activities in place but no organizational strategic policy regarding cybersecurity. The processes are not mature, and isolated efforts are carried out; no data about the effectiveness of employed cybersecurity approaches are available.

At the planned level of our framework, organizations need a well-planned organizational cybersecurity strategy documenting the processes for cybersecurity preparation, deployment, and surveillance. During the surveillance phase, potential vulnerabilities must be regularly assessed through penetration testing or vulnerability scanning. In addition, it is essential for organizations undergoing DT to consider the human factor in cybersecurity. This means providing regular training and awareness programs for employees to identify and respond appropriately to potential cyber threats. Furthermore, as technology advances rapidly, new security risks not yet fully understood or addressed by current security measures will likely emerge. It will be crucial for businesses undergoing DT involving

IoTs devices or other emerging technologies like 5G networks or quantum computing to prioritize comprehensive risk assessments before implementing such solutions.

Organizations aiming for an optimized level need to continuously measure the effectiveness of their cybersecurity planning, preparation, deployment, and surveillance mechanisms. As technology evolves rapidly and new cyber threats constantly emerge, vulnerabilities may arise even with robust security measures. Therefore, it is essential for organizations undergoing DT to perform futuristic technological forecasting and associated cybersecurity planning to continuously innovate their processes. A proactive approach toward optimized security processes can help mitigate future risks associated with digital transformation efforts.

5. Conclusions

This systematic literature review has shed light on the critical role of cybersecurity in digital transformation (DT). Digital transformation has transformed the business sector by transitioning organizational processes to IT solutions, resulting in significant changes across various aspects of an organization. It impacts multiple elements, such as user experience, operations, markets, customers, relationships, and cultural differences. Emerging technologies, including artificial intelligence (AI), big data and analytics, blockchain technology, cloud computing, and services, drive digital transformation worldwide while increasing cybersecurity risks for businesses undergoing this process. And the implications of cybersecurity for digital transformation are significant. As enterprises undergo the process of digital transformation, they become more vulnerable to cyber-attacks and security breaches. Cybersecurity is an essential component of digital transformation as it helps prevent interruptions due to malicious activities or unauthorized access by attackers aiming at sensitive information alteration, destruction, or extortion from users. The COVID-19 pandemic has further highlighted the importance of cybersecurity in DT implementation, as cybercriminals have taken advantage of vulnerabilities created by this rapid shift toward digitalization. Therefore, organizations undergoing DT adoption must prioritize cybersecurity measures to ensure a successful transition without any disruptions caused by security breaches. The study highlights that DT is a complex and ongoing process that requires organizations to be aware of emerging technologies and their associated security risks. As businesses transition their primary operations to IT solutions, they must ensure appropriate measures are in place to protect data and networks from unauthorized access or malicious activities. The findings suggest that implementing encryption or cyber insurance policies can help mitigate these risks during DT implementation. For future studies, we recommend the importance of organizations having comprehensive knowledge of cybersecurity threats throughout the entire process. This includes identifying potential vulnerabilities early on and proactively addressing them.

Author Contributions: Conceptualization, S.S.; methodology, S.A.A., N.A.A. and E.A.; data curation, S.A.A., N.A.A. and E.A.; writing—original draft preparation, S.S., S.A.A., N.A.A. and E.A.; writing—review and editing, D.A.A.; supervision, S.S.; funding acquisition, D.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University, for funding this project.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hai, T.N.; Van, Q.N.; Thi Tuyet, M.N. Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. *Emerg. Sci. J.* **2021**, *5*, 21–36. [CrossRef]
2. Möller, D. *Cybersecurity in Digital Transformation: Scope and Applications*; Springer: Berlin/Heidelberg, Germany, 2020.
3. Matt, C.; Hess, T.; Benlian, A. Digital transformation strategies. *Bus. Inf. Syst. Eng.* **2015**, *57*, 339–343. [CrossRef]
4. Saeed, S. Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability* **2023**, *15*, 6019. [CrossRef]
5. Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. *Appl. Sci.* **2023**, *13*, 1020. [CrossRef]
6. Sharif, M.H.U.; Mohammed, M.A. A literature review of financial losses statistics for cyber security and future trend. *World J. Adv. Res. Rev.* **2022**, *15*, 138–156. [CrossRef]
7. Haislip, J.; Kolev, K.; Pinsker, R.; Steffen, T. The economic cost of cybersecurity breaches: A broad-based analysis. In Proceedings of the Workshop on the Economics of Information Security (WEIS), Boston, MA, USA, 3–4 June 2019; Volume 1, p. 37.
8. Garg, V. Covenants without the Sword: Market Incentives for Cybersecurity Investment. In Proceedings of the TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, Virtual, 22–24 September 2021.
9. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. *Bus. Horiz.* **2021**, *64*, 659–671. [CrossRef]
10. Gordon, L.A.; Loeb, M.P.; Zhou, L. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *J. Cybersecur.* **2020**, *6*, tyaa005. [CrossRef]
11. Krutilla, K.; Alexeev, A.; Jardine, E.; Good, D. The benefits and costs of cybersecurity risk reduction: A dynamic extension of the Gordon and Loeb model. *Risk Anal.* **2021**, *41*, 1795–1808. [CrossRef]
12. Simon, J.; Omar, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *Eur. J. Oper. Res.* **2020**, *282*, 161–171. [CrossRef]
13. Uddin, M.H.; Ali, M.H.; Hassan, M.K. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Manag.* **2020**, *22*, 239–309. [CrossRef]
14. Curti, F.; Ivanov, I.; Macchiavelli, M.; Zimmermann, T. City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity. The Financial Costs of Lax Cybersecurity. Available online: https://ssrn.com/abstract=4465071 (accessed on 15 June 2023).
15. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef] [PubMed]
16. Al-Alawi, A.I.; Al-Bassam MS, A. The significance of cybersecurity system in helping managing risk in banking and financial sector. *J. Xidian Univ.* **2020**, *14*, 1523–1536.
17. Hasan, M.F.; Al-Ramadan, N.S. Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. *Soc. Sci. Humanit. J.* **2021**, *5*, 2312–2323.
18. Joveda, N.; Khan, M.T.; Pathak, A.; Chattogram, B. Cyber laundering: A threat to banking industries in Bangladesh: In quest of effective legal framework and cyber security of financial information. *Int. J. Econ. Financ.* **2019**, *11*, 54–65. [CrossRef]
19. Almudaires, F.; Almaiah, M. Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 732–738.
20. Smith, K.J.; Dhillon, G. Assessing blockchain potential for improving the cybersecurity of financial transactions. *Manag. Financ.* **2020**, *46*, 833–848. [CrossRef]
21. Kuzmenko, O.; Kubálek, J.; Bozhenko, V.; Kushneryov, O.; Vida, I. An approach to managing innovation to protect financial sector against cybercrime. *Pol. J. Manag. Stud.* **2021**, *24*, 276–291. [CrossRef]
22. Rodrigues, A.R.D.; Ferreira, F.A.; Teixeira, F.J.; Zopounidis, C. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Res. Int. Bus. Financ.* **2022**, *60*, 101616. [CrossRef]
23. Fedorov, B.M.; Fedorova, S.V.; Zhang, H.; Mamedova, N.A. Using Cognitive Technologies to Ensure the Information Security of Banks in the Conditions of Digital Transformation and Development of Biometrical Identification. *WSEAS Trans. Bus. Econ.* **2023**, *20*, 382–387. [CrossRef]
24. Patil, R.; Bharathi, S.V. A Study on the Business Transformation, Security issues and Investors Trust in Fintech Innovation. *Cardiometry* **2022**, *24*, 918–932.
25. Rãƒdulescu, C.V.; Bodislav, D.A.; Negescu, M.D.O. The Risks of Digitization in the Context of Economic Development and of Ensuring Social and Informational Security. In Proceedings of the International Management Conference, Poznan, Poland, 27–29 June 2019; Faculty of Management, Academy of Economic Studies: Bucharest, Romania, 2019; Volume 13, pp. 1040–1050.
26. Mijwil, M.; Aljanabi, M.; Ali, A.H. Chatgpt: Exploring the role of cybersecurity in the protection of medical information. *Mesopotamian J. Cybersecur.* **2023**, *2023*, 18–21. [CrossRef]
27. Sethuraman, S.C.; Vijayakumar, V.; Walczak, S. Cyber attacks on healthcare devices using unmanned aerial vehicles. *J. Med. Syst.* **2020**, *44*, 29. [CrossRef]
28. Buzdugan, A. Integration of cyber security in healthcare equipment. In Proceedings of the 4th International Conference on Nanotechnologies and Biomedical Engineering: Proceedings of ICNBME-2019, Chisinau, Moldova, 18–21 September 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 681–684.
29. Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the Internet of medical things. *Health Policy Technol.* **2021**, *10*, 100549. [CrossRef]

30. Abie, H. Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–6.
31. Loi, M.; Christen, M.; Kleine, N.; Weber, K. Cybersecurity in health–disentangling value tensions. *J. Inf. Commun. Ethics Soc.* **2019**, *17*, 229–245. [CrossRef]
32. Ali, K.A.; Alyounis, S. Cybersecurity in healthcare industry. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 695–701.
33. Abbas HS, M.; Qaisar, Z.H.; Ali, G.; Alturise, F.; Alkhalifah, T. Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. *PLoS ONE* **2022**, *17*, e0274550. [CrossRef] [PubMed]
34. Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in healthcare systems: Cyber security and digital transformation. *Technovation* **2023**, *121*, 102583. [CrossRef]
35. Paul, M.; Maglaras, L.; Ferrag, M.A.; AlMomani, I. Digitization of Healthcare Sector: A Study on Privacy and Security Concerns. *ICT Express* **2023**, *in press*. [CrossRef]
36. Nwaiwu, F.; Mbelu, S. Digital Transformation in Healthcare and Surveillance Capitalism: Comparative Assessment of Data and Privacy Protection Compliance across the European Union (5 July 2020). Available online: https://ssrn.com/abstract=3643838 (accessed on 15 June 2023).
37. Maleh, Y.; Mellal, B. Digital transformation and cybersecurity in the context of COVID-19 proliferation. *IEEE Technol. Policy Ethics* **2021**, *6*, 1–4. [CrossRef]
38. Shaheen, K.; Zolait, A.H. The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain. *Inf. Comput. Secur.* **2023**. *ahead-of-print*. [CrossRef]
39. Montasari, R. Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. In *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*; Springer Nature: Berlin/Heidelberg, Germany, 2023; pp. 7–25.
40. Alhalafi, N.; Veeraraghavan, P. Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. *Smart Cities* **2023**, *6*, 1523–1544. [CrossRef]
41. Al Shobaki, M.J.; El Talla, S.A.; Al Najjar, M.T. Digital Transformation and Its Impact on the Application of Cyber Security in the Ministry of Interior and National Security in Palestine. 2022. Available online: http://www.moi.gov.ps (accessed on 15 June 2023).
42. Al Najjar, M.T.; Al Shobaki, M.J.; El Talla, S.A. The Reality of Digital Transformation in the Palestinian Ministry of Interior and National Security. 2022. Available online: www.ijeais.org/ijamsr (accessed on 15 June 2023).
43. Fjord, L.B.; Schmidt, P.K. The Digital Transformation of Tax Systems: Progress, Pitfalls and Protection in a Danish Context. 2022. Available online: https://ssrn.com/abstract=4252832 (accessed on 15 June 2023).
44. Mijwil, M.; Filali, Y.; Aljanabi, M.; Bounabi, M.; Al-Shahwani, H. The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian J. Cybersecur.* **2023**, *2023*, 1–6.
45. Maglaras, L.; Kantzavelou, I.; Ferrag, M.A. Digital Transformation and Cybersecurity of Critical Infrastructures. *Appl. Sci.* **2021**, *11*, 8357. [CrossRef]
46. Bokhari, S.; Hamrioui, S.; Aider, M. Cybersecurity strategy under uncertainties for an IoE environment. *J. Netw. Comput. Appl.* **2022**, *205*, 103426. [CrossRef]
47. Gonchar, V. *The Transformation of Entrepreneurial Activity in the Conditions of the Development of the Digital Economy and a Methodology of Assessing Its Digital Security in Digital Technologies in the Contemporary Economy: Collective Monograph*; Simanavičienė, Ž., Ed.; Mykolas Romeris University Research: Vilnius, Lithuania, 2022; ISBN 9786094880506.
48. Kuzior, A.; Vasylieva, T.; Kuzmenko, O.; Koibichuk, V.; Brożek, P. Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. *J. Open Innov. Technol. Mark. Complex.* **2022**, *8*, 195. [CrossRef]
49. Putri MS, D.; Gultom, R.A.; Wadjdi, A.F. The Concept of an Electronic-Based Government System and the Six-Ware Cyber Security Framework in Supporting the Digitization of the Indonesian Government. *Def. Secur. Stud.* **2023**, *4*, 1–7.
50. Shitta-Bey, A.M. Security Concerns of Cloud Migration and Its Implications on Cloud-Enabled Business Transformation Effect of Quality Education on Poverty Alleviation View Project. Master's Thesis, Università della Svizzera Italiana, Lugano, Switzerland, 2023. Available online: https://www.researchgate.net/publication/369118961 (accessed on 15 June 2023).
51. Trung, N.D.; Huy DT, N.; Van Thanh, T.; Thanh NT, P.; Dung, N.T.; Thanh Huong, L.T. Digital transformation, AI applications and IoTs in Blockchain managing commerce secrets: And cybersecurity risk solutions in the era of industry 4.0 and further. *Webology* **2021**, *18*, 10–14704. [CrossRef]
52. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Alamer, A. An empirical study of mobile commerce and customers security perception in Saudi Arabia. *Electronics* **2022**, *11*, 293. [CrossRef]
53. Anthi, E.; Williams, L.; Rhode, M.; Burnap, P.; Wedgbury, A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. *J. Inf. Secur. Appl.* **2021**, *58*, 102717. [CrossRef]
54. Meeran, Y.A.; Shyry, S.P. Resilient Detection of Cyber Attacks in Industrial Devices. In Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–13 April 2023; pp. 564–569.
55. Ameri, K.; Hempel, M.; Sharif, H.; Lopez Jr, J.; Perumalla, K. Design of a novel information system for semi-automated management of cybersecurity in industrial control systems. *ACM Trans. Manag. Inf. Syst.* **2023**, *14*, 1–35. [CrossRef]

56. Buja, A.; Apostolova, M.; Luma, A. Enhancing Cyber Security in Industrial Internet of Things Systems: An Experimental Assessment. In Proceedings of the 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 14 June 2023; pp. 1–5.
57. Ramirez, R.; Chang, C.K.; Liang, S.H. PLC Cybersecurity Test Platform Establishment and Cyberattack Practice. *Electronics* **2023**, *12*, 1195. [CrossRef]
58. Zanasi, C.; Russo, S.; Colajanni, M. Flexible Zero Trust Architecture for the Cybersecurity of Industrial Iot Infrastructures. Available online: https://ssrn.com/abstract=4481853 (accessed on 15 June 2023).
59. Jacopo, P.; Graziana, C.; Federica, P.; Giarrè, L. Using Digital Twin to Detect Cyber-Attacks in Industrial Control Systems. In Proceedings of the IEEE Proceedings of 2023 EUROCON, Torino, Italy, 6–8 July 2023.
60. Osak, A.; Buzina, E. Flexibility and security of power systems, methods of analysis, and criteria for their evaluation in the conditions of digital transformation of the power industry. *AIP Conf. Proc.* **2023**, *2552*, 040008.
61. Mayhuasca, J.; Sotelo, S. Quantum Technologies for Digital Transformation and Informatica Security. *Int. J. Eng. Sci.* **2022**, *15*, 43–50. [CrossRef]
62. Raza, H.; Baptista, J.; Constantinides, P. *Conceptualizing the Role of IS Security Compliance in Projects of Digital Transformation: Tensions and Shifts between Prevention and Response Modes*; ICIS: Houston, TX, USA, 2019.
63. Trung, N.D.; Huy DT, N.; Le, T.H. IoTs, machine learning (ML), AI and digital transformation affects various industries-principles and cybersecurity risks solutions. *Management* **2021**, *18*, 10–14704. [CrossRef]
64. Di, Z.; Liu, Y.; Li, S. Networked Organizational Structure of Enterprise Information Security Management Based on Digital Transformation and Genetic Algorithm. *Front. Public Health* **2022**, *10*, 921632. [CrossRef]
65. Alenezi, M. Software and Security Engineering in Digital Transformation. *arXiv* **2021**, arXiv:2201.01359.
66. Marelli, M. Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation. *Int. Rev. Red Cross* **2020**, *102*, 367–387. [CrossRef]
67. Dvojmoč, M.; Verboten, M.T. Cyber (In) security of Personal Data and Information in Times of Digitization. *Med. Law Soc.* **2022**, *15*, 287–304. [CrossRef]
68. Zarapina, L.; Mukhlynina, M.; Adamenko, A.; Mukhlynin, D.; Belokopytova, N. Issues of Legal Support of Socio-economic Policy and Environmental Security of Russia in the Context of Digital Transformation. In Proceedings of the International Scientific-Practical Conference "Ensuring the Stability and Security of Socio-Economic Systems: Overcoming the Threats of the Crisis Space" (SES 2021), Kirov, Russia, 17–18 June 2021; Sciete Press: Kirov, Russia, 2021; pp. 336–340, ISBN 978-989-758-546-3. [CrossRef]
69. Halabi, T.; Bellaiche, M.; Fung, B.C. Towards Adaptive Cybersecurity for Green IoT. In Proceedings of the 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bali, Indonesia, 24–26 November 2022; pp. 64–69.
70. Voskresenskaya, E.; Vorona-Slivinskaya, L.; Panov, S. Digital transformation of social sector as the factor of development and security of the country. In *E3S Web of Conferences*; EDP Sciences: Les Ulis, France, 2019; Volume 135, p. 03075.
71. Kuchumov, A.; Pecherictsa, E.; Chaikovskaya, A.; Zhilyaeva, I. Digital transformation in the concept of economic security of Russia and its regions. In Proceedings of the 2nd International Scientific Conference on Innovations in Digital Economy, St. Petersburg, Russia, 22–23 October 2020; pp. 1–8.
72. Alahmadi, A.N.; Rehman, S.U.; Alhazmi, H.S.; Glynn, D.G.; Shoaib, H.; Solé, P. Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors* **2022**, *22*, 3520. [CrossRef]
73. Song, J.; Zhong, Q.; Wang, W.; Su, C.; Tan, Z.; Liu, Y. FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture. *IEEE Sens. J.* **2020**, *21*, 17430–17438. [CrossRef]
74. Gonçalves, M.J.A.; da Silva, A.C.F.; Ferreira, C.G. The Future of Accounting: How Will Digital Transformation Impact the Sector? *Informatics* **2022**, *9*, 19. [CrossRef]
75. Tiron-Tudor, A.; Donțu, A.N.; Bresfelean, V.P. Emerging Technologies' Contribution to the Digital Transformation in Accountancy Firms. *Electronics* **2022**, *11*, 3818. [CrossRef]
76. Rodríguez-Abitia, G.; Bribiesca-Correa, G. Assessing digital transformation in universities. *Future Internet* **2021**, *13*, 52. [CrossRef]
77. Pavlova, E. Enhancing the organisational culture related to cyber security during the university digital transformation. *Inf. Secur.* **2020**, *46*, 239–249. [CrossRef]
78. Ribas Monteiro, L.F.; Rodrigues, Y.R.; Zambroni de Souza, A.C. Cybersecurity in Cyber–Physical Power Systems. *Energies* **2023**, *16*, 4556. [CrossRef]
79. Liang, J.; Zhu, H.; Zhang, B.; Liu, L.; Liu, X.; Lin, H.; Tian, J.; Chen, Q. Research and Prospect of Cyber-Attacks Prediction Technology for New Power Systems. In Proceedings of the 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 24–26 February 2023; Volume 6, pp. 638–647.
80. Dagoumas, A. Assessing the impact of cybersecurity attacks on power systems. *Energies* **2019**, *12*, 725. [CrossRef]
81. Diaba, S.Y.; Shafie-Khah, M.; Elmusrati, M. Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms. *IEEE Access* **2023**, *11*, 18660–18672. [CrossRef]
82. Presekal, A.; Ştefanov, A.; Rajkumar, V.S.; Palensky, P. Attack graph model for cyber-physical power systems using hybrid deep learning. *IEEE Trans. Smart Grid* **2023**. *Early Access*. [CrossRef]
83. Kechagias, E.P.; Chatzistelios, G.; Papadopoulos, G.A.; Apostolou, P. Digital transformation of the maritime industry: A cybersecurity systemic approach. *Int. J. Crit. Infrastruct. Prot.* **2022**, *37*, 100526. [CrossRef]

84. Khashan, O.A.; Alamri, S.; Alomoush, W.; Alsmadi, M.K.; Atawneh, S.; Mir, U. Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments. *Comput. Mater. Contin.* **2023**, *75*, 3133–3158. [CrossRef]
85. Sufyan, A.; Khan, K.B.; Khashan, O.A.; Mir, T.; Mir, U. From 5G to beyond 5G: A Comprehensive Survey of Wireless Network Evolution, Challenges, and Promising Technologies. *Electronics* **2023**, *12*, 2200. [CrossRef]
86. Al-Taleb, N.; Saqib, N.A. Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. *Appl. Sci.* **2022**, *12*, 1863. [CrossRef]
87. Sandhu, K. Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges. In *Handbook of Research on Advancing Cybersecurity for Digital Transformation*; IGI Global: Hershey, PA, USA, 2021; pp. 1–17.
88. Azizi, N.; Haass, O. Cybersecurity Issues and Challenges. In *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*; IGI Global: Hershey, PA, USA, 2023; pp. 21–48. [CrossRef]
89. Lesmana, D.; Afifuddin, M.; Adriyanto, A. Challenges and Cybersecurity Threats in Digital Economic Transformation. *Int. J. Humanit. Educ. Soc. Sci.* **2023**, *2*. [CrossRef]
90. Maglaras, L.; Drivas, G.; Chouliaras, N.; Boiten, E.; Lambrinoudakis, C.; Ioannidis, S. Cybersecurity in the era of digital transformation: The case of Greece. In Proceedings of the 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), Zhenjiang, China, 27–29 November 2020; pp. 1–5.
91. Nobles, C. Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–J. Bus. Public Adm.* **2022**, *13*, 49–72. [CrossRef]
92. Metawa, N.; Elhoseny, M.; Mutawea, M. The role of information systems for digital transformation in the private sector: A review of Egyptian SMEs. *Afr. J. Econ. Manag. Stud.* **2022**, *13*, 468–479. [CrossRef]
93. Özsungur, F. Business Management and Strategy in Cybersecurity for Digital Transformation. In *Handbook of Research on Advancing Cybersecurity for Digital Transformation*; IGI Global: Hershey, PA, USA, 2021; pp. 144–162.
94. Nguyen Duc, A.; Chirumamilla, A. Identifying security risks of digital transformation-an engineering perspective. In *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, 18–20 September 2019*; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 677–688.
95. Kour, R.; Patwardhan, A.; Thaduri, A.; Karim, R. A review on cybersecurity in railways. *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit* **2023**, *237*, 3–20. [CrossRef]

future internet

IMPACT FACTOR 2.8

CITESCORE 7.1

Review

Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods

Tehseen Mazhar, Hafiz Muhammad Irfan, Sunawar Khan, Inayatul Haq, Inam Ullah, Muhammad Iqbal and Habib Hamam

Special Issue

Cybersecurity in the Era of AI

Edited by

Dr. Mazdak Zamani, Dr. Rohit Tanwar and Dr. Touraj Khodadadi

MDPI

https://doi.org/10.3390/fi15020083

future internet

MDPI

Review

Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods

Tehseen Mazhar [1,*], Hafiz Muhammad Irfan [2], Sunawar Khan [2], Inayatul Haq [3], Inam Ullah [4], Muhammad Iqbal [5] and Habib Hamam [6,7,8,9,*]

1 Department of Computer Science, Virtual University of Pakistan, Lahore 51000, Pakistan
2 Department of Computer Science, Islamia University Bahawalpur, Bahawalnagar 62300, Pakistan
3 School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China
4 BK21 Chungbuk Information Technology Education and Research Center, Chungbuk National University, Cheongju 28644, Republic of Korea
5 Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan 29220, Pakistan
6 Faculty of Engineering, Université de Moncton, Moncton, NB E1A3E9, Canada
7 Spectrum of Knowledge Production & Skills Development, Sfax 3027, Tunisia
8 International Institute of Technology and Management, Commune d'Akanda, Libreville 1989, Gabon
9 Department of Electrical and Electronic Engineering Science, School of Electrical Engineering, University of Johannesburg, Johannesburg 2006, South Africa
* Correspondence: tehseenmazhar719@gmail.com (T.M.); habib.hamam@umoncton.ca (H.H.)

Abstract: Smart grids are rapidly replacing conventional networks on a worldwide scale. A smart grid has drawbacks, just like any other novel technology. A smart grid cyberattack is one of the most challenging things to stop. The biggest problem is caused by millions of sensors constantly sending and receiving data packets over the network. Cyberattacks can compromise the smart grid's dependability, availability, and privacy. Users, the communication network of smart devices and sensors, and network administrators are the three layers of an innovative grid network vulnerable to cyberattacks. In this study, we look at the many risks and flaws that can affect the safety of critical, innovative grid network components. Then, to protect against these dangers, we offer security solutions using different methods. We also provide recommendations for reducing the chance that these three categories of cyberattacks may occur.

Keywords: smart grid; cyber security; cyberattacks; machine learning; deep learning; data mining

Citation: Mazhar, T.; Irfan, H.M.; Khan, S.; Haq, I.; Ullah, I.; Iqbal, M.; Hamam, H. Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. *Future Internet* **2023**, *15*, 83. https://doi.org/10.3390/fi15020083

Academic Editors: Mazdak Zamani, Rohit Tanwar, Behrang Samadi and Touraj Khodadadi

Received: 16 January 2023
Revised: 16 February 2023
Accepted: 18 February 2023
Published: 19 February 2023

1. Introduction

Modern technologies were integrated into the traditional electrical infrastructure to create a "smart grid". A smart grid has several ways to control operations and power. Examples of operational and energy measures include smart meters and appliances installed at the client's site, a production meter, renewable energy generators, smart inverters, and resources installed at the grid's location for energy efficiency [1]. Renewable energy generators can lower energy costs because it is free to produce energy from renewable sources, even though it is not always available and depends on variables like temperature, humidity, wind speed and direction, and location. Solar energy is influenced by the sun's brightness, cloud cover, and temperature [2]. The power that can be taken from the wind depends significantly on its direction and speed. Using renewable energy effectively and on time is possible because of the many technologies available for forecasting wind, solar, and battery state of charge. Sensors may communicate to and receive data from the smart grid because it has data transmission and reception capabilities [2]. These sensors provide data packets to the grid continuously. These data packets could include information on the production. Information on energy generation, use, voltage, and frequency may be found. The battery management system is vulnerable to hackers due to the communication channel used by existing battery-integrated grids to convey charge status. Batteries that are

overcharged or undercharged could become worthless as a result of cyber risks [3]. Figure 1 shows the components of a power grid that houses electrical support systems.

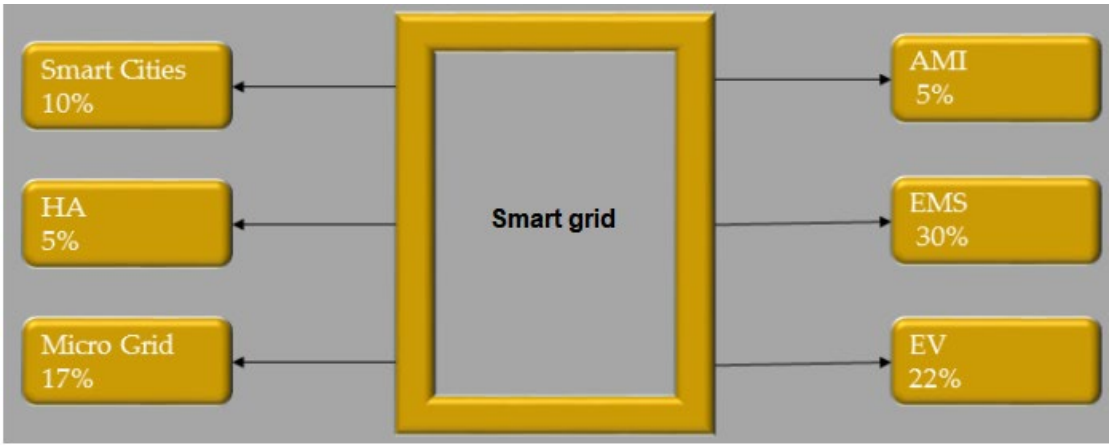

Figure 1. Components of a power grid that houses electrical support systems [2,3].

The smart grid has many benefits over traditional grids, such as better power quality, self-healing, cost-effectiveness with the integration of renewable energy, adaptive energy generation, more environmentally friendly operation, aggregation of distributed energy resources, real-time energy consumption monitoring at the customer end, integration of AI models to automate tasks, remote energy motoring, rapid response to faults, remote fault location. Smart grids are more attractive than conventional grids because of these benefits. The two most important problems are complexity and cybersecurity. It is more challenging to fix these vulnerabilities when smart grid data is stored on the cloud [4]. In addition to physical security, cybersecurity is a crucial element of the smart grid since it ensures its dependability and safety at all times. Not only are smart grids required to have cyber security, but [5] also shows that non-smart and older grids are susceptible to hackers. This study, shown in [5], shows how the power grid is affected when criminal software manages the whole power consumption of computers, including the CPU, GPU, hard drives, screen brightness, and laser printers. The study found that 2.5 to 9.8 million illnesses can potentially upset the system. Another study [6] found that when an attacker gains access to the IoT botnet for high-power smart appliances, it can lead to frequency instability, line failure, and increased operational costs. These kinds of attacks have the power to cause widespread shortages by manipulating energy consumption. As the grid's complexity rises, the likelihood of issues increases. Power networks, which are already noteworthy in and of themselves, are undergoing considerable changes due to the development of renewable energy sources, quick signal processors, and sophisticated sensors. These changes are severely disrupting the industry. These modifications have a considerable impact on the grid. Due to the existing situation, electricity producers and consumers must share information in both directions. A smart grid, which can dynamically monitor and regulate energy flow to deliver constant electricity for clients, is replacing the existing power infrastructure [7]. Data from research that have been published that deal with SG are shown in Figure 2.

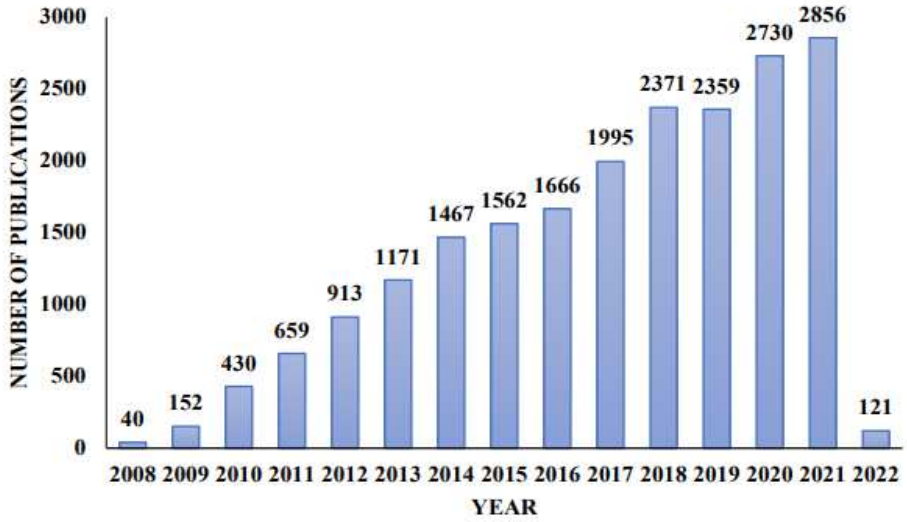

Figure 2. Publication statistics on SG [8].

Table 1. Existing Surveys Related to the Cyber-security of Smart grids.

References	Cyberattacks	Objectives
[10]	Multiple cyberattacks were launched targeting the CIA computers and the five OSI communication layers.	The various forms of cyberattacks and the over-all necessity of taking prevention achievement. An analysis of multiple cyberattacks, including the requirements for their protection, as well as the directions for the future.
[11]	Analysis of traffic, social engineering, scanning an IP address, scanning a port, scanning a vulnerability, worms, denial of service attacks, forward data thefts, replays, violations of privacy, and DDoS.	Cyber-physical security of smart grids and potential attack scenarios based on information technology. Methods of prevention and detection, as well as the difficulties involved, concerning the threats posed by smart grids.
[12]	Attacks against the generation system, attacks against the transmission system, attacks against the distribution system and the client side, and attacks against the electrical market.	Critical cyber-physical attacks and the various ways to defend against them. Investigating the effects of combined cyber and physical attacks on smart grids.
[10]	DoS/DDoS attacks	The smart grid and all of its core elements. Methods now in use for various communication protocols and their underlying systems Attacks of the DoS and DDoS variety, and the effects they have on smart grids.
[13]	Some of the hacking techniques covered in this article are traffic analysis, social engineering, scanning IP addresses, monitoring ports, scanning vulnerabilities, worms, Trojan horses, DoS, FDI, replay, privacy violations, integrity violations, backdoors, MITM, jamming, popping the HMI, and masquerade.	Major cyberattacks against the smart grid and the effects have various security approaches to solve the cyber-security problem in smart grids.
[14]	Various forms of online attacks on confidentiality, integrity, availability, authorization, and authenticity.	The most commonly encountered challenges when dealing with smart homes and smart grids. A variety of cyberattack situations, each with its unique defensive measures. Strategies to protect against or avoid the occurrence of cyberattacks.
[1]	MITM, jamming, FDI, spoofing, DoS, malware, replay attacks.	Multiple cyberattacks have been directed at smart grids and the security systems used.
[15]	Attacks of various forms launched against energy corporations, renewable energy resources, and metering networks.	Vulnerabilities in the traditional electricity network that cyberattacks can target. In the case of smart grid metering networks, security, and privacy criteria must be addressed research in the future, including its trends and problems.

Machine learning, deep learning, Data mining, evolutionary algorithms, fuzzy logic, and other similar techniques are all included in artificial intelligence. Machine learning is becoming increasingly important to researchers for danger detection. The authors of [16] used machine learning methods such as random forest, support vector machine, and neural networks to recognize jamming attacks. Their numerical tests show that the suggested random forest strategy works well. The authors employed machine learning techniques to identify social engineering attacks. The system uses unsupervised learning, so it doesn't need to be familiar with cyberattacks to recognize them. The authors examined different machine learning applications' accuracy, speed, and consistency. They discovered that support vector machines outperform competing strategies using computer simulations [17].

The authors of [18] used machine learning methods to protect against network-layer brute force attacks on the Secure Shell protocol. The authors developed scalable detection models with the help of classifiers like K-Nearest Neighbors decision trees and Naive Bayes that may be effective at making predictions. The author of [19] describes a different experiment that utilized machine learning. The idea of "first difference" from statistics and economics inspired the authors of this study to develop a classifier that can identify dangers to network time synchronization. They found that Artificial Neural Networks outperformed traditional techniques for detecting network security issues. An ANN model was used to identify MITM assaults, and the authors noted a high detection rate. The authors of [20] used machine learning techniques to identify and remove hackers from smart grids. The simulations conducted for this study showed that the suggested approach might have a high detection rate.

Deep learning has also been used to track cyberattacks on the smart grid. For example, the authors of [21] created a deep neural network and a deep learning ensemble technique based on decision trees. Ten-fold cross-validation was employed to assess the model. The evaluation results show that the suggested model beats the most effective methods currently available, such as random forest, Ada Boost, and DNN [22].

Cyberattacks on the smart grid can potentially be discovered through data mining, a type of AI. The authors of [20] discussed past research that used data mining techniques to spot fake data injection attacks in smart grids. These methods allow you to explore data patterns that you usually wouldn't be able to see and find ways in vast amounts of data. In [23], the authors used the data mining method known as Common Path Mining to find FDIA in their networks. To describe how the samples were arranged, they chose to use the idea of a "route." Every unique incident has a different course that has a wide range of flaws. A sequence is considered an attack if it fits within one of the paths. A Casual Event Graph can be used by the authors of [24] to identify FDIA in smart grids.

The training of historical datasets is the primary goal of the data mining techniques used hereafter; training is finished, and data-mining algorithms may have low computational complexity depending on the volume of the data, which helps try to identify FDIA in a smart grid. Fuzzy logic-based techniques for spotting network breaches have also been developed. For example, the developers of [25] constructed artificial immune systems that recognize dangers like network flooding using fuzzy logic. Fuzzy logic is used to discriminate between illegal and legal traffic. The authors present a fuzzy logic-based technique for pinpointing jammer attacks. This serves as yet another example of how fuzzy logic can be used to identify cyberattacks. This method uses the precise channel evaluation, the low packet ratio, and the received signal intensity to ascertain if the connection loss was due to jamming. They had some perfect ideas for intermittent and persistent jamming.

Fuzzy logic was combined with other methods [26] to recognize different cyberattacks. Another crucial AI-based way is evolutionarily based algorithms. They are widely used for global advancement. Well-known evolutionary algorithms include genetic algorithms as examples. This kind of program can simulate how evolution and natural selection work. A genetic algorithm-based technique with two steps—training and detection—was proposed by the authors of [27]. They used a genetic algorithm in their research to remove all but the essential components of the detecting process. The authors conclude that this tactic works

well for various network intrusions. The authors of [28] examined the potential effects of genetic algorithms on various machine-learning approaches. The simulation results show that genetic algorithms and the other three machine learning methods can identify FDIA. Figure 3 shows different components of the smart grid.

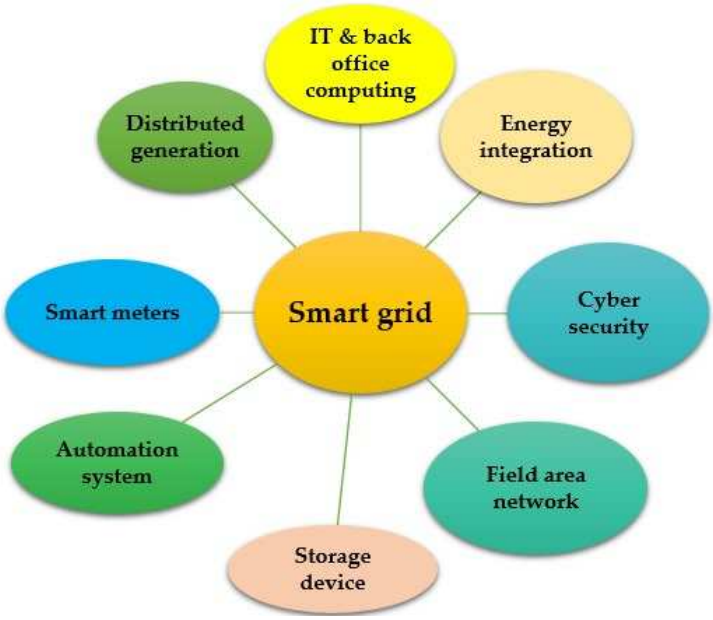

Figure 3. Essential components of the Smart grid [29].

Advanced metering infrastructure is essential to intelligent grid architecture. The primary purpose of AMI is to measure the energy consumption of integrated appliances and other devices, such as solar panels on roofs, gas meters, smart appliances, and water heaters. The smart meter, data concentrator, and central system are all constantly communicating with one another as part of AMI [30]. The meter data management system receives data from electricity meters via the AMI host system. MDMS is in charge of organizing and analyzing the data that utility systems send to it. Utilities and service providers can save costs and improve service quality due to the AMI system [31].

A Process Control System called SCADA enables the real-time monitoring, measuring, and analyzing data from the power grid. However, SCADA can also guarantee connections over short and long distances, making it ideal for installations [30]. The three main parts of this system are the Human Machine Interface, Master Terminal Unit, and Remote Terminal Unit [32]. There are three parts to the remote Terminal Unit. The first component has data processing capabilities, the second component has logic program execution capabilities downloaded from the MTU Master Terminal Unit, and the third component is primarily in charge of network configuration [33]. Another element of SCADA that assists in controlling and keeping track of the RTU is the MTU. The system's final element, the HMI, gives the SCADA operator a graphical user interface. Demand Side Management is a crucial part of the smart grid. This system regulates residential energy use. Demand Side Management can improve power market stability by balancing supply and demand [34]. Demand-side management has several benefits, including improved short-term reliability, lower peak-to-average demand and power supply ratios, cheaper user bills, and lower production costs. The stretcher of paper is shown in Figure 4.

Figure 4. Structure of the paper.

Table 2 shows the list of abbreviations.

Table 2. List of abbreviations.

Abbreviations	Full Form	Abbreviations	Full Form
P.M.U.s	power monitoring units	N.I.S	National Institute of Standards
A.I	Artificial Intelligence	A.M.I	advanced metering infrastructure
W.A.M.R	wireless asset management relay	IoE	Internet of Energy
S.G	Smart grid	E.I	Energy Internet
S.S	Smart system	IoT	Internet of Things
S.H	Smart House	D.O.E	Department of Energy
E.V	Electric Vehicle	EISA	Energy Independence and Security Act
I.G	Intelligent grid	NASPI	North American Synchro Phasor Initiative
N.E.T.L	National Energy Technology Laboratory	NERC	North American Electric Reliability Corporation
L.A.N	Local area network	EEGI	European Electric Grids Initiative
H.A.N	home-area network	ISGTF	Indian Smart grid Task Force
S.G.M.M	Smart grid Maturity Model	CPRI	Central Power Research Institute's

2. Literature Review

In a multi-energy microgrid, numerous unknowns exist regarding the interactions between renewable energy sources, power demands, and electricity transaction costs. A two-stage, mixed-integer, deterministic, linear programming model of the problem has been developed, and it can be addressed by linearizing constraints and generating and reducing uncertain scenarios. The suggested approach is then tested on a microgrid that uses an IEEE 33 bus distribution network to control energy from various sources [34]. As smart grids replace conventional electrical grids, one of the significant problems that have developed is maintaining the system's safety. However, if the design and supporting infrastructure are created from the initial concept with security in mind, this problem can be solved. Therefore, implementing cyber security is a crucial and additional step. The National Institute of Standards and Technology initially recognized confidentiality, integrity, and availability as the three principles of smart grid security [35]. However, the authors highlighted the importance of accountability for smart grid security in Secrets that are frequently compromised when unauthorized people access private data.

On the other hand, integrity guarantees that data is sent without being changed or deleted. However, accessibility is a critical feature that ensures users access to the system's data in the context of smart grids. People cannot obtain information since it is not available [36]. Accountability assures that the system can be tracked and must be verified by a person, a device, or a government organization, which is essential for the security of the smart grid. Additionally, the recorded data can be used as proof in the event

of an attack to establish the actions taken by each user, including administrators, and to guarantee the accuracy of the data collected from each device [36]. Consequently, adopting the following four rules confidentiality, integrity, availability, and accountability, is the best way to safeguard smart grid systems. Smart grid networks are vulnerable to numerous attacks due to insufficient communication.

AI is widely used in the field of Cybersecurity. The digitization of manufacturing processes is usually correlated with machine learning, natural language processing, and robot-assisted process automation [37]. However, Cybersecurity has long used techniques of a similar nature. Consider the filtering system as an example of how machine learning might be helpful. It has been used since the early 2000s [38]. It is clear that methods have changed through time, and current algorithms can draw much more complex judgments. The digital security of smart grids has significantly improved due to recent AI developments. These improvements enhance the defenses against various threats. The five most common uses of machine learning are security (detection of fraud and viruses), privacy, business, and IT. Most people are unaware of how often artificial intelligence is used. Companies can quickly understand threats due to AI, which speeds up response times and ensures that best security practices are followed. Even while technologies like AI, 5G, and others are on the threshold of helping to resolve these problems, the energy sector must continue to invest to remain ahead of cyberattacks [39]. AI is also used to identify and stop intrusions into computer networks. Deep learning systems can also keep track of user identities if needed. Figure 5 describes the relationship between AI and Cybersecurity.

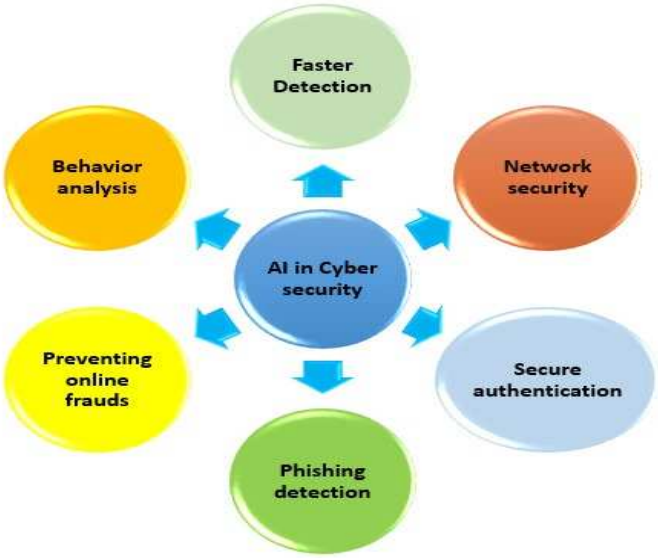

Figure 5. AI in Cybersecurity [40].

The use of databases infrequently or never, frequent location changes, access times, or other anomalies can all be picked up by AI algorithms [41]. Machine learning, in contrast, makes it easier to find data patterns that enable automated learning [42]. Utilizing cyber threat knowledge, smart grid users can quickly and effectively fix problems. Although today's security systems are perfect for identifying and stopping common threats, they cannot keep up with the growing need for Cybersecurity. None of these methods can contain zero-day vulnerabilities, an extremely slow cyberattack. A more flexible approach is needed to investigate data sets and find hidden security problems [43]. Machine learning has shown to be quite capable of identifying threats that were not there before using adaptive baseline behavior models. The security landscape would drastically change when predictive analytics and machine intelligence are combined with known and unknown data sets [44]. Table 3 illustrates how AI can be applied to strengthen security.

Table 3. Summary of AI Methods on smart grid.

AI Technique	Advantages	Disadvantages
ANN	AI methods are more complex to understand than artificial neural networks. A multi-step process known as information technology is used to analyze data and look for a potentially unexpected pattern. It works with a range of teaching techniques [45].	It has a higher computational cost and tends to overload. The model creation process is based on empirical research [45].
SVM	Control parameters in ANN keep the model without being too accurate. This works best when there are apparent differences between the groups in the data set. The kernel technique makes it quick and easy to become an authority on a particular subject [46].	Large data sets are too complicated for this method. Using this method when there are overlapping categories is not practical. Testing is a slow process [46].
ANFIS	By combining the learning capabilities of an ANN with fuzzy systems, a neuro-fuzzy system may automatically create fuzzy if-then rules and optimize their parameters. This fixes the fundamental problems that have prevented designing fuzzy systems up to now [47].	Depending on the number of fuzzy rules that were initially used. More calculations must be done as unclear regulations are added.

One of the most popular ways to attack a smart grid is by jamming. An attacker can block communication by sending out constant or irregular signals. The operation of the smart grid network may be affected by various jammers [48], including continuous, random, misleading, and reactive jammers. Attacks known as "flow-jamming" use several jammers distributed throughout a network to slow down or stop normal traffic flow. Information is taken from the current network layer for these attacks. Jamming can be an extremely powerful strategy when used against a weak opponent. With centralized management, the jammer may be set to use just the right amount of power to stop a specific packet [49]. In a non-centralized jammer model, each jammer shares information with neighbor jammers to maximize efficiency. As a type of attack, spoofing attacks can be harmful to smart grid networks. These "spoofing" attacks fall under this category and include MAC spoofing, ARP spoofing, GPS spoofing, identity/data spoofing, and others.

A spoofed creates a fake grant in any of these attacks to deceive other nodes and damage the network's security, dependability, stability, and operation, which can compromise the integrity, confidentiality, and accountability of the smart grid [7]. Attacks can be launched against the network layer, the data link layer, and the physical layer. Injection attacks can happen when an attacker tries to remove, change, or add new data to a network, claim the authors of [50]. This might interfere with the smart grid's functionality and lead to a blackout. This cyberattack also corrupts data, compromises data integrity, and introduces malicious nodes into the network. Unlike earlier assaults, injection attacks might target the transport layer, the network layer, or the data-link layer [50]. A flooding attack is another hack that can be used against smart grid networks. This attack may limit system access at the network or application layer [51]. The target can expend all of its resources processing the fake messages sent to it. Another effect of this attack is that individual nodes cannot join the network. Man-in-the-Middle attacks on the smart grid are another type of cyberattack. The session and network layers are these intrusions' targets [52]. A man-in-the-middle attack happens in a smart grid when an attacker physically placed between two authorized devices connects to and sends communication between them. While the devices seem to speak, the attacker includes a third device in the conversation. These attacks' main goals are to interrupt network activity, change data while it is being transmitted, or obtain unauthorized access to sensitive data [53]. The security and privacy of a network may be risked if MITM is used. Social engineering is another cyberattack that could be used against smart grid technology. These attacks aim at the application layer and potentially risk the system's privacy [54]. According to the authors, social engineering is the greatest threat to information security. They explored social engineering techniques such as rob calls, phone/windows fraud, and reverse social engineering. Each of these attacks aims to trick victims into disclosing private information. These risks put users at

risk of having their personal information stolen for impersonation purposes, which can reduce their sense of security. A well-known passive attack on communication routes for smart grids is listening [54]. It goes after the network layer and affects the smart grid's specific privacy requirements. According to the attacks occur when a malicious user listens in on a conversation between two nodes on a LAN network to gather information. A user could use this sensitive data maliciously to interfere with the network. These assaults compromise the network's security.

A smart grid's physical and data link layers are known targets for timing-sensitive attacks [55]. The TSA is capable of managing, monitoring, and protecting large regions and 3-phase measuring devices. Synchronized measurements are required for numerous smart grid applications, and the vast majority of measuring instruments now come standard with GPS to provide accurate time information. These are vulnerable to spoofing attempts, just like other GPS-enabled devices. Smart grids require quick communication and control signals, making them more susceptible to cyberattacks such GPS spoofing and time-sensitive access [56]. By using hybrid brute force, reverse brute force, and credential stuffing, the presentation layer, session layer, or network layer can be compromised. Figure 6 shows the Cyber-Attack Classification.

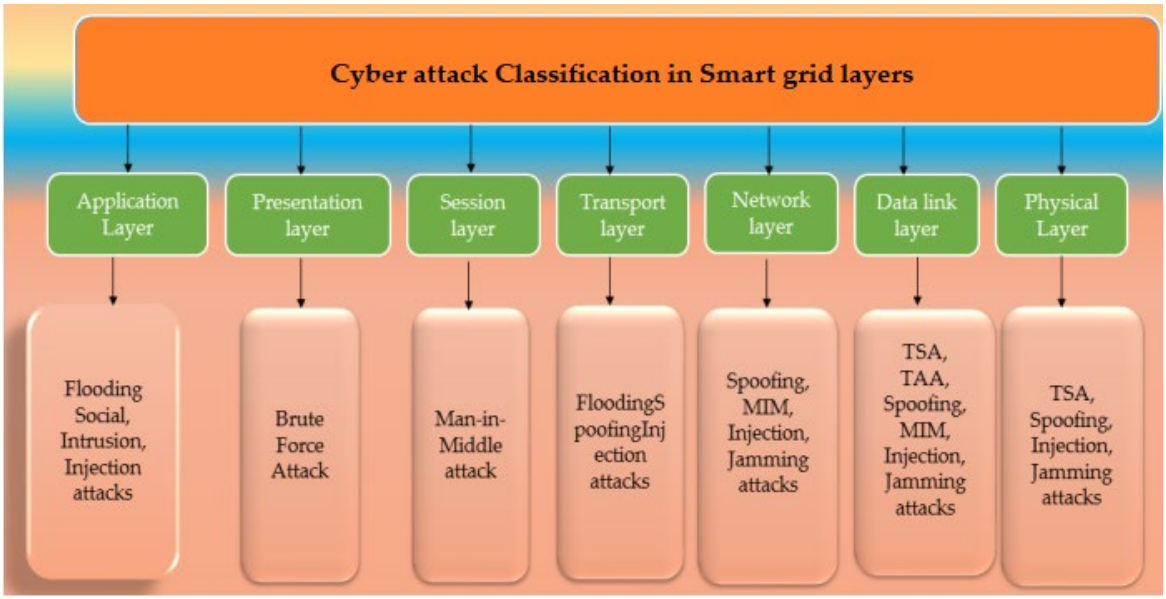

Figure 6. Cyber-Attack Classification Based on Communication Layers [10].

A "password guessing attack" is when an attacker attempts to guess or decode a user's username or passphrase to access the user's account or system. The authors of [57] explored the effects of attacks, including unauthorized access to the system and user accounts and the use of security flaws to reduce the system's privacy and dependability. An attacker can use a brute-force attack to get private data about smart grid users [24]. Another type of cyberattack on the smart grid is intrusions, in which an attacker takes advantage of flaws in the network to gain unauthorized access to nodes. Therefore, improper behavior, such as using force or making threats, may result in an invasion [58]. By interfering with the network's security and privacy at both the application and network layers, it also wants to waste network resources. The relevance and sensitivity of the smart grid make it especially vulnerable to intrusion attacks that could compromise the security of its network. Due to problems with authentication and integrity, modern SCADA systems, including smart grids, are becoming more vulnerable to cyberattacks like infiltration. Therefore, the network will function more effectively, and system downtime will be decreased if this attack can be located and halted. Traffic analysis attacks occur when an attacker listens to conversations and analyses what they hear. This attack aims to take over computers and other smart grid devices. The data connection layer is the target of this kind of attack [59].

Additionally, it may reveal confidential network data. In this attack, the assailant can listen in on conversations and analyze them to learn how network nodes converse with one another. Another well-known cyberattack on the data link layer of smart grids is the masquerade attack. This attack puts the security of the network's confidentiality, availability, integrity, and accountability at risk. To access a network or carry out illegal activity, an adversary could pretend to be an authorized user. To reduce the energy used by a home's electronic devices, an attacker usually alters a Programmable Communicating Thermostat in a smart grid [60]. Manipulating smart meters is one of the most common ways to undermine the smart grid. An attack at the physical layer can risk the security of a network. The information sent to any client can be changed in case of an assault on a smart meter. The consumer may pay more or less for electricity, depending on the results. Cyberattacks like buffer overflow, which require sending data to specific systems and components, are becoming more common in the smart grid. Concentrating on the application and transport layers also decreases network availability [61]. Because it could lead to a system crash and consume all network resources, this exploit should be avoided. Table 4 shows the Cyber-Attacks in Smart grids.

Another well-known smart grid vulnerability is the dummy attack. To attack the network layer, it makes use of network availability. The AMI network of the smart grid is penetrated by this attack, which takes advantage of a flaw in the Dynamic Source Routing protocol. As a result, storage space on our communication systems can become limited. One of the most noticeable effects of this attack is a 10–20% reduction in the number of packets that can be transmitted [62]. Targeting the smart grid in a hack known as an "IP spoofing attack" can also be used to decrease network accessibility. This kind of attack slows down and affects the person and the network's processing power in addition to hitting a single smart grid node. An attacker could use the broadcast address of the bounce site to deliver counterfeit packets from the source site. The bounce site may send incorrect packets to all hosts if it gets them. The approach can cause the target network to become overloaded. The network layer is the primary target of this kind of attack [63]. The HMI attack is a form of malicious online behavior that might result in a lack of the smart grid. In this case, the attacker uses a standard device attack (weaknesses in the operating system or software of the device) to get remote access to the server from their computer. The attackers' goal is to take total control of the machine that is being attacked. Infrastructure for smart grids and substations is managed and automated by SCADA devices, which could have security flaws. This attack necessitates little network expertise because the device's documentation is accessible. A hacker can easily take complete control of a compromised machine. The application layer's responsibility, availability, and integrity are all at risk [64].

Because it enables utility companies, customers, and producers to communicate automatically and in both directions via smart grid networks, advanced metering infrastructure has grown to be a critical part of the developing smart grid industry. Smart meters are high-tech devices that, in contrast to conventional meters, record a variety of information about a person's energy use, energy production, energy status, and diagnostics [65]. For purchasing, managing and watching user appliances, and troubleshooting, this data is really helpful. These data transfers all take place across a wide area network and are all kept in data centers that are hosted in the cloud. A centralized system may result in problems including a single point of failure, the potential for manipulation, and the loss of sensitive data. Performance, availability, and response time may be affected if more users connect to the same server. Smart meters and electric vehicles in smart grid systems also save a lot of information about payments and energy use [66]. These details and data are frequently disseminated to other businesses for monitoring, billing, and trading. Sharing a lot of data in such a complicated system; however, offers major privacy problems since middlemen, intermediaries, and trusted third parties might divulge private data on identities, locations, patterns of energy output and consumption, energy profiles, charging, or discharging quantities. The situation is made worse by the mistrust that exists between consumers and manufacturers. Because of this, it could be challenging for centralized parties to win

the trust of producers and customers by being truthful and open. It is a difficult effort to develop a decentralized AMI system that is dependable, private, and safe. Research on AMI and blockchain.

Table 4. Cyber-Attacks in Smart grids [14].

Cyber-Attack	Objectives	Layers	Impacts	Security Requirements
Jamming Attacks	The main objective is to create trouble with both the data transfer and the data receiving.	Physical Data Link Networks	To prevent the sending and receiving of information collisions by blocking one or more nodes.	Availability
Spoofing Attacks	Trying to trick an authorized node into getting unauthorized access to the system	Physical Data Link Network Transport	Trying to mislead other nodes in the network.	Integrity Availability Confidentiality Accountability
Injection Attacks	The practice of inserting false or untrusted data packets into a network.	Data Link Network Transport Application	It injects false data perverting legal procedures and business activities with corruption the appearance in the network of nodes not authorized to be there.	Integrity
Flooding Attack	The main objective is to Bring about the loss and destruction of system resources.	Data Link Network Transport Application	In a network, failure of individual nodes and loss of availability of resources.	Availability
Man-in-the-Middle Attack	It blocks or alters the flow of data while it is being transmitted over the network.	Data Link Network Session	Access to confidential information that was not allowed.	Integrity Confidentiality
Social Engineering Attacks	Using fraud to encourage people to provide confidential information	Application	The users' right to privacy was violated. The system may suffer either temporary or permanent damage. Take confidential and sensitive information without permission. Theft of personal identity	Confidentiality
Eavesdropping Attack	Following up on and recording every bit of network activity	Physical Network	A violation of somebody's security	Confidentiality
Intrusion Attack	Acquire access to the node or network in an unauthorized manner.	Network Application	To Misuse the resources that are accessible on the network.	Integrity Confidentiality
Brute Force Attacks	Cracking user names and passwords requires a lot of work.	Session Presentation	It is obtaining access to a user's system or account without permission.	Integrity Confidentiality
Time synchronization Attack	Attacking the timing data and causing the nodes to lose their time synchronization	Physical	Events that compromise security, such as location estimation and fault detection, Performance decrease.	Integrity Availability
Traffic Analysis Attack	Execute command over the computers and other electronic devices linked to the network.	Data Link	Detect the message and analyze it to obtain information about the communication patterns between the nodes.	Confidentiality

The authors in [67] offers a paradigm in which the authors use blockchain technology and smart contracts to improve the security and dependability of the smart grid. Both energy buyers and sellers will profit from the contracts' capacity to serve as a middleman. Productivity will rise, costs will drop, and the system will be safer as a result. After a transaction, a smart meter connected to the blockchain will submit the record, adding a new block to the distributed ledger with a timestamp that may be used to verify the data. The customer's bill can then be determined using the ledger information. The book's main issue is that it doesn't provide enough technical information.

In order to achieve decentralization and autonomy, a demand-side management paradigm for intelligent energy networks is described in [68]. This architecture creates a decentralized, secure, and autonomous energy network using blockchain technology, allowing each node to function independently of the others and the DSO. In addition, it is utilized to safely store the data blocks that smart meters collect about energy consumption. By establishing a prototype on the Ethereal blockchain platform using energy consumption and production traces from UK building databases, the method is finally assessed and confirmed. The findings show that this model is able to take into account different levels of energy flexibility and validate every demand response agreement in a manner that is almost real-time. Uncertainty exists over the energy profiles' anonymity in an open-source blockchain. The user can be identified by looking at transactions that are available to the public.

Security, privacy, and trust are three of any system's most important components. The similar level of security will be necessary for future intelligent grid systems [69]. This is sure that no unauthorized entity obtains information by putting in place the necessary cryptographic safeguards.

The most popular use of blockchain technology to date is Bitcoin. This is due to Nakamato's invention of a novel consensus technique in [70], which made it possible to create trust in distributed systems. A cryptographically secure data structure, a digital signature method, a time-stamp, and a numerous benefit are used in addition to the consensus process. Consensus mechanisms, for instance, are commonly used in blockchain applications to establish credibility. To handle fundamental security issues including privacy, integrity, authentication, authorization, non-repudiation, and anonymity, a variety of cryptographic approaches are used. It is not necessary to build a cryptocurrency in order to develop a blockchain-based decentralized system, even though coin applications are where the principles of consensus mechanisms and blockchain are initially exposed [9].

Nowadays, centralized platforms are used for a number of services by smart grid components such billing and monitoring, bidding, and energy trading. Although these technologies are advanced and work well, the existing smart grid system still has a number of important problems. As was already said, the smart grid also makes it possible to connect various RES, consumers, and cyber-physical systems. The grid's architecture is changing from a centralized, fully automated network to a decentralized, fully automated network as a result of the need for better interoperability. The EI idea is assisting in the transition in the smart grid industry from a producer-controlled network to a high-end decentralized network [68].

The decentralized nodes of the network all agree regarding what is happening, guaranteeing that the blockchain always works as intended.

Many times, the peers in this network are able to carry out tasks like approving new members and keeping the network running without the aid of a centralized authority. The blockchain's network capacity grows as more computers join it on its own. The blockchain is a decentralized network that is mostly controlled by its users, which explains this. The blockchain is a safe but unreliable network because nodes can connect with each other without the help of a reliable third party and because all data and transactions are encrypted asymmetrically [71].

Blockchain differs from earlier systems that demanded constant trust in those in authority.

The data in the blocks cannot be changed until a majority of users oppose it because blockchain technology uses cryptography and keeps a shared global record across all nodes.

The immutability of the blocks and the validity of the contents may both be independently confirmed by nodes on the blockchain network [72]. As a result, the blockchain's architecture is incredibly transparent and reliable. Any node on the network may check the legitimacy of the blocks with this level of openness without requiring access to confidential information.

3. Methods and Materials

3.1. Research Method

The literature on IoT Security studies has grown in recent years as more and more academics have developed an interest in the field. With the use of the AND OR search operators, we were able to find a vast amount of information that was relevant to topics like "IoT", Machine Learning", Deep Learning", threats, "cyberattacks", and "vulnerabilities". We have also included other terms like "blockchain", healthcare", and "Data Mining. ML and DL" in our search for a solution to the issue of IoT security breaches.

3.2. Exclusion and Inclusion

IoT and machine learning approaches were used as a keyword string to find publications in databases from the IEEE, Springer, Scopus, Google Scholar, A.C.M., Science Direct, and Wiley. These works include research on machine learning categorization, IoT security, and integration of health systems. Papers that were first chosen for review are peer-reviewed before being published. To better understand how machine learning works and how it might be used to improve IoT security, this research explores publications that concentrate on machine learning-based approaches. After the initial search, any papers found were discarded. We only looked at a few articles because the review aimed to set standards for machine learning research criteria and methodology. The committee did not even read the additional recommendations.

3.3. Objective of the Study

Our main objectives of the study are.

1. To know about the smart grid and its security issues.
2. To know about the different types of attacks on smart grid.
3. To know about the different methods to overcome these issues.
4. To know about the Open Issues, Challenges, and Future Research Directions.

3.4. Smart Grid Communication Challenges

The Smart grid Communication Challenges are explained below.

3.4.1. Interference

For the smart grid to work, smart meters must be installed in homes and businesses. In the typical household, more and more technologies are becoming standard. Nowadays, H.A.N.s are almost ubiquitous in homes. Under conditions of dense distribution, Network Area Controllers and smart meters may interact. This might result in inaccurate readings from smart meters, endangering the system's stability. Power line harmonics may cause communication equipment on the smart grid to malfunction.

3.4.2. Transmission of Data Rate

The smart grid's communication infrastructure is essential for various reasons, some of which are the collection and analysis of data and the distribution of instructions to the system's numerous nodes. On the other hand, the smart grid necessitates an abundance of real-time sensors as well as smart meters, both of which, when combined, generate a substantial quantity of data that has to be sent rapidly while maintaining its integrity. In

addition, the foundation for mutual comprehension has to be created. Because of this, the smart grid requires a network connection that is both reliable and secure.

3.4.3. Regulation

A wide variety of different parts come together to form the electrical Grid. The smart grid relies on the interplay of many other factors, each of which plays a specific role. A well-integrated communication channel network is crucial for adequately constructing such a system. This has resulted in a proliferation of global initiatives aimed at standardization and developing generally accepted standards. These efforts have the backing of various institutions, including the IEEE, the European Committee for Standardization, the American National Standards Institute, and the International Telecommunication Union.

4. Results

4.1. Cyber-Attacks and Security Risks

It is common to see attacks, including who's conducting them, which system vulnerabilities are being used, which security gaps are being targeted, and the outcomes of the attack s possible risks. These are all important considerations that need to be considered [73]. When there is a risk to the confidentiality, integrity, or accessibility of data, systems, or other resources, a security flaw occurs. Each cybersecurity event offers a different threat to an individual or organization's systems and networks. Commonly referred to as "malware," malicious software is computer code created to harm a user's computer, server, or network [74]. Malware can enter a system by taking advantage of a security hole, such as when a user accidentally installs spyware by opening a malicious attachment or visiting a compromised website. Usually, the system's actual user won't be aware that this malicious program is present. Malicious software can easily access a system since there are many different ways to do it. A user may be deceived into installing malware by accessing a fake version of a valid file, going to a website known to spread malware, or connecting to an infected system or device. Another situation is when someone views malicious websites and is deceived into installing them. Any computing device is vulnerable to being infected by malicious software. Cyberattacks can target process control systems like Supervisory Control and Data Collection systems, end users, servers, and the hardware that connects them. Like the people it hurts, malicious software comes in various shapes and sizes. Examples include bot executables, Trojan horses, spyware, viruses, ransomware, and worms. Unhealthy programmed are constantly evolving and getting more complex [75].

The most cost-effective way to make long-term savings is to install efficient controls at the system's boundaries. A detection and prevention system is one type of this technology (firewall, anti-virus software). Using a security barrier, administrators can limit user access to a protected internal resource. Despite these safeguards, it is still possible for someone to misuse their access credentials. The degree of the misbehavior will determine whether a corporation uses a punishment from its accountability policy. Regrettably likely, comprehensive security strategies, access control techniques, and accountability mechanisms won't work [76].

The idea behind the Internet of Things is that everyday things may communicate with one another and other computers via the internet without the need for human interaction. Fires, break-ins, overheating, and door locks that unlock as someone approaches can all be detected and prevented with the use of Internet of Things technology.

The Smart workspace system, which makes use of Telegram messengers and the on-hand AI Chabot, is made to make it easier for employees to use electronic devices at their workplaces. Remote management is possible for the office's technology [77]. Additionally, the Chabot can inform staff members whether a device can be turned on or off or remind them to turn on the fan if the temperature rises too high. By enabling workers to manage all office technology from a single internet-connected device, such as a smartphone or laptop, the Internet of Things and artificial intelligence in the workplace can help employees save money on utilities and time.

The number of people using the messaging programmed Telegram Messenger is growing. There are 62 million active Telegram users right now, 15 million DAU, and 1 million new users join every week [78]. Since Telegram Messenger can be used with or without a smartphone and can also be accessed through a web browser, many people use it every day to connect with family, friends, and coworkers.

The term "smart grid" describes a power system that makes use of sensing technologies, communication, digital control, information technology, and other field equipment to coordinate its current operations and improve the efficiency and responsiveness of the power grid. The Photovoltaic Generation System may be tracked and measured with the help of the Internet of Things, and the WSN in particular [79].

The Internet of Things has also been utilized in agriculture to find farming-friendly places so that the correct plants can be planted [80]. IoT is used in medical to track heart rate.

It is feasible to build Smart door locks with Mobile Backend as a Service and home automation and smart security systems with Low Cost Real-Time [81] using an ESP 8266, a straightforward and affordable Internet of Things key.

Researchers in a range of fields are interested in neuro-fuzzy systems because of their better learning and reasoning capabilities. In neuro-fuzzy systems, the representation of implicit information via fuzzy inference systems and the ability of artificial neural networks to learn from their experiences are merged. Because of the speed, accuracy, and difficulty of creating computers, researchers have thought about using soft computing techniques to characterize, forecast, and manage dynamic nonlinear systems. Fuzzy logic systems and artificial neural networks are examples of soft computing techniques. To address critical difficulties, a number of research and engineering sectors are starting to combine the two schools of thinking. An intelligent machine's ability to reason and draw conclusions can be greatly enhanced by fuzzy logic. Fuzzy logic describes qualitative yet flawed data, allowing machine learning to be symbolically expressed. Neural networks are used because they can learn, are reliable, and offer a lot of parallel to a system. The neuro-fuzzy system is a great place to start when trying to solve machine learning problems because it can represent knowledge and self-learn. The Takagi-Sugeno-Kang fuzzy inference method is the most effective way to represent nonlinear dynamic systems. As a "multimodal" technique, TSK system modelling can use linear sub models to show how a complex nonlinear dynamic system behaves as a whole. One of the most well-liked neuro-fuzzy methods is ANFIS. Regression, modelling, forecasting, and control have all used it. The ANFIS utilizes a fuzzy inference system of the TSK type on a 5-layer network design. The two types of parameters in ANFIS are assumption and consequence. The relationship between the two groups of variables is described using fuzzy if-then rules. The biggest problem with ANFIS is that it uses a lot of computer resources and frequently produces models that are unnecessarily complex for even the most straightforward problems. The accuracy and training time of standard neuro-fuzzy networks have recently increased due to recent developments in learning algorithms and network architecture. A neuro-fuzzy system needs the following qualities to perform well: Positive qualities include one that can learn quickly, adapt on the fly, continuously optimize itself to attain the minimum possible global error, and use the least amount of computing power possible. Because hybrid techniques are used to continuously good them, most neuro-fuzzy inference systems take a long time to learn. On occasion, it's necessary to manually change some parameters. On the other hand, overfitting and local minima are easily induced by diffusion learning methods. While the input weights and hidden layer biases are chosen at random and can be thought of as a linear system, the output weights of ELM are determined using a straightforward generalized inverse operation. as opposed to the norm. Most CPSGs rely on wireless communication, it is simple for enemies to target that channel. Information technology attacks are those that limit access to data. Classical Intricate attacks operate on communication networks such as cognitive radio networks and mobile Adhoc networks [82]. By blocking trusted routing, these attacks slow down the network by taking advantage of infected insider nodes. A faulty sensing node may post inaccurate channel sensing data following an attack, which

is advantageous to the node but harmful to more reliable nodes. Intricate attacks are typically used by enemies for two reasons. The main goal is to stop criminal damage, which happens when untruthful people claim a channel is empty when it's actually in use. The second goal is exploitation when sensing indicates that a channel is not being used. This happens when an attacker makes up a busy signal to try to use a channel exclusively. Attackers can increase the efficacy of their attacks by giving priority to these goals [83]. The flaw in the aurora generator was found by the Idaho National Laboratory. By using a series of improper control commands, the attacker tries to open and close the circuit breaker on a generator in this type of attack. The disconnecting of the generator from the utility grid is referred to as interruptions. When the system and generator lose synchronization the safety mechanism can react, the Aurora Assault's goal is to reclose the circuit breaker. The aurora attack alters the generator's electrical output and rotational speed, which causes physical damage. This is due to the safety features of the generator being purposefully delayed to prevent accidental tripping. Closing the circuit breakers could be harmful to the generator because of the difference in frequency and phase angle between the generator and the main grid. Which circuit breakers are most vulnerable to Aurora attacks can be determined using a score method using vulnerability rating variables. Modeling and research into the effects of an aurora attack on the PCC and synchronous generator breakers of the micro grid may be found in [84]. Sync-check relays, which were previously used to defend against aurora attacks, are not permitted according to the IEEE 1547 Standard because they have the potential to unintentionally turn a micro grid into an island. The authors showed that tripping a micro grid's main circuit breaker could cause harm to the synchronous generator. The retail industry has recently given demand-response technology, which can enhance the functioning of the electrical grid, more attention [85]. At its core, demand-response demands, response an incentive-based control system in which incentives are communicated through command signals. In [86] simulation of an attacker with the goal of increasing the gap between production and consumption by hacking the transmission channel and changing market prices using an assault time series made the attack considerably more potent. One-shot assaults, in which harmful code is inserted just once, are different from this kind of attack. In [87] Looked at attacks that might insert false pricing information at any point over an extended period of time. Attacks that occur frequently can lead to power imbalances that cause overproduction, financial losses, and poor power quality. The amount of damage caused by repeated strikes was calculated by the authors using a technique called "sensitivity analysis." The authors used a sensitivity function based on the z-transform to model the system's behavior when analyzing its behavior over time. Challenges with energy-exchange systems were looked at by [88]. The end-user network's controllers quickly receive a price signal from the active market, and the network rapidly transmits bid information back to the controllers. Hackers can access the data that is sent between a prosumer and a market agent. The pricing attack was made worse by the insertion of fictitious prices and quantities from prosumers due to the deployment of malware. These attacks caused the market clearing price to fluctuate, each prosumer used a different amount of energy, and the overall demand on distribution feeders decreased. The authors in [88] examined two types of attacks: one that aims to undermine the system's reliability by changing the bid price to extreme values and another that aims to make money over time by keeping the bid price within predetermined limits in order to avoid detection. Prosumers are aware of their maximum bid amount thanks to the service agreement. Signal manipulation can be used by an attacker to get around these restrictions, but their actions will be exposed. Frequency regulation is extensively used in connected power networks. Controlling automatic generation would serve as an example. It guarantees that power moves along the tie-line between control zones at the predetermined rates and that the system's frequency stays within safe bounds. AGC uses data from distant sensors to ascertain a region's frequency and power flow. This enables it to assess how well the area is regulated The ACE shows the discrepancy between the recommended configuration for power exchange and system frequency and the current

configuration. Every few seconds, the AGC generators use the ACE to determine the control instructions automatically. Only a few minutes' worth of measurement validation processes, like state estimation, are carried out, which is insufficient to support the second-level frequency required by AGC. Since there is no way to check or locate the accuracy of measurements, AGC is vulnerable to attack. AGC is highly automated and only needs occasional system administrators' maintenance. When damaged, it can quickly alter how the system works [89].

Some of the most frequent outcomes of malware entering a network include the following:

- It prevents essential network elements.
- To spy using malware itself, it installs extra harmful software.
- It receives information and has access to personal data.
- It interferes with some components, rendering the system unusable for users.

Malicious malware, known as ransomware, has users pay in return for keeping their files from being deleted or denied access. Trojan horses are the most dangerous kind of malware because they can seem to be helpful, popular software while attempting to access sensitive financial information. Such "drive-by" attacks are a common way for malware to spread. The user must act before these records are created. Users only need to visit a secure website for their PC to become silently infected [90]. A compromised user's computer transforms into an Iframe and sends the victim's browser to a malicious website under the attacker's control after being compromised. Phishing is using email corruptly or falsely, for example, by sending spam or phishing emails. The goal is to gain the victim's private information to be used maliciously to access their bank accounts. This extreme threat is frequently used as part of a more extensive operation to gain access to corporate or governmental networks. As a result, it is commonly used in conjunction with other strategies. A type of phishing called spear phishing targets particular people or organizations, including those working in government or military intelligence. Criminals can get private company information through these attacks, which they can use to steal money or carry out other crimes. Whale phishing is spear phishing that targets powerful people, like the CFO or CEO, to gain sensitive data. When an attacker can place himself between two participants in a transaction or conversation, they commit a man-in-the-middle attack or listen in on a discussion [91]. Man-in-the-middle attackers most typically employ the following entries:

- Public Wi-Fi that isn't secure when unauthorized users place their devices in between a visitor's device and the network.
- If an attacker's virus successfully infiltrates the victim's PC, they can install software to obtain the victim's secure information.

IoT is becoming more and more popular because it can be used for a wide range of tasks, including intelligent energy management and industrial automation. At various grid nodes, Internet of Things sensors are installed to guarantee that electricity is transferred efficiently and correctly. IoT-SG integration problems must be fixed for the network to operate as planned. A neuro-fuzzy smart grid energy monitoring system for the Internet of Things is used by the operator's backbone to gather and transmit the parameters of the prediction model. we assess the effectiveness of an SG power monitoring system that is based on the Neuro-Fuzzy Internet of Things. Both customers and energy providers can gain from better resource analysis and management. Artificial neural network and fuzzy systems are combined in the ANFIS to provide a model that incorporates the best features of each. It makes use of a method called "Takagi-Surgeon fuzzy inference". This structure's layers each carry out a certain task and produce an output after processing inputs. The hybrid model combines the iteratively approach and the least-squares method. Any inference system with outputs from linear or constant membership functions can be built using Surgeon-type systems. For modern grids to function properly, the electrical infrastructure needs to be intelligent. Because it addresses the problems that plagued earlier grids, SG is a better and more dependable grid. A power monitoring system that is

enhanced by the Neuro-Fuzzy Internet of Things. Systems for managing solar and wind energy are controlled by the ANFIS smart grid controller. Wind and solar power plants will be able to produce much more energy with ANFIS-based power management. Using load power, current, and voltage as inputs, a Neuro-Fuzzy notion for power monitoring based on the Internet of Things was constructed A network or service must be taken down to stop responding to valid requests via a denial-of-service attack. DDoS attacks typically target the servers of well-known organizations, including financial markets, news organizations, banks, and governments. SQL injection changes database data that shouldn't be accessible to users [92]. A website's search bar is regularly used for malicious ends. This is known as SQL injection. A security flaw that cannot be addressed or that programmers are unaware of is called a "zero-day exploit." Engineers must constantly be on the lookout for this vulnerability. DNS tunneling enables the transmission of non-DNS communications on port 53, including HTTP and other protocols. As a standard and authorized method, DNS tunneling is usually disregarded when used for illegal activities [93]. Attackers can transmit their traffic outside and cloak it as DNS to hide the data they transport via the Internet. Table 5 shows the Cyber-Attacks and Security Risks.

Table 5. Cyber-Attacks and Security Risks.

References	Types of Attacks	Solution
[94]	FDIA	A method based on data-driven ML to identify stealthy FDIA on state estimate.
[95]	FDIA	Consider the notion drift while analyzing historical data, and concentrate on the distribution shift. Dimensionality reduction and statistical testing of hypotheses are used.
[96]	SCA	The data are transformed into a lower-dimensional space using the KPCA approach. The KPCA-transformed data are inputted for the ERT's SCA assault detection system.
[97]	DoS	A multi-class classification technique used in the smart grid for anomaly detection.
[98]	Pulse, ramp, relay trip, and replay attack	Supervised machine learning and model-based mitigation for anomaly detection (AD). The robustness and detection accuracy of the ML model was boosted by physics and signal entropy-based feature extraction.
[99]	FDIA	A CPADS created using ML techniques, network packet characteristics, and PMU. Metrics.
[100]	FDIA	A new FLGB ensemble classifier and optimum feature extraction ensemble learning-based FDIA detection algorithm are used.
[101]	FDIA	Extreme learning machines create a classifier that can identify abnormalities brought on by FDIAs.

Data streams from the control center may be altered by intruders, resulting in incorrect choices that put the whole system in danger. Despite using encrypted communication, the P.M.U. and PDC, two essential components of the smart grid, are still vulnerable to hackers.

Components like P.M.U.s may have problems if a dependable connection cannot be ensured, which makes these problems worse. The selected method of communication has to be able to overcome these obstacles to be successful. The other components must still be able to carry out their intended tasks, notwithstanding the safety precautions that have been put in place. Because of this, measurements made by P.M.U.s, for example, rely on time. These measurements ought to arrive at the data-gathering facility within two seconds. No time must be wasted when a new security measure is implemented. The interconnection of the many cutting-edge and complex technologies that make up the smart grid is another reason for worry—the synchronization of measurements with P.M.U. Data is made possible by the use of G.P.S. The efficiency and dependability of the measures may be compromised if the G.P.S. signal is hacked or interfered with. The measurements collected from the P.M.U. will be worthless due to incorrect time stamping. Figure 7 shows the different types of attacks on the smart grid.

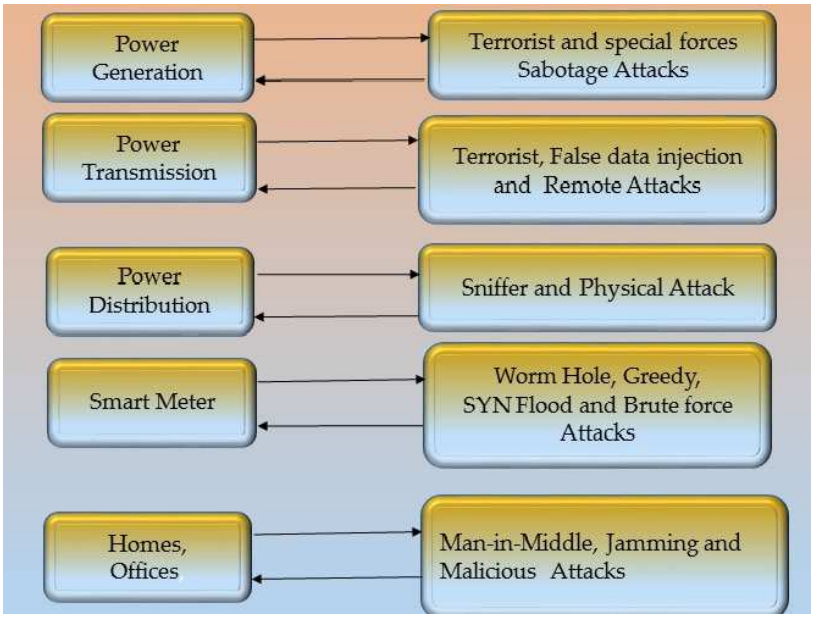

Figure 7. The possible attacks on the smart grid [102].

4.2. ML and DL Algorithms for Cybersecurity

As we'll see below, one of the most popular ways to overcome the limitations of traditional cybersecurity strategies is to use machine learning and deep learning algorithms. These methods can recognize intrusions that target the network in the issue. Machine learning is frequently seen as an essential part of cybersecurity because it can be used to attack and defend. One of these studies [103] looked at different machine-learning methods for identifying security flaws in IT systems. These techniques were random forests, support vector machines, naive Bayes, decision trees, artificial neural networks, and deep belief networks. The three main security challenges of intrusions, spam, and malware were the main areas of our examination.

4.2.1. Support Vector Machine Support Vector Machine

The usage of Support Vectors improves machine learning. The performance of numerous cybersecurity applications has been shown to benefit from the use of support vector machines. SVM is rarely used since it uses many resources, especially in real-time applications. Using kernel changes on the data, SVM establishes the ideal split between samples [104]. SVM transforms data using kernels to discover the best border between pieces. The authors in [105] created a model combining deep feature extraction with multi-layer support vector machines to identify abnormal behavior in a sizable amount of network traffic data. Distributed networks' security was ensured by doing this.

4.2.2. K-Nearest Neighbor

The K-Nearest Neighbor method uses a dataset's distance between two classes to assess their similarity or dissimilarity [106]. Since KNNs don't make assumptions, they can adapt to the numerous data formats now available more readily than other ML algorithms [107]. The decision tree is a supervised learning method in which the labeled dataset accurately predicts the model's output. The Wisdom Tree. A type of supervised learning known as decision trees uses labeled data to predict a model's production correctly. This machine learning method uses supervised learning and looks like a flowchart tree. To better prepare the large-scale cybersecurity dataset (UGR'16) for the anomaly detection model, used a decision tree and multilayer perceptron processing [108].

4.2.3. Deep Belief Network

According to one definition, a deep belief network comprises numerous layers, each of which can function as a restricted Boltzmann machine. Applications in the field of cybersecurity that require access to massive databases may find this helpful strategy. In [109], the writers thoroughly examined the use of deep belief networks and other deep learning techniques in cybersecurity. In the same way, the authors in [110] used the NSL-KDD dataset to assess the performance of the deep belief network for face recognition, pedestrian detection, and intrusion detection compared to a region extreme learning machine technique. In [111], Network performance may be monitored using traffic and payload parameters, enabling a secure deep neural network-based design. This framework was created to help identify hackers' behaviors in SCADA environments. A healthcare system's use of a blockchain-based architecture made it easier to pinpoint where unauthorized access attempts were attempted [112].

4.2.4. Recurrent Neural Networks

The directed graph structure of the recurrent neural network sets it aside from other neural networks. RNN also creates bidirectional signals and extends the network via loops. Since RNNs take longer to process than feed-forward neural networks, they are used less commonly in real-time applications. However, RNN was used to improve the accuracy of intrusion detection systems that used the dataset. In [113], To solve the issue of improper data injection in DC microgrids, a novel artificial intelligence-based method has been created. Researchers used RESs and a nonlinear auto-regressive external model to forecast dc voltages and currents. NARX aims to improve network performance compared to traditional RNNs in terms of speed, accuracy, and ease of understanding [114].

4.2.5. Convolutional Neural Networks

Compared to other deep learning algorithms, CNNs can learn from raw data. As a result, data extraction, which is generally done before training a model, is no longer necessary. Hidden networks, pooling networks, convolutional networks, and fully-connected networks are frequently included in convolutional networks (CNNs). In terms of cyber security, CNN lacks a particular leader in the field. The many security and privacy issues that organizations currently confront have led to the development of many CNN-based methods. For instance, as part of a cutting-edge method for identifying abnormal incursions, CNN was used to create a multiclass classification model for IoT networks. This process was used to find any possible threats [115]. The authors in [116] used this technique to find cyber-attacks on industrial control systems to create a small version of a wide range of industrial water treatment facilities. In [117], To recognize DoS attacks on IoT networks, writers used CNN. A distinct deep CNN technique was also recommended for malware identification [118]. It also allows the network to be used successfully on a GPU. A multi-CNN fusion technique was suggested to detect intrusion attacks on industrial IoT networks [119].

Thousands of sensors are being included in the smart grid's infrastructure to make the switch from a traditional grid to a smart grid. These sensors produce enormous amounts of data in the form of log files or time series data since they continuously check the health of the hardware to which they are connected. A smart grid system has several different kinds of sensors, including those that measure voltage, current, module temperatures, and irradiance. The information gathered by these sensors is processed before being sent to a server for storage. Both local and remote hosting options exist. The most secure way to store data is on a local server, but doing so limits the data's usefulness for identifying novel patterns or developing a deeper understanding of the subject of the study. The user has more control over how data is used when information is stored on a cloud server, accessible from a distance, and scraped to a computer using the GETS command. Machine learning approaches have lately been effective at locating cases of cyber intrusion. By examining past events, machine learning, on the other hand, may be able to identify intrusions. To

prepare for power outages, 54 linked J Ripper with Ada boost. The model divided the data into three categories based on its findings (assault, natural disturbances, and no event). An attack known as the false data injection attack is typical and has the potential to damage smart grid networks seriously. For utilities and consumers, tampering with data from smart meters might be pretty expensive. To locate the FDIA, researchers used ensemble-based machine learning [55]. Figure 8 shows the supervised learning process.

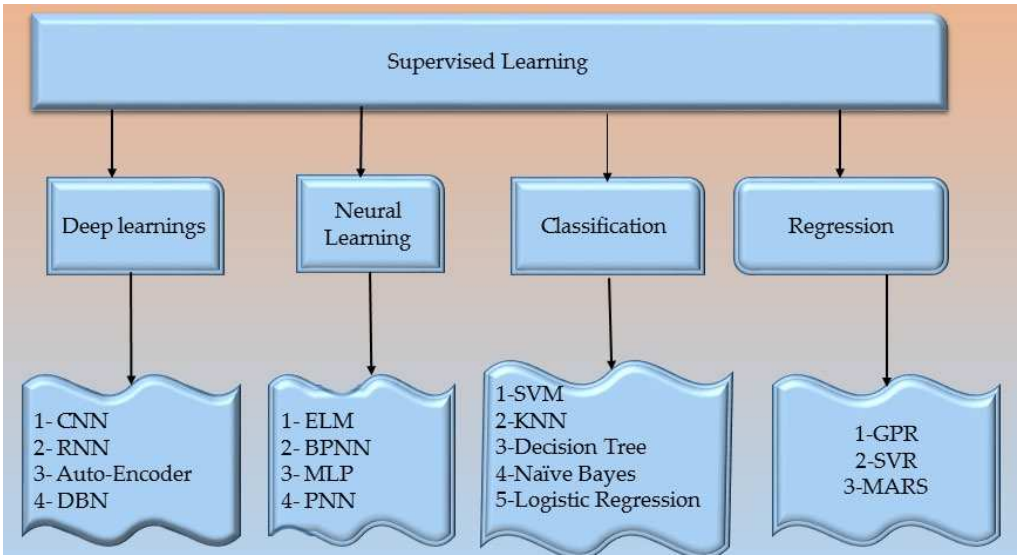

Figure 8. Supervised learning techniques in the smart grid.

The IEEE 14 bus system was used to evaluate the model. Unlike linear regression, naive Bayes, decision trees, and support vector machines, unsupervised ensemble models were more accurate than individual models, with the most incredible accuracy reaching 73%. The multilayer perceptron is used in [56] to examine how FDIA affects AI-based smart grids thoroughly. The study found that even if only 20% of the data is false, machine learning algorithms' accuracy might drop by 15%. This may significantly impact the decision-making process for the smart grid. Suppose a disruption happens, and the model cannot predict it because of inaccurate data, for example. In that case, data poisoning could cause the grid to become unstable and have unfavorable effects. The entire system can be negatively affected. The authors in [33] suggests using a conditional deep belief network technique to identify FDIA for power theft in real-time. The IEEE 118 bus and the IEEE 300 bus were used to test the model. The model's outcomes contrasted with support vector machines and artificial neural networks. Attacks that cause distributed denial-of-service to a smart grid are another possible danger. Attacks using distributed denial of service render servers and other crucial communication channels unusable. The goal of a DDoS assault is to bring down the targeted communication server by flooding it with fake requests. The authors in [57] proposes a multilevel auto-encoder model for detecting distributed denial of service attacks. An autoencoder has one input layer, at least one hidden layer, and one output layer. 49 characteristics and 700,000 data packets were used to train the model. These packets could be identified from others by their source IP address and ports, destination IP address and ports, both ends' jittering, record time, and type of attack. The UNSW-NB15 data set, available to the public for free, was used to develop the model. The results show that the auto-encoder-based prediction model performs better than the LSTM, random forest, naive Bayes approach, decision tree, k-nearest neighbor, and LSVM. Table 6 shows the Summary of different Machine Learning and deep learning Methods.

Table 6. Summary of different Machine Learning and deep learning Methods.

References	Methods	Solution
[120]	Naive Bayes	Can be applied to analyses of both discrete and continuous variables. Features are assessed mutually exclusive, speeding up the process and making it applicable for real-time decision-making.
[121]	Support Vector Machines	In high-dimensional spaces, it effetely uses memory. Features that use numbers and categories
[122]	Decision Tree	Effectively uses memory in elevated environments. Features that employ categories and numbers
[123]	Sequential Pattern Mining	Frequent sequential patterns for a frequency support measure.
[124]	DBSCAN	Identify outliers and separate clusters of high density from sets of low density.
[125]	ADMIT	It doesn't need a lot of labeled data to function. Makes use of a recursive clustering algorithm, A K-means clustering variant.
[126]	A priori algorithm	As a result, the resulting restrictions make sense. Unsupervised, therefore labeled data aren't needed.
[73]	Radial Basis Function	Real-time network anomaly detection.
[127]	Random forest	Multi-class classification of network traffic threat
[128]	Extra-tree classifier	Multi-class classification of DoS, probe, R2L, and U2R
[129]	Radial Basis Function	Comparative classification between lazy, eager learning, and deep learning
[130]	Random forest	Comparative classification between lazy, eager learning, and deep learning.
[130]	Random forest	Android malware detection
[131]	ANN	Abilities to learn, classify, and process information; faster self-organization.
[132]	Deep Flow	Specifically designed to identify malicious software. Flow Droid, a program for static impurity analysis, is employed. Determines the paths taken by potentially sensitive data within Android applications
[133]	DBNs	Discovers layers of features and uses a feed-forward neural network to optimize discrimination.
[134]	Deep Belief Network	Real-time network anomaly detection.
[135]	Gated Recurrent Unit	Multi-class classification of network traffic threats
[136]	CNN-LSTM	Multi-class classification of DoS, probe, R2L, and U2R.
[137]	Deep Feed Forward	Differentiating between shallow, intermediate, and deep learning
[138]	Temporal convolutional networks	Comparative classification between lazy, eager learning, and deep learning.
[139]	CNN	Android malware detection.
[140]	Bi-LSTM	Classification of spam and ham from emails.

Machine learning techniques such as unsupervised pattern discovery look for patterns in data without the help of labels. Although supervised learning algorithms have been the subject of decades of research, their use still depends on the users' access to the truth or their knowledge of the patterns to seek. This rarely happens when theory is applied in practice. Unsupervised learning can be used to find ways before data or predict what will happen in the future because it doesn't require labels. The method is, therefore, beneficial. Unsupervised neural networks can be used for several tasks, such as predicting load [63], determining stability [64], and detecting errors [65]. Auto encoders, variant auto encoders, and constrained Boltzmann machines are a few of these machines, but they are not the only ones. There are many examples of this. Clustering is a statistical approach by dividing a population or set of data points into subgroups that are comparable to the total. Untrained and uncontrolled persons carry out clustering. Some clustering methods include k-means, fuzzy c-means, hierarchical clustering, and DBSCAN. Additional clustering techniques not covered here exist. Applications are categorized using efficiency noise analysis. Data handling for smart grids typically use dimension reduction. Moving data from a high-dimensional space to a low-dimensional area is crucial to this method. These techniques have made it much simpler to utilize the information obtained [66]. Principal component analysis (PCA), linear discriminant analysis, extended linear discriminant analysis, and nonnegative matrix factorization is DR approaches used in smart grids [67]. The un-supervised learning process is shown in Figure 9.

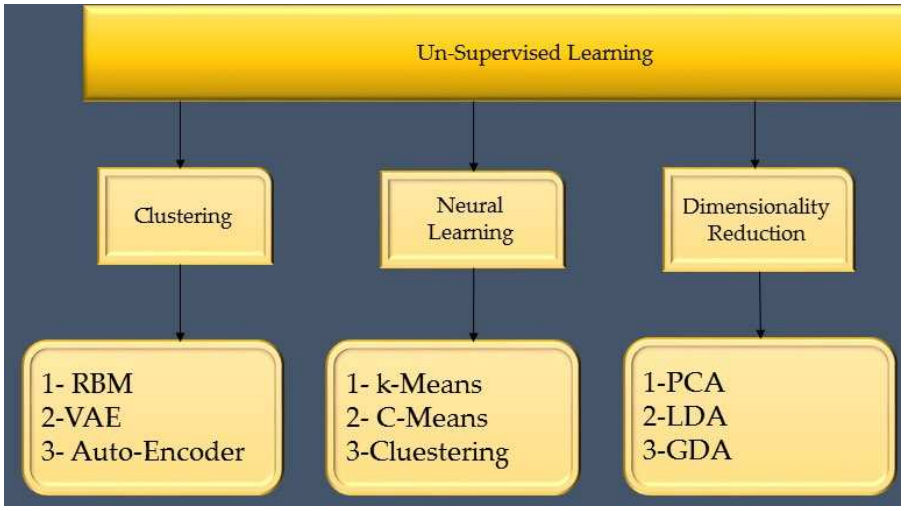

Figure 9. UN Supervised learning techniques in the smart grid.

4.2.6. Deep Reinforcement Learning

Reinforcement learning (RL) algorithms have the ability to maintain order in unpredictable situations. Therefore, the described POMDP challenge can be resolved using RL. The issue can be resolved using either a model-based RL algorithm for POMDPs [141] or a model-free RL algorithm without having to learn the underlying model. In general, only an unsubtle model can be learned using the model-based approach because it requires a two-step solution that is more challenging to compute. Attack-free worldwide anomaly identification methods include the Euclidean detector [142] and the arcos metric-based detector [26]. These systems compare expected and actual meter readings (using the Kalman filter) and, if the difference is greater than a set threshold, they declare an attack or anomaly. These detectors, however, only look at one sample at a time, so they cannot tell if attacks are taking place at the same time as strange results. Because of this, they are unable to differentiate between short-term anomalies generated, for instance, by an unfavorable system intervention and longer-term anomalies caused by system-level randomness. As a result, we need methods for universal attack detection that are more reliable than those that look for anomalies. Here, we look at the issue of smart grid security from the defender's point of view and use RL approaches to find an effective detection system [143]. The issue can also be viewed from the perspective of an attacker, in which case the goal is to determine the most harmful attack strategies. For vulnerability analysis, which is the process of identifying the worst possible thing an attacker might do to a system and then taking precautions against it, a challenge like this can be very helpful. RL has been the focus of numerous vulnerability investigations. For examples of FDI and sequential network topology attacks [50]. We also point out that the issue can be seen simultaneously from both the defenders and the attacker's points of view, just like in game theory. Multiage RL is a single-agent RL extension that heavily relies on game theory. This is thus because each actor's best behaviors depend on both their surroundings and the actions of other agents. Furthermore, stochastic games extend Markov decision processes to the multi-agent environment, where the game is played in a certain order, has many states, and is subject to payoffs that depend on the actions of all agents. To solve stochastic games, offer a number of RL-based techniques [144]. Additionally, if the environment's fundamental state, other agents' actions and rewards, etc. are only partially observable, the game is a partially observable stochastic one, which is often more challenging to solve.

4.2.7. Cloud-Based Detection and Mitigation

When combined with IoT technologies, cloud computing offers quick Internet access to a range of cloud services, including memory, storage, processing, network capacity, and database applications. One helpful feature of cloud computing is "pay as you go".

It is challenging for utility companies to build and execute this architecture to lower the cost of the hardware, software, and network services for the Smart grid. It is crucial to maximizing the network infrastructure's existing buffer, storage, constrained processing, and bandwidth since smart meters generate much additional traffic in the Smart grid. The authors of [60] examined how cloud computing features could be used to defend smart grids from DDoS attacks. The authors of [61] suggest using a cloud-based firewall to prevent DDoS attacks on smart grids. We created 250 Gbps of data for this experiment to simulate a distributed denial of service attack. According to the simulation results, the grid Open Flow firewall is not particularly slow. To ensure that only authorized users have access to cloud-based data, [62] proposes an attribute-based online/offline searchable encryption solution for smart grid applications. Figure 10 shows a cloud-Based Detection and Mitigation.

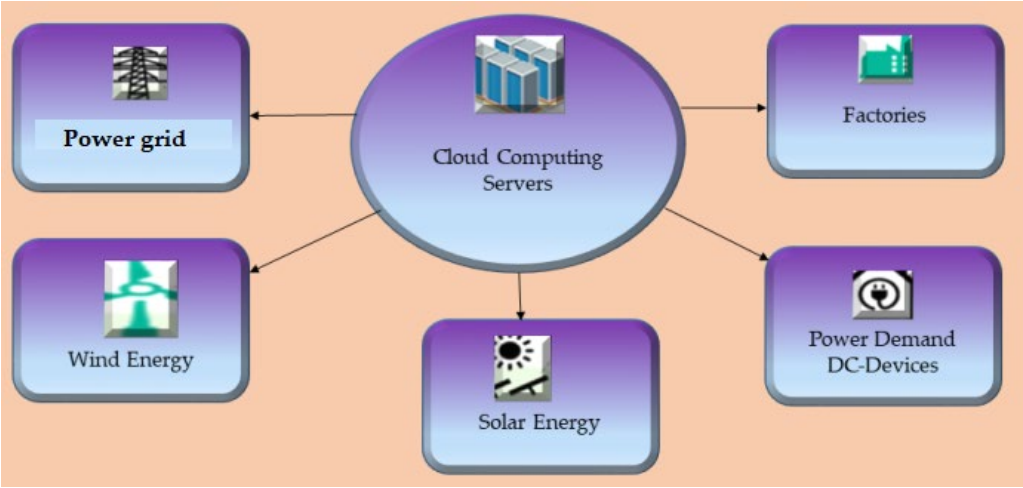

Figure 10. Cloud-Based Detection and Mitigation.

The authors of [63] describe a secure home area network that uses the cloud of things and is protected against threats, including brute force, replay, and capture. A model for assessing the security of a smart grid is created in [64]. A deep belief network comprises numerous RBMs, and a BP neural network is used to achieve this. To assess the overall level of security risks related to policy and organization and technological risks in general, SaaS, PaaS, and IaaS risks were looked at. Table 7 shows the Cloud-Based Detection and Mitigation.

Table 7. The Cloud-Based Detection and Mitigation.

References	Objectives	Techniques	Limitations	Solutions
[145]	Auto-scaling of VM and VM-to-PM packing.	The approach is based on shadow routing.	Less no. of hosting PMs by intelligently packing VMs-into-PM.	Less no. of hosting PMs by intelligently packing VMs-into-PM.
[146]	Balance the load of network resources.	Layered virtual machine migration.	The migration cost is high.	High performance in balancing the bandwidth utilization rate of hosts and sound management of both the physical and network resources.

Table 7. *Cont.*

References	Objectives	Techniques	Limitations	Solutions
[147]	Minimize resource consumption and heavy traffic.	Cluster-aware VM collaborative migration scheme for media cloud.	The approach that has been proposed does not optimize the virtual machine migration in the media cloud. The expense of migration is costly.	A perfect migration is achieved by the utilization of clustering and placement algorithms, as well as an efficient migration of VM media servers.
[148]	Reduce energy consumption with high migration costs.	An improved grouping genetic algorithm (IGGA).	The migration cost is still high because of the migration of one VM at a time.	Increases the concentration score while bringing down the energy consumed while the consolidation score is high.
[149]	Minimize energy consumption and excellent migration cost.	Ant colony system (ACO)	The migration cost is still high because of migrating one VM at a time.	Reduces the overall amount of energy used by reducing the number of active PMs while ensuring compliance with the SLA's quality of service requirements.
[150]	Lessen energy consumption and excellent migration cost.	Firefly optimization approach.	Because migration may only result in a high utilization rate of network resources, the load cloud data centers are currently carrying is not going away.	Technique for migrating virtual machines in the cloud that is sensitive to energy consumption and moves overloaded VMs to regular PMs.

4.3. Blockchain-Based Detection and Mitigation

The authors of [151] analyses each publication published between 2016 and 2022 that exclusively discusses protective measures for blockchain-based systems. The first cryptocurrency built on a blockchain, Bitcoin, was announced in 2008. The first blockchain-based cryptocurrency with smart contracts, Ethereum, made its debut in 2015. An alternate use of blockchain technology is the public blockchain project. blockchain technology was initially connected to the virtual currency bitcoin, but a new study suggests that it might be used for much more. Taking into account [152] claims, More investigation was done to determine whether blockchain technology might be used to improve cybersecurity. The authors looked into various potential fixes for blockchain security problems. To reduce the risk of cybercrime, a web-based cybersecurity awareness was developed. To maintain software security against hackers, the suggested method uses blockchain technology [112].

It was shown that a data-transfer system with an object-categorization algorithm might be created using blockchain technology due to its security; blockchain a sort of distributed ledger technology that has recently appeared as one of the most useful in numerous industries. On the blockchain, each block contains data, an index, a time stamp, a hash, and the hash of the block before it. A block cipher, in the opinion of many, forms the basis of blockchain dependability. Suppose the hash value of one block changes; all succeeding blocks in the chain must also change. Usually, it takes a lot of time and money to achieve this on a computer. According to the authors of [153], a policy architecture for data flow between autonomous system operations and agents that aren't performing their duties should be built using blockchain technology. These actions were all taken to combat the FDIA. Three sections make up the model: "data", "detection", and "blockchain". Figure 11 shows the blockchain Applications.

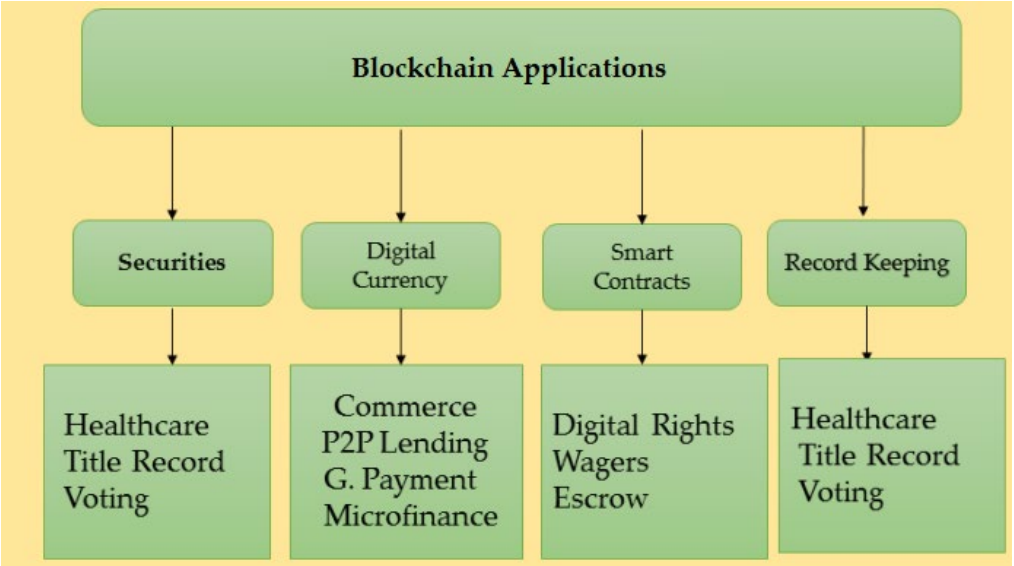

Figure 11. The blockchain Applications.

Information is gathered by the data layer and sent to the detection layer for community detection. The blockchain layer also secures the community detection and transaction record. In their article, the authors created a blockchain-based system for smart meters and service providers to communicate through encrypted communications [154]. The technique stops FDIA from happening on the smart meter's side. Smart meters serve as controller nodes in this study, starting all interactions with the service provider. Data is shared and validated throughout a network by auditing and broadcasting transactions. Service providers communicate with one another over P2P networking. A new transaction or block cannot be added until consensus has been validated, and only then can a new block be added. Each trade generates a unique key using the SHA-256 method. In this study, the authors showed that a framework built on a blockchain might be used to speed up data transmission and reception inside a P2P service provider network. This study [155] created a decentralized security paradigm using smart contracts and the lightning network in a blockchain environment. The registration, scheduling, verification, and payment processes are among the several procedures in this method. The authors of [156] created a product power system device design that combines hardware security with a blockchain-based method for maintaining a distributed security mechanism that checks the provenance of incoming communications. Table 8 shows the blockchain-Based Detection and Mitigation.

Table 8. Blockchain-Based Detection and Mitigation.

References	Methods	Short Description	Findings
[157]	A game theoretic approach	A framework for energy trade and decision-making based on game theory	The strategy makes P2P trade both fair and optimum.
[158]	Networks of bilateral agreements for peer-to-peer energy trading	Networks for P2P energy trade that are bilateral and scalable	combines real-time and forward contract trading strategies
[61]	blockchain Applications in Smart grid	It looked at new blockchain applications and how they were used in the SG.	It showed the advantages of blockchain in the electrical network and the SG framework SPB, which reduces the costs, size, and processing time associated with energy trade.

Table 8. *Cont.*

References	Methods	Short Description	Findings
[159]	A Distributed Private Energy Trading Platform.	Presented a proof-of-concept for a secure private blockchain energy transaction system.	It showed the advantages of using blockchains in the electrical network and the SPB framework, which lowers the expenses, volume, and processing times related to energy trade.
[160]	Energy Trading Between Individuals Using a Virtual Power Plant Which Is Powered by Smart Contracts Stored on a blockchain	A public, sale price purchasing mechanism SC enables is recommended for energy trading.	Auction-based energy-trading platform
[161]	blockchain-based smart contract architecture for distributed generation trade and management	An infrastructure built on the blockchain to close the demand-response gap between energy supply by producers and consumer demand in peer-to-peer energy trading.	More than 25 individuals can trade energy at once due to it.
[162]	Blockchain-enabled Peer-to-Peer energy trading	investigates the best application of blockchain technology for peer-to-peer energy trading	The method is cheap for blockchain transactions.
[163]	Energy sharing between peers using batteries	It proposed an energy-sharing architecture based on energy pieces in a community market with a shareholder energy storage system, consumers, and users	Maximizes the income output for the energy supplier
[164]	Energy-backed token trading that is peer-to-peer and based on a decentralized blockchain platform for active producers and consumers	Utilize the blockchain to enable peer-to-peer trading of energy tokens	The suggested strategy ensures a global and practical resolution while requesting no private information from the participants.

4.4. Hardware-Based Security

The smart grid system is useless without devices connecting to the internet. These devices must resist cyberattacks since they gather, process, and transmit data over the channel. The authors in [165] discussed some of the most critical hardware security issues. Security flaws might appear in many ways, including physical attacks, hardware Trojans, and side-channel analyses. The attacker wants to avoid being identified during the actual physical attack by the authentication procedure. System flaws were exploited using reverse engineering to plan the attack. An opponent can determine the cryptographic keys by analyzing the profile of numerous variables, including current, voltage, and frequency, using a method called "side-channel analysis". Any deliberate alterations or additions to a circuit are referred to as hardware Trojans. Hardware Trojans are malicious applications that steal sensitive information, change circuitry, or lower the system's dependability. According to the authors' analysis, path delay fingerprinting may be utilized to identify hardware Trojans. Smart meters, sensors, and communication devices are examples of IoT devices that battle with how much energy they can use and how little power they can use [166]. Because they allow fully secure authentication without requiring the device to have cryptographic expertise, PUFs are perfect for low-power Internet of Things (IoT) devices. Even so, by analyzing historical data and events, it is now possible to predict PUF behavior with a 95% degree of accuracy because of the development of machine learning [167]. To prevent machine learning-based attacks from breaching PUFs, the study's authors [167] developed a CTPUF, or configurable tristate PUF, using an XOR-based technique that hides the connection between the issue and the solution. The environment is too chaotic for the

machine learning model to detect recurring patterns between the challenge and responses. The results of this study showed that the accuracy of machine learning models that used CTPUF, such as support vector machines, artificial neural networks, and logistic regression models, was about 60%. Another study [168] used machine learning models to show the shortcomings of voltage-over-scaling (VOS)-based authentication. The studies also made abuse a possibility. The authors of this work developed a VOS technique that is immune to ML by fusing earlier challenges with keys. The results showed that when the challenge self-obfuscation structure was used, the ML model was approximately 51.2% accurate.

4.5. Future Improvements and Challenges

Source datasets are crucial for both cybersecurity and machine learning in a similar way. Most publicly available data is older, which might not be enough to identify trends in undetected cyberattacks. The most recent attacks and their repeated patterns remain a mystery, even though current data can be processed into knowledge through several different processing steps. As a result, it's possible that certain conclusions won't be drawn with exceptional precision using future processing or machine learning approaches. The production of numerous new cybersecurity datasets for particular problems like predicting attacks or detecting intrusions is a significant difficulty when using machine learning techniques in cybersecurity. Security datasets may be unbalanced, noisy, lacking crucial details, meaningless, or include examples of security vulnerabilities that are inconsistent with one another. The training of machine learning models may be more challenging and time-consuming when a dataset contains this kind of consistency [169]. These data concerns need to be fixed before using machine learning to create a data-driven cybersecurity solution.

Knowing everything there is to know about the issues with cybersecurity data is essential, as is finding reasonable solutions to these issues by using either current algorithms or brand-new algorithms to, among other things, locate malware and intrusions. One method to directly address these problems is feature engineering [170], which examines model features to remove related parts.

This method reduces the complexity of the data. A key strategy for dealing with measurement errors is using hybrid models, as explained in [73], or data creation, as described in [171]. More vulnerabilities that could lead to data leakage need to be addressed. The most popular and well-known techniques in cyber security use signatures to find intrusion attempts [172]. Due to data shortages, overly simplified characteristics, or inadequate profiling, these systems might overlook some assaults or events. These problems can be mitigated by signature-based or hybrid detection strategies combining signature-based and anomaly-based detection techniques. With a hybrid learning strategy that makes use of numerous machine learning techniques, intrusion detection, malware analysis, phishing detection, etc., all perform better. Machine learning, statistical analysis, and deep learning algorithms can be combined to make wise cybersecurity management decisions.

Due to the enormous amount of network traffic data and the high number of minute traffic features, a security model based on machine learning has frequently been questioned regarding its effectiveness and performance. Principal component analysis, singular value decomposition [73], and linear discriminant analysis have all been used by researchers to handle high-dimensional data [173].

Contextually, it might be advantageous to include low-level information in datasets that could be connected to problematic behaviors. This kind of contextual data may be categorized using an ecosystem or taxonomy for upcoming research. Therefore, choosing the best features or extracting the most important ones while considering machine-readable aspects and the context presents another challenge for machine-learning approaches in cybersecurity. To create effective cybersecurity solutions, this is necessary.

When models are used to produce predictions even while essential data is missing or significantly varies between datasets, this is known as data leakage [169]. Prediction models frequently result in too hopeful conclusions when they are being created. Still, when evaluated on new data, unsatisfactory findings list this problem, known as "leaks

from the future," as "one of the top 10 data mining defects." They suggest using exploratory data analysis to find and fix leakage sources. EDA enables machine learning models to collect more accurate data, enhancing the dataset's usefulness. Leakage detection and exploitation are substantial contributors, according to recent studies [174]. They were also noted as a critical factor in the failure of a data mining program. Researchers address the use of giveaway characteristics in data mining competitions to forecast the objective in another paper. This is because certain qualities were added afterward [175]. This article looks at the most popular techniques for categorizing documents and possible dataset structures for binary prediction. Each observation was given a "legitimacy tag" during the data collection phase, and data breaches were subsequently identified using a learn-predict separation. Maximum accuracy values of 91.2% for naive Bayes, 87.5% for k-NN, and 94.4% for centroid suggest that the suggested strategy is effective based on numerous categories.

The use of EDA to detect leaks is an exciting area for future research since it can be used in various situations when the machine learning scientist has little control over the data-gathering procedure. Homomorphic Encryption (HE) is regarded as a significant technological achievement by many cryptography experts [176]. HE gives unreliable third-party access to private data without disclosing anything. The encrypted data may end up on the user's computer or an unauthorized distant server, but not the decryption key. No information will be disclosed to unauthorized parties so the host can relax. HE can be used for various things, including cloud computing, financial transactions, and defense against quantum computing. HE can be used in a constrained or expansive way. During machine learning training, Fully Homomorphic Encryption (FHE) aids in maintaining the confidentiality of sensitive data. Shallow machine learning and deep learning substantially rely on domain data, which isn't always easy to come by for free [177].

Asymmetric encryption techniques were first thought to be straightforward for quantum computers to decrypt [178]. A pair of keys—one public and one private—are used for asymmetric key encryption. By multiplying two huge prime numbers, these keys are created. We employ large encryption keys to ensure the security of our data because it is challenging to factor in large prime numbers but simple to factor in small ones. A more labor-intensive approach for factoring such enormous prime integers is Shor's algorithm. The superposition quantum computing method may allow the factors to be discovered in a small portion of the time needed by a traditional binary computer. Elliptic curve algorithms and digital signature technologies like RSA and DES are weak points. Grover's method [73], based on quantum computing, claims that it will only take 185 searches to find the key to a 56-bit DES. Despite the existence of quantum computers, symmetric essential techniques like AES are still secure. Researchers are examining if these constraints may be overcome using mathematical and quantum methods. A quantum key distribution example is the BB84 protocol [179]. Lattice-based cryptography and other mathematical techniques are also being researched. Asymmetric encryption cannot be solved with quantum computing; however, using it as subroutine helps speed up machine learning [180].

This can drastically shorten prediction times for algorithms like SVM, where constructing a hyperplane and performing kernel modifications can take some time.

They may also be used for deep learning if they are well-designed. However, there are problems because quantum neural networks move in a straight path.

5. Conclusions

Transitioning from a traditional grid to a smart grid is complex and loaded with the inherent risks of testing out trying to cut technologies. Creating and maintaining an effective communication network architecture is one of the smart grid's most difficult tasks. In addition, creating a reliable physical architecture and keeping it up-to-date are challenging tasks. In this study, the communication infrastructure of the smart grid was studied, and future cyberattacks and defense strategies were taken into account. It would help if you never risked starting an attack because even a small one can have harmful effects. We think the people who use or operate the communication network are just as vulnerable

to attacks as the network itself. If the attacks are not successfully dealt with, they can turn into easy targets. It was suggested that security measures be put in place for smart grid clients, their communications network, and smart grid operators to build a reliable smart grid network. We took this action because we know that hackers target computer systems and their users and administrators. We considered many essentials before concluding this conclusion, including the nature of the attack, its scope, the individuals it affected, and the results it produced. Cyberattacks were also categorized according to the features of the attacks, such as the large areas that were compromised, the methods that were utilized to carry them out, and the measures necessary to establish dependable and efficient defenses. To successfully implement smart grid technology, network security must be addressed. However, previous studies have shown that their impact is minimal when assessing cyber-security solutions for smart grid networks. Therefore, this study completes the gaps left by earlier research by providing an in-depth description of potential smart grid attacks and assessing various security solutions.

In this research, we propose a layer-based classification of cyberattacks and a grading of these attacks regarding integrity, availability, confidentiality, and accountability. Finally, we highlight persistent issues that can guide future studies. Based on the results of this study, it is clear that there is a great need for novel approaches that may collectively resolve the complications associated with security issues in smart grid infrastructures without compromising the efficiency and usefulness of the network. For instance, "important regions impacted" refers to geographical locations essential to the network's functioning. Cyberattacks on smart grids are currently the focus of an extended investigation into the formation of a categorical classification. In this article, we will examine the many challenges that the sector is presently facing regarding cyber security, as well as the solutions that are currently accessible and the expected needs for future research. A comprehensive understanding of the types of security threats and assaults that smart grids are vulnerable to, as well as how these threats and attacks can be avoided, can be obtained by a review of the available research and literature. A comprehensive understanding of the types of security threats and assaults that smart grids are susceptible to and how these threats and attacks can be avoided can be attained by reviewing the available research and literature.

Author Contributions: Conceptualization, T.M. and I.H.; methodology, T.M. and H.M.I.; software, T.M. and H.M.I.; validation, T.M. and S.K.; formal analysis, T.M. and S.K.; investigation, T.M. and I.U.; resources, M.I. and T.M.; data curation, M.I. and T.M.; writing—original draft preparation, T.M. and I.H.; writing—review and editing, T.M. and I.H.; visualization, H.H., I.U. and I.H. All authors have read and agreed to the published version of the manuscript.

Funding: The authors thank the Natural Sciences and Engineering Research Council of Canada (NSERC) and New Brunswick Innovation Foundation (NBIF) for the financial support of the global Project. These granting agencies did not contribute to the study design and collection, analysis, and interpretation of data.

Data Availability Statement: Not applicable.

Acknowledgments: The authors thank Spectrum of Knowledge Production and Skills Development (Sfax) for giving access to its premises and for its logistical support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies* **2022**, *15*, 6799. [CrossRef]
2. Mololoth, V.K.; Saguna, S.; Åhlund, C. Blockchain and Machine Learning for Future Smart Grids: A Review. *Energies* **2023**, *16*, 528. [CrossRef]
3. Moreno-Munoz, A.; Bellido-Outeirino, F.; Siano, P.; Gomez-Nieto, M. Mobile social media for smart grids customer engagement: Emerging trends and challenges. *Renew. Sustain. Energy Rev.* **2016**, *53*, 1611–1616. [CrossRef]
4. Abrahamsen, F.E.; Ai, Y.; Cheffena, M. Communication technologies for smart grid: A comprehensive survey. *Sensors* **2021**, *21*, 8087. [CrossRef]

5. Ugwu, J.; Odo, K.C.; Ohanu, C.P.; García, J.; Georgious, R. Comprehensive Review of Renewable Energy Communication Modeling for Smart Systems. *Energies* **2022**, *16*, 409. [CrossRef]
6. Jaiswal, D.M.; Thakre, M.P. Modeling & designing of smart energy meter for smart grid applications. *Glob. Transit. Proc.* **2022**, *3*, 311–316.
7. Kim, Y.; Hakak, S.; Ghorbani, A. Smart grid security: Attacks and defence techniques. *IET Smart Grid* **2022**. [CrossRef]
8. Appasani, B.; Mishra, S.K.; Jha, A.V.; Mishra, S.K.; Enescu, F.M.; Sorlei, I.S.; Bîrleanu, F.G.; Takorabet, N.; Thounthong, P.; Bizon, N. Blockchain-enabled smart grid applications: Architecture, challenges, and solutions. *Sustainability* **2022**, *14*, 8801. [CrossRef]
9. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
10. Takiddin, A.; Ismail, M.; Zafar, U.; Serpedin, E. Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids. *IEEE Syst. J.* **2022**, *16*, 4106–4117. [CrossRef]
11. Abed, A.K.; Anupam, A. Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Secur. Priv.* **2022**, e285. [CrossRef]
12. Vatsyayan, V.; Chakraborty, A.; Rajarajan, G.; Fernandez, A.L. A Detailed Investigation of Popular Attacks on Cyber Physical Systems. In *Cyber Security Applications for Industry 4.0*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2023; pp. 1–42.
13. Ghiasi, M.; Niknam, T.; Wang, Z.; Mehrandezh, M.; Dehghani, M.; Ghadimi, N. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electr. Power Syst. Res.* **2023**, *215*, 108975. [CrossRef]
14. Khoei, T.T.; Slimane, H.O.; Kaabouch, N. A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions. *arXiv* **2022**, arXiv:2207.07738.
15. Zeng, H.; Ng, Z.W.; Zhou, P.; Lou, X.; Yau, D.K.; Winslett, M. Detecting Cyber Attacks in Smart Grids with Massive Unlabeled Sensing Data. In Proceedings of the 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Singapore, 25–28 October 2022; pp. 1–7.
16. Berghout, T.; Benbouzid, M.; Muyeen, S. Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100547. [CrossRef]
17. Shah, S.F.A.; Iqbal, M.; Aziz, Z.; Rana, T.A.; Khalid, A.; Cheah, Y.-N.; Arif, M. The role of machine learning and the internet of things in smart buildings for energy efficiency. *Appl. Sci.* **2022**, *12*, 7882. [CrossRef]
18. Luo, J. A Bibliometric Review on Artificial Intelligence for Smart Buildings. *Sustainability* **2022**, *14*, 10230. [CrossRef]
19. Mazhar, T.; Irfan, H.M.; Haq, I.; Ullah, I.; Ashraf, M.; Shloul, T.A.; Ghadi, Y.Y.; Elkamchouchi, D.H. Analysis of Challenges and Solutions of IoT in Smart Grids Using AI and Machine Learning Techniques: A Review. *Electronics* **2023**, *12*, 242. [CrossRef]
20. Szczepaniuk, H.; Szczepaniuk, E.K. Applications of Artificial Intelligence Algorithms in the Energy Sector. *Energies* **2023**, *16*, 347. [CrossRef]
21. Zamponi, M.E.; Barbierato, E. The Dual Role of Artificial Intelligence in Developing Smart Cities. *Smart Cities* **2022**, *5*, 728–755. [CrossRef]
22. Aguilar, J.; Garces-Jimenez, A.; R-Moreno, M.; García, R. A systematic literature review on the use of artificial intelligence in energy self-management in smart buildings. *Renew. Sustain. Energy Rev.* **2021**, *151*, 111530. [CrossRef]
23. Yılmaz, Y.; Uludag, S. Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *J. Frankl. Inst.* **2021**, *358*, 172–192. [CrossRef]
24. Farrukh, Y.A.; Ahmad, Z.; Khan, I.; Elavarasan, R.M. A sequential supervised machine learning approach for cyber attack detection in a smart grid system. In Proceedings of the 2021 North American Power Symposium (NAPS), College Station, TX, USA, 14–16 November 2021; pp. 1–6.
25. Haque, N.I.; Shahriar, M.H.; Dastgir, M.G.; Debnath, A.; Parvez, I.; Sarwat, A.; Rahman, M.A. Machine learning in generation, detection, and mitigation of cyberattacks in smart grid: A survey. *arXiv* **2020**, arXiv:2010.00661.
26. Gumaei, A.; Hassan, M.M.; Huda, S.; Hassan, M.R.; Camacho, D.; Del Ser, J.; Fortino, G. A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. *Appl. Soft Comput.* **2020**, *96*, 106658. [CrossRef]
27. Khazaei, J.; Amini, M.H. Protection of large-scale smart grids against false data injection cyberattacks leading to blackouts. *Int. J. Crit. Infrastruct. Prot.* **2021**, *35*, 100457. [CrossRef]
28. Bertone, F.; Lubrano, F.; Goga, K. Artificial intelligence techniques to prevent cyber attacks on smart grids. *Ann. Disaster Risk Sci. ADRS* **2020**, *3*, 208. [CrossRef]
29. Deepa, N.; Pham, Q.-V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Maddikunta, P.K.R.; Fang, F.; Pathirana, P.N. A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Gener. Comput. Syst.* **2022**, *131*, 209–226. [CrossRef]
30. Tufail, S.; Batool, S.; Sarwat, A.I. False data injection impact analysis in ai-based smart grid. In Proceedings of the SoutheastCon 2021, Atlanta, GA, USA, 10–13 March 2021; pp. 1–7.
31. Acharya, S.; Dvorkin, Y.; Karri, R. Causative cyberattacks on online learning-based automated demand response systems. *IEEE Trans. Smart Grid* **2021**, *12*, 3548–3559. [CrossRef]
32. Kumari, A.; Patel, R.K.; Sukharamwala, U.C.; Tanwar, S.; Raboaca, M.S.; Saad, A.; Tolba, A. AI-Empowered Attack Detection and Prevention Scheme for Smart Grid System. *Mathematics* **2022**, *10*, 2852. [CrossRef]
33. Yamin, M.M.; Ullah, M.; Ullah, H.; Katt, B. Weaponized AI for cyber attacks. *J. Inf. Secur. Appl.* **2021**, *57*, 102722. [CrossRef]

34. Li, Y.; Yan, J. Cybersecurity of smart inverters in the smart grid: A survey. *IEEE Trans. Power Electron.* **2022**, *38*, 2364–2383.
35. De Dutta, S.; Prasad, R. Cybersecurity for microgrid. In Proceedings of the 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC), Okayama, Japan, 19–26 October 2020; pp. 1–5.
36. Mohammadi, E.; Alizadeh, M.; Asgarimoghaddam, M.; Wang, X.; Simões, M.G. A review on application of artificial intelligence techniques in microgrids. *IEEE J. Emerg. Sel. Top. Ind. Electron.* **2022**, *3*, 878–890. [CrossRef]
37. Naderi, E.; Asrari, A. Toward detecting cyberattacks targeting modern power grids: A deep learning framework. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 357–363.
38. Wang, W.; Harrou, F.; Bouyeddou, B.; Senouci, S.-M.; Sun, Y. Cyber-attacks detection in industrial systems using artificial intelligence-driven methods. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100542. [CrossRef]
39. Hassani, H.; Beneki, C.; Unger, S.; Mazinani, M.T.; Yeganegi, M.R. Text mining in big data analytics. *Big Data Cogn. Comput.* **2020**, *4*, 1. [CrossRef]
40. Bonfanti, M.E. Artificial intelligence and the offence-defence balance in cyber security. In *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*; Routledge: London, UK, 2022; pp. 64–79.
41. Kurt, M.N.; Ogundijo, O.; Li, C.; Wang, X. Online cyber-attack detection in smart grid: A reinforcement learning approach. *IEEE Trans. Smart Grid* **2018**, *10*, 5174–5185. [CrossRef]
42. Ahmed, S.; Lee, Y.; Hyun, S.-H.; Koo, I. Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning. *IEEE Access* **2018**, *6*, 27518–27529. [CrossRef]
43. Li, X.; Ma, J.; Zhu, Y.; Liu, Y. Extraction of Abnormal Points from On-line Operation Data of Intelligent Meter Based on LSTM. In Proceedings of the 2019 IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Suzhou, China, 29 July–2 August 2019; pp. 586–591.
44. Singh, S.; Yassine, A.; Benlamri, R. Towards hybrid energy consumption prediction in smart grids with machine learning. In Proceedings of the 2018 4th International Conference on Big Data Innovations and Applications (Innovate-Data), Barcelona, Spain, 6–8 August 2018; pp. 44–50.
45. Sengan, S.; Subramaniyaswamy, V.; Indragandhi, V.; Velayutham, P.; Ravi, L. Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. *Comput. Electr. Eng.* **2021**, *93*, 107211. [CrossRef]
46. Yetis, Y.; Tehrani, K.; JamshidI, M. A Machine Learning Approach for Wind Speed Forecasting in Microgrids. In Proceedings of the 2022 World Automation Congress (WAC), San Antonio, TX, USA, 11–15 October 2022; pp. 12–17.
47. Ghenai, C.; Al-Mufti, O.A.A.; Al-Isawi, O.A.M.; Amirah, L.H.L.; Merabet, A. Short-term building electrical load forecasting using adaptive neuro-fuzzy inference system (ANFIS). *J. Build. Eng.* **2022**, *52*, 104323. [CrossRef]
48. Zhang, T.; Ji, X.; Xu, W. Jamming-resilient backup nodes selection for RPL-based routing in smart grid AMI networks. *Mob. Netw. Appl.* **2022**, *27*, 329–342. [CrossRef]
49. Ortega-Fernandez, I.; Liberati, F. A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning. *Energies* **2023**, *16*, 635. [CrossRef]
50. Rouzbahani, H.M.; Karimipour, H.; Lei, L. Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids. *Int. J. Electr. Power Energy Syst.* **2023**, *146*, 108798. [CrossRef]
51. Khoei, T.T.; Kaabouch, N. Densely Connected Neural Networks for Detecting Denial of Service Attacks on Smart Grid Network. In Proceedings of the 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 26–29 October 2022; pp. 0207–0211.
52. Chahal, A.; Gulia, P.; Gill, N.S.; Chatterjee, J.M. Performance Analysis of an Optimized ANN Model to Predict the Stability of Smart Grid. *Complexity* **2022**, *2022*, 7319010. [CrossRef]
53. Starke, A.; Nagaraj, K.; Ruben, C.; Aljohani, N.; Zou, S.; Bretas, A.; McNair, J.; Zare, A. Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security. *IET Smart Grid* **2022**, *5*, 398–416. [CrossRef]
54. Hadjidemetriou, L.; Tertytchny, G.; Karbouj, H.; Charalambous, C.; Michael, M.K.; Sazos, M.; Maniatakos, M. Demonstration of man in the middle attack on a feeder power factor correction unit. In Proceedings of the 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, The Netherlands, 26–28 October 2020; pp. 126–130.
55. Mohammadpourfard, M.; Khalili, A.; Genc, I.; Konstantinou, C. Cyber-resilient smart cities: Detection of malicious attacks in smart grids. *Sustain. Cities Soc.* **2021**, *75*, 103116. [CrossRef]
56. Radoglou Grammatikis, P.; Sarigiannidis, P.; Efstathopoulos, G.; Panaousis, E. ARIES: A novel multivariate intrusion detection system for smart grid. *Sensors* **2020**, *20*, 5305. [CrossRef]
57. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
58. Chen, J.; Mohamed, M.A.; Dampage, U.; Rezaei, M.; Salmen, S.H.; Obaid, S.A.; Annuk, A. A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks. *Appl. Sci.* **2021**, *11*, 9972. [CrossRef]
59. Chhaya, L.; Sharma, P.; Bhagwatikar, G.; Kumar, A. Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control. *Electronics* **2017**, *6*, 5. [CrossRef]
60. Zhang, H.; Liu, B.; Wu, H. Smart grid cyber-physical attack and defense: A review. *IEEE Access* **2021**, *9*, 29641–29659. [CrossRef]
61. Musleh, A.S.; Yao, G.; Muyeen, S. Blockchain applications in smart grid–review and frameworks. *IEEE Access* **2019**, *7*, 86746–86757. [CrossRef]

62. Nabil, M.; Ismail, M.; Mahmoud, M.; Shahin, M.; Qaraqe, K.; Serpedin, E. Deep learning-based detection of electricity theft cyber-attacks in smart grid AMI networks. In *Deep Learning Applications for Cyber Security*; Springer: Cham, Switzerland, 2019; pp. 73–102.
63. Zhang, K.; Hu, Z.; Zhan, Y.; Wang, X.; Guo, K. A smart grid AMI intrusion detection strategy based on extreme learning machine. *Energies* **2020**, *13*, 4907. [CrossRef]
64. Ismail, M.; Shahin, M.; Shaaban, M.F.; Serpedin, E.; Qaraqe, K. Efficient detection of electricity theft cyber attacks in AMI networks. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
65. Goranović, A.; Meisel, M.; Fotiadis, L.; Wilker, S.; Treytl, A.; Sauter, T. Blockchain applications in microgrids an overview of current projects and concepts. In Proceedings of the IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 29 October–1 November 2017; pp. 6153–6158.
66. Ahl, A.; Yarime, M.; Tanaka, K.; Sagawa, D. Review of blockchain-based distributed energy: Implications for institutional development. *Renew. Sustain. Energy Rev.* **2019**, *107*, 200–211. [CrossRef]
67. Mylrea, M.; Gourisetti, S.N.G. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In Proceedings of the 2017 Resilience Week (RWS), Wilmington, DE, USA, 18–22 September 2017; pp. 18–23.
68. Pop, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors* **2018**, *18*, 162. [CrossRef]
69. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, M.S.H. Application of big data and machine learning in smart grid, and associated security concerns: A review. *IEEE Access* **2019**, *7*, 13960–13988. [CrossRef]
70. De Dutta, S.; Prasad, R. Security for smart grid in 5G and beyond networks. *Wirel. Pers. Commun.* **2019**, *106*, 261–273. [CrossRef]
71. Van Cutsem, O.; Dac, D.H.; Boudou, P.; Kayal, M. Cooperative energy management of a community of smart-buildings: A Blockchain approach. *Int. J. Electr. Power Energy Syst.* **2020**, *117*, 105643. [CrossRef]
72. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A blockchain-based smart grid: Towards sustainable local energy markets. *Comput. Sci.-Res. Dev.* **2018**, *33*, 207–214. [CrossRef]
73. Ahsan, M.; Nygard, K.E.; Gomes, R.; Chowdhury, M.M.; Rifat, N.; Connolly, J.F. Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *J. Cybersecur. Priv.* **2022**, *2*, 527–555. [CrossRef]
74. Fischer, E. *Cybersecurity Issues and Challenges*; Library of Congress: Washington, DC, USA, 2017.
75. Fakiha, B. Business organization security strategies to cyber security threats. *Int. J. Saf. Secur. Eng* **2021**, *11*, 101–104. [CrossRef]
76. Sun, N.; Zhang, J.; Gao, S.; Zhang, L.Y.; Camtepe, S.; Xiang, Y. Data analytics of crowdsourced resources for cybersecurity intelligence. In Proceedings of the Network and System Security: 14th International Conference, NSS 2020, Proceedings 14, Melbourne, VIC, Australia, 25–27 November 2020; pp. 3–21.
77. Singh, H.; Pallagani, V.; Khandelwal, V.; Venkanna, U. IoT based smart home automation system using sensor node. In Proceedings of the 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 15–17 March 2018; pp. 1–5.
78. Muslih, M.; Supardi, D.; Multipi, E.; Nyaman, Y.M.; Rismawan, A. Developing smart workspace based IOT with artificial intelligence using telegram chatbot. In Proceedings of the 2018 International Conference on Computing, Engineering, and Design (ICCED), Bangkok, Thailand, 6–8 September 2018; pp. 230–234.
79. Nur Asyik, H.; Dirvi Eko, J. Design and Application of Internet of Things (IoT) for smart grid power system. In *Electrical Engineering and Computer Control*; Politeknik Negeri Madiun: Madiun, Indonesia, 2017.
80. Junfitrhana, A.P.; Langlangbuana, M.L.; Fatah, W.A. Developing potential agriculture land detector for determine suitable plant using Raspberry-Pi. In Proceedings of the 2017 International Conference on Computing, Engineering, and Design (Icced), Kuala Lumpur, Malaysia, 23–25 November 2017; pp. 1–4.
81. Kishore, P.; Veeramanikandasamy, T.; Sambath, K.; Veerakumar, S. Internet of things based low-cost real-time home automation and smart security system. *Int. J. Adv. Res. Comput. Commun. Eng.* **2017**, *6*, 505–509.
82. Geetha, A.; Sreenath, N. Byzantine attacks and its security measures in mobile adhoc networks. *Int'l J. Comput. Commun. Instrum. Eng. (IJCCIE 2016)* **2016**, *3*, 42–47.
83. Ding, G.; Wang, J.; Wu, Q.; Zhang, L.; Zou, Y.; Yao, Y.-D.; Chen, Y. Robust spectrum sensing with crowd sensors. *IEEE Trans. Commun.* **2014**, *62*, 3129–3143. [CrossRef]
84. Arani, M.F.; Jahromi, A.A.; Kundur, D.; Kassouf, M. Modeling and simulation of the aurora attack on microgrid point of common coupling. In Proceedings of the 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Montreal, QC, Canada, 15 April 2019; pp. 1–6.
85. Generation, D.; Storage, E. *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces Amendment 1: To Provide More*; IEEE: Piscataway, NJ, USA, 2020.
86. Giraldo, J.; Cárdenas, A.; Quijano, N. Integrity attacks on real-time pricing in smart grids: Impact and countermeasures. *IEEE Trans. Smart Grid* **2016**, *8*, 2249–2257. [CrossRef]
87. Maharjan, S.; Zhu, Q.; Zhang, Y.; Gjessing, S.; Basar, T. Dependable demand response management in the smart grid: A Stackelberg game approach. *IEEE Trans. Smart Grid* **2013**, *4*, 120–132. [CrossRef]
88. Zhang, Y.; Krishnan, V.; Pi, J.; Kaur, K.; Srivastava, A.; Hahn, A.; Suresh, S. Cyber physical security analytics for transactive energy systems. *IEEE Trans. Smart Grid* **2019**, *11*, 931–941. [CrossRef]

89. Tan, R.; Nguyen, H.H.; Foo, E.Y.; Yau, D.K.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Modeling and mitigating impact of false data injection attacks on automatic generation control. *IEEE Trans. Inf. Secur.* **2017**, *12*, 1609–1624. [CrossRef]
90. Sun, G.; Cong, Y.; Dong, J.; Wang, Q.; Lyu, L.; Liu, J. Data poisoning attacks on federated machine learning. *IEEE Internet Things J.* **2021**, *9*, 11365–11375. [CrossRef]
91. Dunn, C.; Moustafa, N.; Turnbull, B. Robustness evaluations of sustainable machine learning models against data poisoning attacks in the internet of things. *Sustainability* **2020**, *12*, 6434. [CrossRef]
92. Velliangiri, S.; Kasaraneni, K.K. Machine learning and deep learning in cyber security for IoT. In *Proceedings of the ICDSMLA 2019: Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications*; Springer: Singapore, 2020; pp. 975–981.
93. Handa, A.; Sharma, A.; Shukla, S.K. Machine learning in cybersecurity: A review. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2019**, *9*, e1306. [CrossRef]
94. Chen, C.; Wang, Y.; Cui, M.; Zhao, J.; Bi, W.; Chen, Y.; Zhang, X. Data-driven detection of stealthy false data injection attack against power system state estimation. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8467–8476. [CrossRef]
95. Bi, J.; Luo, F.; Liang, G.; Yang, X.; He, S.; Dong, Z.Y. Impact Assessment and Defense for Smart Grids with FDIA Against AMI. *IEEE Trans. Netw. Sci. Eng.* **2022**, 1–13. [CrossRef]
96. Saber, A.M.; Youssef, A.; Svetinovic, D.; Zeineldin, H.H.; El-Saadany, E.F. Anomaly-Based Detection of Cyberattacks on Line Current Differential Relays. *IEEE Trans. Smart Grid* **2022**, *13*, 4787–4800. [CrossRef]
97. Abdel-Basset, M.; Moustafa, N.; Hawash, H. Privacy-Preserved Generative Network for Trustworthy Anomaly Detection in Smart Grids: A Federated Semisupervised Approach. *IEEE Trans. Ind. Inform.* **2022**, *19*, 995–1005. [CrossRef]
98. Luo, H.; Zhu, H.; Liu, S.; Liu, Y.; Zhu, X.; Lai, J. 3-D Auxiliary Classifier GAN for Hyperspectral Anomaly Detection via Weakly Supervised Learning. *IEEE Geosci. Remote Sens. Lett.* **2022**, *19*, 6009805. [CrossRef]
99. Zheng, X.; Xu, N.; Trinh, L.; Wu, D.; Huang, T.; Sivaranjani, S.; Liu, Y.; Xie, L. A multi-scale time-series dataset with benchmark for machine learning in decarbonized energy grids. *Sci. Data* **2022**, *9*, 359. [CrossRef]
100. Cao, J.; Wang, D.; Wang, Q.-M.; Yuan, X.-L.; Wang, K.; Chen, C.-L. Network Attack Detection Method of the Cyber-Physical Power System Based on Ensemble Learning. *Appl. Sci.* **2022**, *12*, 6498. [CrossRef]
101. Zhang, Q.; Bai, J.; Liu, Y.; Zhou, Y. Classifying Dynamic Motor Imagery with the Locals-Balanced Extreme Learning Machine. *SSRN* **2022**, 10. [CrossRef]
102. Gui, Y.; Siddiqui, A.S.; Tamore, S.M.; Saqib, F. Security vulnerabilities of smart meters in smart grid. In Proceedings of the IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, 14–17 October 2019; pp. 3018–3023.
103. Konstantinou, C.; Maniatakos, M. Hardware-layer intelligence collection for smart grid embedded systems. *J. Hardw. Syst. Secur.* **2019**, *3*, 132–146. [CrossRef]
104. Siddiqui, A.S.; Gui, Y.; Lawrence, D.; Laval, S.; Plusquellic, J.; Manjrekar, M.; Chowdhury, B.; Saqib, F. Hardware assisted security architecture for smart grid. In Proceedings of the IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 2890–2895.
105. Nath, A.P.D.; Amsaad, F.; Choudhury, M.; Niamat, M. Hardware-based novel authentication scheme for advanced metering infrastructure. In Proceedings of the 2016 IEEE National Aerospace and Electronics Conference (NAECON) and Ohio Innovation Summit (OIS), Dayton, OH, USA, 25–29 July 2016; pp. 364–371.
106. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 13–27. [CrossRef]
107. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
108. Javed, A.R.; Usman, M.; Rehman, S.U.; Khan, M.U.; Haghighi, M.S. Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4291–4300. [CrossRef]
109. Zhou, A.; Li, Z.; Shen, Y. Anomaly detection of CAN bus messages using a deep neural network for autonomous vehicles. *Appl. Sci.* **2019**, *9*, 3174. [CrossRef]
110. Papernot, N.; McDaniel, P. Deep k-nearest neighbors: Towards confident, interpretable and robust deep learning. *arXiv* **2018**, arXiv:1803.04765.
111. Sheatsley, R.; Durbin, M.; Lintereur, A.; McDaniel, P. Improving radioactive material localization by leveraging cyber-security model optimizations. *IEEE Sens. J.* **2021**, *21*, 9994–10006. [CrossRef]
112. Larriva-Novo, X.; Vega-Barbas, M.; Villagra, V.A.; Rivera, D.; Alvarez-Campana, M.; Berrocal, J. Efficient distributed preprocessing model for machine learning-based anomaly detection over large-scale cybersecurity datasets. *Appl. Sci.* **2020**, *10*, 3430. [CrossRef]
113. Podder, P.; Bharati, S.; Mondal, M.; Paul, P.K.; Kose, U. Artificial neural network for cybersecurity: A comprehensive review. *arXiv* **2021**, arXiv:2107.01185.
114. Mathai, K.J. Performance comparison of intrusion detection system between deep belief network (DBN) algorithm and state preserving extreme learning machine (SPELM) algorithm. In Proceedings of the 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 20–22 February 2019; pp. 1–7.
115. Huda, S.; Yearwood, J.; Hassan, M.M.; Almogren, A. Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. *Appl. Soft Comput.* **2018**, *71*, 66–77. [CrossRef]

116. Nguyen, G.N.; Le Viet, N.H.; Elhoseny, M.; Shankar, K.; Gupta, B.; Abd El-Latif, A.A. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *J. Parallel Distrib. Comput.* **2021**, *153*, 150–160. [CrossRef]
117. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *9*, 5294–5310. [CrossRef]
118. Lin, T.-N.; Giles, C.L.; Horne, B.G.; Kung, S.-Y. A delay damage model selection algorithm for NARX neural networks. *IEEE Trans. Signal Process.* **1997**, *45*, 2719–2730.
119. Ullah, I.; Mahmoud, Q.H. Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access* **2021**, *9*, 103906–103926. [CrossRef]
120. Kravchik, M.; Shabtai, A. Detecting cyber attacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, Toronto, ON, Canada, 15–19 October 2018; pp. 72–83.
121. Susilo, B.; Sari, R.F. Intrusion detection in IoT networks using deep learning algorithm. *Information* **2020**, *11*, 279. [CrossRef]
122. McLaughlin, N.; del Rincon, J.M.; Kang, B.; Yerima, S.; Miller, P.; Sezer, S.; Safaei, Y.; Trickel, E.; Zhao, Z.; Doupé, A.; et al. Deep android malware detection. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, Scottsdale, AZ, USA, 22–24 March 2017; pp. 301–308.
123. Li, Y.; Xu, Y.; Liu, Z.; Hou, H.; Zheng, Y.; Xin, Y.; Zhao, Y.; Cui, L. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement* **2020**, *154*, 107450. [CrossRef]
124. Kaddoura, S.; Alfandi, O.; Dahmani, N. A spam email detection mechanism for English language text emails using deep learning approach. In Proceedings of the 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Bayonne, France, 10–13 September 2020; pp. 193–198.
125. Prakash, A.; Priyadarshini, R. An intelligent software defined network controller for preventing distributed denial of service attack. In Proceedings of the 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 20–21 April 2018; pp. 585–589.
126. Meti, N.; Narayan, D.; Baligar, V. Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017; pp. 1366–1371.
127. Mulyanto, M.; Faisal, M.; Prakosa, S.W.; Leu, J.-S. Effectiveness of focal loss for minority classification in network intrusion detection systems. *Symmetry* **2021**, *13*, 4. [CrossRef]
128. Ravipati, R.D.; Abualkibash, M. Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets-a review paper. *Int. J. Comput. Sci. Inf. Technol. (IJCSIT)* **2019**, *11*, 1–16. [CrossRef]
129. Abrar, I.; Ayub, Z.; Masoodi, F.; Bamhdi, A.M. A machine learning approach for intrusion detection system on NSL-KDD dataset. In Proceedings of the 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 10–12 September 2020; pp. 919–924.
130. Gao, X.; Shan, C.; Hu, C.; Niu, Z.; Liu, Z. An adaptive ensemble machine learning model for intrusion detection. *IEEE Access* **2019**, *7*, 82512–82521. [CrossRef]
131. Kocher, G.; Kumar, G. Performance analysis of machine learning classifiers for intrusion detection using unsw-nb15 dataset. *Comput. Sci. Inf. Technol.(CS IT)* **2020**, *10*, 31–40.
132. Kasongo, S.M.; Sun, Y. Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *J. Big Data* **2020**, *7*, 105. [CrossRef]
133. Russel, M.O.F.K.; Rahman, S.S.M.M.; Islam, T. A large-scale investigation to identify the pattern of app component in obfuscated Android malwares. In Proceedings of the Machine Learning, Image Processing, Network Security and Data Sciences: Second International Conference, MIND 2020, Proceedings Part II 2, Silchar, India, 30–31 July 2020; pp. 513–526.
134. Singh, M. User-Centered Spam Detection Using Linear and Non-Linear Machine Learning Models. 2019. Available online: https://dspace.library.uvic.ca/handle/1828/10751 (accessed on 15 January 2023).
135. Ding, Y.; Zhai, Y. Intrusion detection system for NSL-KDD dataset using convolutional neural networks. In Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence, Shenzhen, China, 8–10 December 2018; pp. 81–85.
136. Gamage, S.; Samarabandu, J. Deep learning methods in network intrusion detection: A survey and an objective comparison. *J. Netw. Comput. Appl.* **2020**, *169*, 102767. [CrossRef]
137. Potluri, S.; Ahmed, S.; Diedrich, C. Convolutional neural networks for multi-class intrusion detection system. In Proceedings of the Mining Intelligence and Knowledge Exploration: 6th International Conference, MIKE 2018, Proceedings 6, Cluj-Napoca, Romania, 20–22 December 2018; pp. 225–238.
138. Ferrag, M.A.; Maglaras, L.; Janicke, H.; Smith, R. Deep learning techniques for cyber security intrusion detection: A detailed analysis. In Proceedings of the 6th International Symposium for ICS & SCADA Cyber Security Research 2019, Athens, Greece, 10–12 September 2019; pp. 126–136.
139. Muhuri, P.S.; Chatterjee, P.; Yuan, X.; Roy, K.; Esterline, A. Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks. *Information* **2020**, *11*, 243. [CrossRef]
140. Sun, P.; Liu, P.; Li, Q.; Liu, C.; Lu, X.; Hao, R.; Chen, J. DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. *Secur. Commun. Netw.* **2020**, *2020*, 8890306. [CrossRef]

141. Khan, R.U.; Zhang, X.; Alazab, M.; Kumar, R. An improved convolutional neural network model for intrusion detection in networks. In Proceedings of the 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, VIC, Australia, 8–9 May 2019; pp. 74–77.
142. Hasan, M.N.; Toma, R.N.; Nahid, A.-A.; Islam, M.M.; Kim, J.-M. Electricity theft detection in smart grid systems: A CNN-LSTM based approach. *Energies* **2019**, *12*, 3310. [CrossRef]
143. Tian, J.; Wang, B.; Li, J.; Wang, Z. Adversarial attacks and defense for CNN based power quality recognition in smart grid. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 807–819. [CrossRef]
144. Rouzbahani, H.M.; Karimipour, H.; Lei, L. An ensemble deep convolutional neural network model for electricity theft detection in smart grids. In Proceedings of the 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Toronto, ON, Canada, 11–14 October 2020; pp. 3637–3642.
145. Doshi, F.; Pineau, J.; Roy, N. Reinforcement learning with limited reinforcement: Using Bayes risk for active learning in POMDPs. In Proceedings of the 25th International Conference on Machine Learning, Helsinki, Finland, 5–9 July 2008; pp. 256–263.
146. Liu, Y.; Cheng, L. Relentless false data injection attacks against Kalman-filter-based detection in smart grid. *IEEE Trans. Control Netw. Syst.* **2022**, *9*, 1238–1250. [CrossRef]
147. Chen, J.; Wang, Y.; Lan, T. Bringing fairness to actor-critic reinforcement learning for network utility optimization. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021; pp. 1–10.
148. Mekni, M.; Jayaramireddy, C.S.; Naraharisetti, S.V.V.S.S. Reinforcement Learning Toolkits for Gaming: A Comparative Qualitative Analysis. *J. Softw. Eng. Appl.* **2022**, *15*, 417–435. [CrossRef]
149. Yu, D.; Ma, Z.; Wang, R. Efficient smart grid load balancing via fog and cloud computing. *Math. Probl. Eng.* **2022**, *2022*, 3151249. [CrossRef]
150. Kaur, M.; Aron, R. A systematic study of load balancing approaches in the fog computing environment. *J. Supercomput.* **2021**, *77*, 9202–9247. [CrossRef]
151. Tran, C.H.; Bui, T.K.; Pham, T.V. Virtual machine migration policy for multi-tier application in cloud computing based on Q-learning algorithm. *Computing* **2022**, *104*, 1285–1306. [CrossRef]
152. Singh, G.; Malhotra, M.; Sharma, A. An adaptive mechanism for virtual machine migration in the cloud environment. *Int. J. Cloud Appl. Comput. (IJCAC)* **2022**, *12*, 1–10. [CrossRef]
153. Cai, T.; Dong, M.; Liu, H.; Nojavan, S. Integration of hydrogen storage system and wind generation in power systems under demand response program: A novel p-robust stochastic programming. *Int. J. Hydrog. Energy* **2022**, *47*, 443–458. [CrossRef]
154. Fan, S.; Wang, X.; Cao, S.; Wang, Y.; Zhang, Y.; Liu, B. A novel model to determine the relationship between dust concentration and energy conversion efficiency of photovoltaic (PV) panels. *Energy* **2022**, *252*, 123927. [CrossRef]
155. Kumari, A.; Chintukumar Sukharamwala, U.; Tanwar, S.; Raboaca, M.S.; Alqahtani, F.; Tolba, A.; Sharma, R.; Aschilean, I.; Mihaltan, T.C. Blockchain-Based Peer-to-Peer Transactive Energy Management Scheme for Smart Grid System. *Sensors* **2022**, *22*, 4826. [CrossRef]
156. Razaque, A.; Al Ajlan, A.; Melaoune, N.; Alotaibi, M.; Alotaibi, B.; Dias, I.; Oad, A.; Hariri, S.; Zhao, C. Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system. *Appl. Sci.* **2021**, *11*, 7880. [CrossRef]
157. Xie, M.; Li, H.; Zhao, Y. Blockchain financial investment based on deep learning network algorithm. *J. Comput. Appl. Math.* **2020**, *372*, 112723. [CrossRef]
158. Alzubi, O.A.; Alzubi, J.A.; Shankar, K.; Gupta, D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4360. [CrossRef]
159. Kim, S.-K.; Huh, J.-H. A study on the improvement of smart grid security performance and blockchain smart grid perspective. *Energies* **2018**, *11*, 1973. [CrossRef]
160. Alladi, T.; Chamola, V.; Rodrigues, J.J.; Kozlov, S.A. Blockchain in smart grids: A review on different use cases. *Sensors* **2019**, *19*, 4862. [CrossRef]
161. Long, C.; Zhou, Y.; Wu, J. A game theoretic approach for peer to peer energy trading. *Energy Procedia* **2019**, *159*, 454–459. [CrossRef]
162. Morstyn, T.; Teytelboym, A.; McCulloch, M.D. Bilateral contract networks for peer-to-peer energy trading. *IEEE Trans. Smart Grid* **2018**, *10*, 2026–2035. [CrossRef]
163. Dorri, A.; Hill, A.; Kanhere, S.; Jurdak, R.; Luo, F.; Dong, Z.Y. Peer-to-peer energytrade: A distributed private energy trading platform. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Republic of Korea, 14–17 May 2019; pp. 61–64.
164. Seven, S.; Yao, G.; Soran, A.; Onen, A.; Muyeen, S. Peer-to-peer energy trading in virtual power plant based on blockchain smart contracts. *IEEE Access* **2020**, *8*, 175713–175726. [CrossRef]
165. Han, D.; Zhang, C.; Ping, J.; Yan, Z. Smart contract architecture for decentralized energy trading and management based on blockchains. *Energy* **2020**, *199*, 117417. [CrossRef]
166. Wongthongtham, P.; Marrable, D.; Abu-Salih, B.; Liu, X.; Morrison, G. Blockchain-enabled Peer-to-Peer energy trading. *Comput. Electr. Eng.* **2021**, *94*, 107299. [CrossRef]
167. He, L.; Liu, Y.; Zhang, J. Peer-to-peer energy sharing with battery storage: Energy pawn in the smart grid. *Appl. Energy* **2021**, *297*, 117129. [CrossRef]

168. Mehdinejad, M.; Shayanfar, H.; Mohammadi-Ivatloo, B. Decentralized blockchain-based peer-to-peer energy-backed token trading for active prosumers. *Energy* **2022**, *244*, 122713. [CrossRef]
169. Sarker, I.H.; Colman, A.; Han, J. Recencyminer: Mining recency-based personalized behavior from contextual smartphone data. *J. Big Data* **2019**, *6*, 49. [CrossRef]
170. Ahsan, M.; Gomes, R.; Chowdhury, M.M.; Nygard, K.E. Enhancing machine learning prediction in cybersecurity using dynamic feature selector. *J. Cybersecur. Priv.* **2021**, *1*, 199–218. [CrossRef]
171. Ahsan, M.; Gomes, R.; Denton, A. Smote implementation on phishing data to enhance cybersecurity. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 531–536.
172. Shi, Y. *Advances in Big Data Analytics*; Springer: Berlin/Heidelberg, Germany, 2022.
173. Freitas, L.O.; Henriques, P.R.; Novais, P. Uncertainty Identification in Context-Aware Systems Using Public Datasets. In *Proceedings of the Ambient Intelligence–Software and Applications–12th International Symposium on Ambient Intelligence*; Springer: Cham, Switzerland, 2022; pp. 115–125.
174. Mantas, J. The hazards of data mining in healthcare. *Inform. Empower. Healthc. Transform.* **2017**, *238*, 80.
175. Gupta, I.; Mittal, S.; Tiwari, A.; Agarwal, P.; Singh, A.K. TIDF-DLPM: Term and inverse document frequency based data leakage prevention model. *arXiv* **2022**, arXiv:2203.05367.
176. Pulido-Gaytan, L.B.; Tchernykh, A.; Cortés-Mendoza, J.M.; Babenko, M.; Radchenko, G. A survey on privacy-preserving machine learning with fully homomorphic encryption. In Proceedings of the High Performance Computing: 7th Latin American Conference, CARLA 2020, Revised Selected Papers 7, Cuenca, Ecuador, 2–4 September 2020; pp. 115–129.
177. Kjamilji, A.; Savaş, E.; Levi, A. Efficient secure building blocks with application to privacy preserving machine learning algorithms. *IEEE Access* **2021**, *9*, 8324–8353. [CrossRef]
178. Mavroeidis, V.; Vishi, K.; Zych, M.D.; Jøsang, A. The impact of quantum computing on present cryptography. *arXiv* **2018**, arXiv:1804.00200. [CrossRef]
179. Thomas, T.; Vijayaraghavan, A.P.; Emmanuel, S. *Machine Learning Approaches in Cyber Security Analytics*; Springer: Singapore, 2020.
180. Chio, C.; Freeman, D. *Machine Learning and Security: Protecting Systems with Data and Algorithms*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2018.