A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions

Article *in* Electronics · March 2023

DOI: 10.3390/electronics12061333

5 authors, including:

Ömer Aslan
Bandirma Onyedi Eylül Üniversitesi
26 PUBLICATIONS **1,012** CITATIONS
SEE PROFILE

Merve Ozkan Okay
Ankara University
26 PUBLICATIONS **446** CITATIONS
SEE PROFILE

Abdullah Asım Yılmaz
Atilim University
18 PUBLICATIONS **432** CITATIONS
SEE PROFILE

electronics

MDPI

Review

A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions

Ömer Aslan [1], Semih Serkant Aktuğ [2], Merve Ozkan-Okay [3,*], Abdullah Asim Yilmaz [4] and Erdal Akin [5]

[1] Department of Software Engineering, Bandırma Onyedi Eylül University, Balıkesir 10200, Turkey
[2] Department of Economics, Siirt University, Siirt 56100, Turkey
[3] Department of Computer Engineering, Ankara University, Ankara 06830, Turkey
[4] Department of Computer Engineering, Atılım University, Ankara 06830, Turkey
[5] Department of Computer Engineering, Bitlis Eren University, Bitlis 13000, Turkey
* Correspondence: merveozkan@ankara.edu.tr; Tel.: +90-0312-203-3300-1707

Abstract: Internet usage has grown exponentially, with individuals and companies performing multiple daily transactions in cyberspace rather than in the real world. The coronavirus (COVID-19) pandemic has accelerated this process. As a result of the widespread usage of the digital environment, traditional crimes have also shifted to the digital space. Emerging technologies such as cloud computing, the Internet of Things (IoT), social media, wireless communication, and cryptocurrencies are raising security concerns in cyberspace. Recently, cyber criminals have started to use cyber attacks as a service to automate attacks and leverage their impact. Attackers exploit vulnerabilities that exist in hardware, software, and communication layers. Various types of cyber attacks include distributed denial of service (DDoS), phishing, man-in-the-middle, password, remote, privilege escalation, and malware. Due to new-generation attacks and evasion techniques, traditional protection systems such as firewalls, intrusion detection systems, antivirus software, access control lists, etc., are no longer effective in detecting these sophisticated attacks. Therefore, there is an urgent need to find innovative and more feasible solutions to prevent cyber attacks. The paper first extensively explains the main reasons for cyber attacks. Then, it reviews the most recent attacks, attack patterns, and detection techniques. Thirdly, the article discusses contemporary technical and nontechnical solutions for recognizing attacks in advance. Using trending technologies such as machine learning, deep learning, cloud platforms, big data, and blockchain can be a promising solution for current and future cyber attacks. These technological solutions may assist in detecting malware, intrusion detection, spam identification, DNS attack classification, fraud detection, recognizing hidden channels, and distinguishing advanced persistent threats. However, some promising solutions, especially machine learning and deep learning, are not resistant to evasion techniques, which must be considered when proposing solutions against intelligent cyber attacks.

Keywords: cyber security; cyber attacks; cyber threats; network security

Citation: Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics* **2023**, *12*, 1333. https://doi.org/10.3390/electronics12061333

Academic Editor: Wojciech Mazurczyk

Received: 11 February 2023
Revised: 4 March 2023
Accepted: 7 March 2023
Published: 11 March 2023

1. Introduction

The Internet, which emerged as a communication and sharing environment, quickly impacted the geography of the whole world. In particular, the 21st century has been and continues to be the century in which world geography is intertwined with the Internet network. Hence, people worldwide can communicate with each other at high speeds through the Internet, and a strong bond has been formed between states in critical commercial, political, economic, and sociocultural fields. The Internet has three basic entities: computers, users, and networks [1]. It has been observed that network technologies have developed thanks to constantly changing computer technologies and user segments that have started to have various abilities. However, the developing and widespread use of network technologies has also brought about critical security problems. Therefore, attempts

have been made to provide a cyber security environment to protect the assets of institutions, organizations, and individuals [2].

The word "cyber" is used to describe networks with infrastructure information systems [3], also referred to as "virtual reality". Cyber security protects the security, integrity, and confidentiality of communication, life, integration, tangible or intangible assets, and data in an electronic environment established by institutions, organizations, and individuals in information systems. In summary, cyber security ensures the security of virtual life on cyber networks. The infrastructure of information systems data integrity protection, and confidentiality are protected under the name of cyber security [4]. The primary purpose of cyber security is to secure the data of individuals and institutions on the Internet. Ignorance of this vital issue can cause serious threats. For instance, someone with malicious intentions can infiltrate devices over the network and hijack the data [5] or steal user credentials such as credit card details or user ID passwords. Such attacks may cause financial damage to individuals, institutions, big companies, and even state governments. According to recent studies, cyberattacks cost billions of dollars to the world economy. Nowadays, cyber attacks are not just simple computer attacks but big businesses that large companies and state governments support. Each example is a cyber attack that can only be prevented with a good cyber security policy [6].

Considering all these mentioned points/aspects together, in this study, we aim to conduct a comprehensive analysis explaining the basics and importance of cyber security. In this context, all aspects of cyber security were discussed, shared risks and threats were presented, and solutions to prevent them were examined and discussed. A guided study was conducted for researchers in this field, from the fundamentals of cyber and network security to common attacks.

To facilitate a more transparent and precise understanding of the paper's language, frequently used phrases and their acronyms are listed in Table 1. This review paper is, to our knowledge, the most comprehensive article on cyber security from all perspectives. It differs from previous survey papers in many aspects. Previous studies mainly focused on one or two subjects, such as cyber security threats, attacks, using blockchain technology, using machine learning techniques in cyber security, challenges, or historical development [7–13]. In contrast, this study discusses various aspects of cyber security in detail. To understand the cyber security problem altogether, we break down the problem into smaller pieces, with each piece extensively covered in different sections. Each section lists the attack vector, possible remedies for each attack class, and challenges. Although some sections mention the same or similar information (threats, vulnerabilities, attacks, etc.), the aspects of the depicted information are different. Moreover, in some sections, more detailed information is provided on similar subjects. This paper contributes to researchers and anyone who wants to learn more about cyber security, from essential to advanced levels. The main topics covered in the article are summarized as follows:

Table 1. Most used phrases and their acronyms.

Phrase	Acronym
Authentication, Authorization, and Accounting	AAA
Access Control List	ACL
Address Resolution Protocol	ARP
Advanced Research Projects Agency Network	ARPANET
Amazon Web Services	AWS
Apple Filing Protocol	AFP
Bridge Protocol Data Unit	BPDU
Change Cipher Specification	CCS

Table 1. *Cont.*

Phrase	Acronym
Compatible Time-Sharing System	CTSS
Computer Network Attacks	CNAs
Confidentiality, Integrity, and Availability	CIA
Content Access Memory	CAM
Coronavirus	COVID-19
Cross-Site Scripting	XSS
Department of Defense	DoD
Distributed Denial of Service	DDoS
Distributed Network Protocol 3	DNP3
Domain Name System	DNS
Dynamic Host Configuration Protocol	DHCP
Email Security Appliance	ESA
General Public License	GPL
Gratuitous ARP	GARP
HyperText Markup Language	HTML
HyperText Transfer Protocol	HTTP
Hypertext Transfer Protocol Secure	HTTPS
Independent Computing Architecture	ICA
Internet Control Message Protocol	ICMP
Internet Message Access Protocol	IMAP
Internet of Things	IoT
Internet Protocol	IP
Internet Protocol Security	IPsec
Internet Protocol Versions 4	IPv4
Internet Protocol Versions 6	IPv6
Intrusion Detection, Prevention, and Protection Systems	IDPS
Lightweight Presentation Protocol	LPP
Linear Discriminant Analysis	LDA
Local Area Network	LAN
Machine Learning	ML
Mail Transfer Agent	MTA
Malicious Software	Malware
Microsoft Baseline Security Analyzer	MBSA
Media Access Control	MAC
Network Data Representation	NDR
Network Time Protocol	NTP
NetWare Core Protocol	NCP
International Organization for Standardization	ISO
Open Systems Interconnection	OSI
Password Authentication Protocol	PAP

Table 1. *Cont.*

Phrase	Acronym
Peer-to-Peer	P2P
Personal Identification Number	PIN
Post Office Protocol 3	POP3
Principal Component Analysis	PCA
Quality of Service	QoS
Real-Time Transport Control Protocol	RTCP
Remote Procedure Calls	RPCs
Secure Socket Layer	SSL
Security Development Lifecycle	SDL
Serial Line Internet Protocol	SLIP
Service Set Identifier	SSID
Session Control Protocol	SCP
Simple Mail Transfer Protocol	SMTP
Simple Network Management Protocol	SNMP
Software Defined Network	SDN
Spanning Tree Protocol	STP
Structured Query Language	SQL
Supervisory Control and Data Acquisition	SCADA
Support Vector Machine	SVM
Synchronize	SYN
TCP Reset	TCP RST
TELetype NETwork	TELNET
Top-Level Domain	TLD
File Transfer Protocol	FTP
Transmission Control Protocol	TCP
Transport Layer Security	TLS
Trusted Computer System Evaluation Criteria	TCSEC
User Datagram Protocol	UDP
Virtual LAN	VLAN
Virtual Machine Monitor	VMM
Virtual Private Network	VPN
Web Security Appliance	WSA
Wired Equivalent Privacy	WEP
Wireless Sensor Networks	WSNs

1. Cyber Security Fundamentals

This section covers the history of cyber crime and the fundamentals of security. It discusses the basic principles of possible cyber security solutions and why cyber attacks have increased. Additionally, it emphasizes the importance of cyber security, explores cyber attacks from both technical and nontechnical perspectives, and proposes measures that can be taken to address them.

2. **Threats, Vulnerabilities, Exploits, and Attacks**

This part of the study extensively discusses widely known cyber threats, security risks, vulnerabilities, and attacks. First, viruses, Trojans, worms, rootkits, and hackers are examined as cyber threats. Then, known threats such as spyware, scareware, joke programs, and ransomware are explained. Next, security vulnerabilities and primarily used vulnerability scanning tools are presented. Finally, the most common types of attacks, from social engineering attacks to applications, cryptography, hijacking, computer networks, phishing, malware, bots, and botnets, as well as password and man-in-the-middle attacks, are discussed in detail. Recommendations, precautions, and awareness for each type of attack are also included.

3. **Network Security**

In this section, the details of the network security issue are presented. The Open Systems Interconnection (OSI) model, its layers, and layer protocols are explained first. Next, the attacks against each layer are examined in detail. Next, network protection devices and tools are described. Finally, wireless network security, attacks on wireless networks, and security methods are discussed.

The contributions of this study, which were made by considering the topics mentioned above in detail, are summarized below:

- The current situation and deficiencies of the cyber security field and the technological developments in this context are explained;
- Basic information about cyber security fundamentals is provided;
- Cyber security risks, threats, attacks, and current studies in these areas are presented;
- Network security, OSI layers, and attacks on each layer are explained;
- Existing challenges, problems, and new assumptions are proposed.

Considering the mentioned contributions, this study has some advantages for researchers in this field:

- The importance of cyber security can be understood;
- Even a beginner researcher can learn the basics of cyber security;
- One can easily obtain information about the most known and common threats and attack types;
- One can be informed about the latest current studies in this field;
- One can acquire a systematic overview of the cyber security field for further studies.

The rest of the article is organized as follows. Section 2 gives basic information about cyber security fundamentals. Section 3 explains the well-known threats, vulnerabilities, exploits, and cyber attacks. General information about network security is presented in Section 4, and Section 5 describes cyber security solutions, recommendations, challenges in their implementation, and directions for future research. Finally, the conclusion is given in Section 6.

2. Cyber Security Fundamentals

In this section, the history of cyber crime and security fundamentals are explained. Additionally, the importance of cyber security, the reasons for the increasing number of cyber attacks from both technical and nontechnical perspectives, and potential countermeasures are discussed.

2.1. History of Cyber Crime and Cyber Security

There have been different definitions for cyber security, such as data security, information security, network security, and cyber security, when protecting data in a digital world. Data security aims to protect digital data from unauthorized access, modification, or disclosure throughout its lifecycle [14]. Information security is the practice of preventing unauthorized access, use, disclosure, modification, review, recording, or destruction of physical or electronic information [15]. The primary purpose of information security is

to protect the confidentiality, integrity, and availability of data. Network security aims to safeguard the confidentiality, integrity, and accessibility of computer networks and data transmitted in communication media [16]. On the other hand, cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, computer networks, and data from malicious attacks. While data security, information security, and network security aim to prevent unauthorized access, use, modification, or destruction of stored data or data in transit, cyber security has a much wider application area that covers end-to-end information flows. Nowadays, the term "cyber security" is mainly being used.

Cyber crime started several years ago. At that time, it was easier to defend the digital world because there were fewer machines in the digital environment, and the attacks were not as complicated as they are now. However, technological developments have allowed cyber criminals to build automated tools to launch sophisticated cyber attacks over time. Additionally, various machines and platforms have been added to the Internet, including smartphones, tablets, IoT devices, cloud platforms, social media platforms, and many more [17]. All of these reasons have made cyber crime evolve from simple jokes to sophisticated attacks that cost trillions of dollars to the world economy annually in the digital environment. The classification of cyber crimes over the decades is given in Table 2.

Table 2. The classification of cyber crimes over the decades.

Period	Cyber Crimes
1940s	Years without computer crime
1950s	Phone phreaking decade
1960s	Hacking and vulnerability terms appear
1970s	Born of computer security
1980s	The years of ARPANET to Internet
1990s	Computer viruses and worms have become popular
2000s	The Internet grows excessively
2010s	Cyber criminals discover several security breaches in computer systems
2020s	Cyber crimes have become an industry

The first computers appeared in the early 1940s [18]. At that time, there was no Internet connection, and only limited usage of computers was possible. Since there was no information sharing between computers, there were no threats or attacks on computers. Phone phreaking started in the 1950s. Phone phreaks attempted to hijack the protocols used in the phone systems to make free calls or reduce the phone call fees for long distances. At that time, several phone companies could not prevent phone phreaking. In the future, similar techniques to phone phreaking would be used to hack computer systems.

The term "hacking" for computer systems first appeared in the 1960s. In 1965, the first vulnerability was found in the IBM 7094 Compatible Time-Sharing System (CTSS) machine [19]. In 1967, IBM hired a group of students to explore their newly designed computer [18]. The students learned the computer system's language and gained access to different system parts. This example proved that computer systems have vulnerabilities, and this case was the first example of the ethical hacking practice. The foundation of cyber security began in the early 1970s with a project called "The Advanced Research Projects Agency Network" (ARPANET). This was the first packet-switched network before the Internet. In 1971, Bob Thomas created the first virus called the "Creeper", which could move over an ARPANET network [20]. Following the "Creeper", Ray Tomlinson created "Reaper", which could also move across the ARPANET and delete the "Creeper" [21]. "Reaper" was the first example of an antivirus program. In 1979, a famous hacker, Kevin Mitnick, was arrested for the first time for cyber criminal behavior [20].

Several computer-related attacks were seen in the 1980s. Mainly, computer viruses were used in this decade. The term "cyber espionage" began to be used in this period because a significant fear was the threat from other governments. In 1985, the United States of America (USA) Department of Defense (DoD) created computer security guidelines called "Trusted Computer System Evaluation Criteria" (TCSEC), which were later named "Orange Book" [22,23]. The TCSEC was the first security guide for computer systems. In 1986, German hacker Marcus Hess infiltrated the systems of the governments of the USA, East Asia, and Europe [24]. He could access around 400 military computers. The hacked information included space, satellite, and aircraft technologies [25]. Security became a primary concern for businesses at this time. Commercial antivirus software was first released in 1987 [18]. In the 1990s, there was tremendous growth in computer systems and the Internet. The computer virus and its different versions became very popular. Macroviruses were released in 1996. In the late 1990s, the Melissa and ILOVEYOU viruses infected millions of computers across many countries [26]. In 1995, Netscape introduced the Secure Sockets Layer (SSL) protocol, which secured user connections over a computer network.

Throughout the 2000s, the Internet grew exponentially, and computers became increasingly common in work and home environments. While the widespread use of computers has increased productivity, it has also introduced security risks for many users. In other words, the increased usage of computers has also increased cyber crime. The first organized hacker group emerged in the 2000s, and computer worms and Trojans became popular attack methods. Simply visiting an infected website was enough to contract a virus without downloading files. In 2004, the MyDoom worm was responsible for distributed denial of service (DDoS) attacks and remote access [26]. In 2007, the Zeus Trojan used drive-by downloads and spam emails to steal login credentials, including bank, social networking, and email accounts.

During the 2010s, cyber criminals identified several security breaches in software and computer network protocols. These breaches resulted in individuals losing millions of dollars and big companies and countries losing billions yearly. In 2016, Mirai malware exploited an IoT device vulnerability to launch DDoS attacks [27]. Between 2010 and 2020, ransomware-related attacks became increasingly popular. The WannaCry ransomware, for example, encrypted computer systems and affected 150 countries across the globe [28,29], while the LockerGoga ransomware blocked infected systems and caused millions of dollars in damage [30]. In 2020, the CovidLock ransomware encrypted data on Android devices and denied access to the data [31], affecting several Android devices.

In the 2020s, hacking almost anything in the digital world is possible. Some professional websites even provide automatic applications and tools for hacking as a service [32]. Cyber attacks that are timely and effective can result in huge profits, which is why big companies and governments are investing heavily in this area [33]. The evolution of cyber attacks over the years can be seen in Table 3.

The methods used to spread attacks have changed over time. Vulnerabilities in hardware, software, and networks, phishing scams, and social engineering techniques are all commonly used. These attacks are often spread through drive-by downloads, malicious email attachments, and fake applications (Table 3). With the development of new attack tools, it is now possible to access someone's banking system, steal sensitive data from big companies, encrypt computer data on hard drives, and prevent access to big companies' resources by launching DDoS attacks. These attacks cost billions of dollars annually across the globe. In addition, new devices such as smartphones and IoT devices have increased attack surfaces. Cyber criminals constantly elaborate on existing cyber attacks by generating different versions and using new attack variants for smartphones and IoT devices. Recent studies have shown that fake applications, backdoors, and banking Trojans are rising for mobile devices [34]. Furthermore, cyber attacks related to social media, IoT devices, cryptocurrency, and the cloud computing environment are also increasing.

Table 3. The evolution of cyber attacks over the years [26–31].

Cyber-Related Attack	Year	Attack Spread Method	Consequences
Vladimir Levin's Attack the Citibank1	1994–1995	unknown	around 10 million dollars were stolen
Melissa Virus	1999	used users' trust to click an email attachment	billions of dollars were lost in many countries
ILOVEYOU Worm3	2000	used users' trust to click an email attachment	more than 45 million computers were infected
MyDoom worm4	2004	used attention-grabbing subjects by email, such as errors, tests, etc.	DDoS attacks by allowing remote access was launched
Zeus Trojan	2007	spam email with drive-by downloads	login details such as email and bank accounts were stolen
Stuxnet Worm	2010	attack the programmable logic unit by stealing source codes	control of industrial processes was taken
Attack on USA Natural Gas Pipeline	2012	accessing confidential information through phishing	security credentials were stolen
Mirai Malware	2016	vulnerability of IoT devices was exploited	DDoS attacks were launched
WannaCry Ransomware	2017	windows vulnerability was exploited	computer hard drives were encrypted, and 150 countries were affected
Emotet Trojan	2018	emails in the form of spam and phishing campaigns	sensitive information such as credit card details was stolen
MyFitnessPal	2018	software vulnerability was exploited	150 million users were affected
Ransomware Attack on Magellan	2020	emails in the form of spam and phishing campaigns	health data of 365,000 patients were stolen
CovidLock Ransomware	2020	exploited users' trust by using COVID-19 statistic	android devices' data were encrypted, and data access was denied
Accellion Supply Chain Attack	2021	third-party vulnerabilities were exploited	confidential data from large organizations were stolen
Kaseya Ransomware Attack	2021	zero-day exploits were used	around 1500 companies' data were compromised with the request of 50,000 to 5 million dollar ransoms per victim

2.2. Principle of Information Security

Figure 1 illustrates the three dimensions of cyber security. The first dimension is focused on protecting information from attackers, also known as the "principle of information security." This principle includes the concepts of confidentiality, integrity, and availability (CIA) [35]. The second dimension of cyber security aims to protect data in all states, whether in storage, transit [36], or in process. For example, data can be transferred between devices using Sneakernet, wired, and wireless networks. Therefore, cyber security measures must ensure data confidentiality, integrity, and availability when data are stored or transmitted between network devices and hosts (Figure 1). Finally, the third dimension of cyber security involves using additional tools, such as policies and practices, new technologies, and user awareness, to assist in protecting cyberspace.

The principles of information security, including confidentiality, integrity, and availability, are explained as follows.

2.2.1. Confidentiality

Confidentiality is the protection of information from unauthorized users and programs in the digital world. Data can be categorized as Top Secret, Secret, Confidential, and Unclassified [37]. Top Secret and Secret data are crucial and require the highest levels of

protection, as their disclosure can cause enormous damage to national security. Hence, access to such data must be strictly restricted. Confidential data are also sensitive and should not be disclosed. On the other hand, unclassified data are not sensitive and are publicly available to anyone, with no impact on national security. Therefore, governments, organizations, and companies must train employees to safeguard their valuable assets from cyber attackers, including Top Secret, Secret, and Confidential Information. To maintain the confidentiality of data, encryption, authentication, and access control techniques can be used.

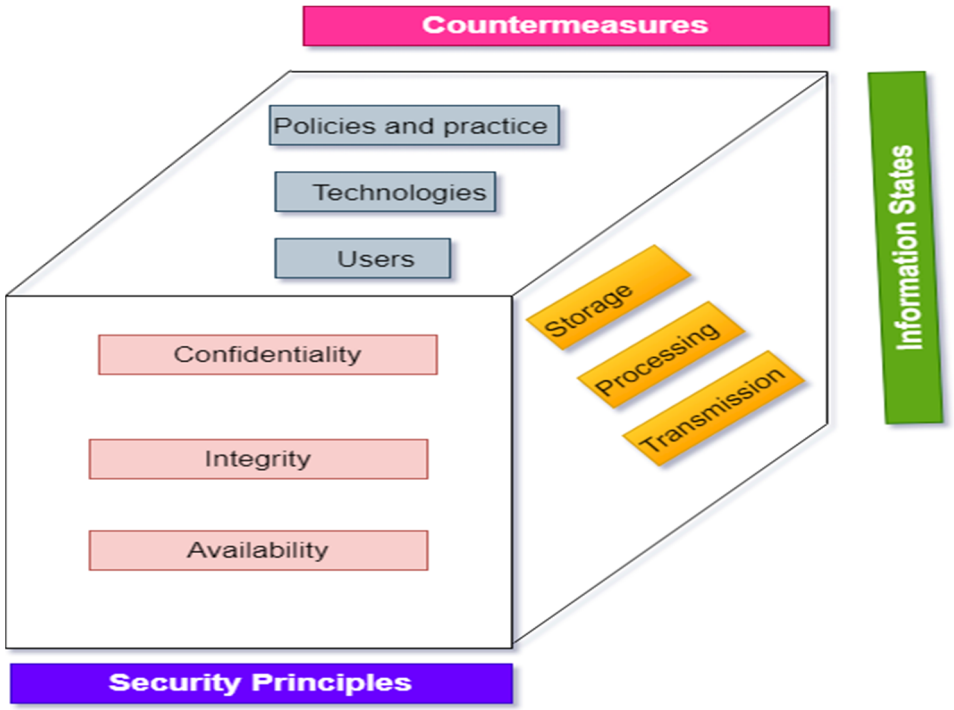

Figure 1. Three dimensions of cyber security.

Encryption is a mathematical technique that converts the original information into an unreadable version, concealing it from unauthorized access [38]. Encryption has been extensively used in cyber security to safeguard computer systems and data from brute-force attacks, spyware, and ransomware. Access control identifies various protection mechanisms that prevent unauthorized access to computer systems and networks. Access control is a fundamental security concept that minimizes the risk for organizations. The concept of AAA provides three security services: Authentication, Authorization, and Accounting. Authentication prevents unauthorized access by verifying the users' identities through a username–password combination [39]. Authorization identifies which computer and network resources users can access and which operations they can perform [40]. Accounting monitors users' activities, the resources they access, and the changes they make. In the later sections, we explain in detail how encryption, authentication, and access control work.

2.2.2. Integrity

Integrity is related to data accuracy, quality, consistency, and completeness [41] during their entire life cycle. To ensure its integrity, information can be changed only by users with the right to change it. Data integrity is a top priority for modern enterprises for various reasons [42]. Data integrity ensures recoverability, traceability, and connectivity. Data integrity can be lost due to physical device compromise, disk crashes, malware, hacking, inconsistent formats, data transfer errors among devices, and human error. Hashing, data consistency checks, and data validation checks can be used to preserve data integrity.

2.2.3. Availability

Availability is related to data accessibility. In other words, data are available when an authorized user requests or uses them [43]. System failures and cyber attacks may prevent access to information systems and services. DDoS attacks are one of the most destructive cyber attacks that target a system's availability when legitimate users try to access it. Unfortunately, there is no well-known system that completely stops DDoS attacks. To ensure availability, system backups, system redundancy, system resiliency, and up-to-date operating systems, as well as software, must be used. In addition, the system should eliminate single points of failure and detect failures as soon as they occur.

2.3. Why Cyber Attacks Are Increasing

In recent years, the importance and use of the Internet have rapidly increased worldwide. This increase has led to the transfer of daily life to the digital world. The COVID-19 (2019 Coronavirus disease) epidemic accelerated this process. For example, people now develop friendships in social media environments, access online banking systems, and plan online seminars and meetings (Figure 2). These reasons have also led to the transfer of daily crimes to the Internet. Cyber crime is carried out by individuals or organized groups known as hackers. Hackers have in-depth knowledge of operating systems, can write computer programs quickly, and can detect program and system vulnerabilities in a short period [44]. The development of new attack tools, as well as the tremendous economic benefit, motivates cyber attackers. According to recent studies, the damage caused by cyber attacks to the world economy is expressed in trillions of dollars, and this damage is increasing gradually. For the reasons mentioned above, cyber-related attacks are increasing day by day. Before discussing these attacks in detail, reviewing the main reasons that cause and motivate cyber attacks is beneficial. The major reasons for cyber attacks can be listed as follows (Figure 2):

1. Causes arise from existing system errors;
2. Causes arising from emerging technologies;
3. Reasons arising from the increase in knowledge;
4. Transferring daily life into a digital environment;
5. The attacks have no geographical boundaries, which makes detecting attacks challenging.

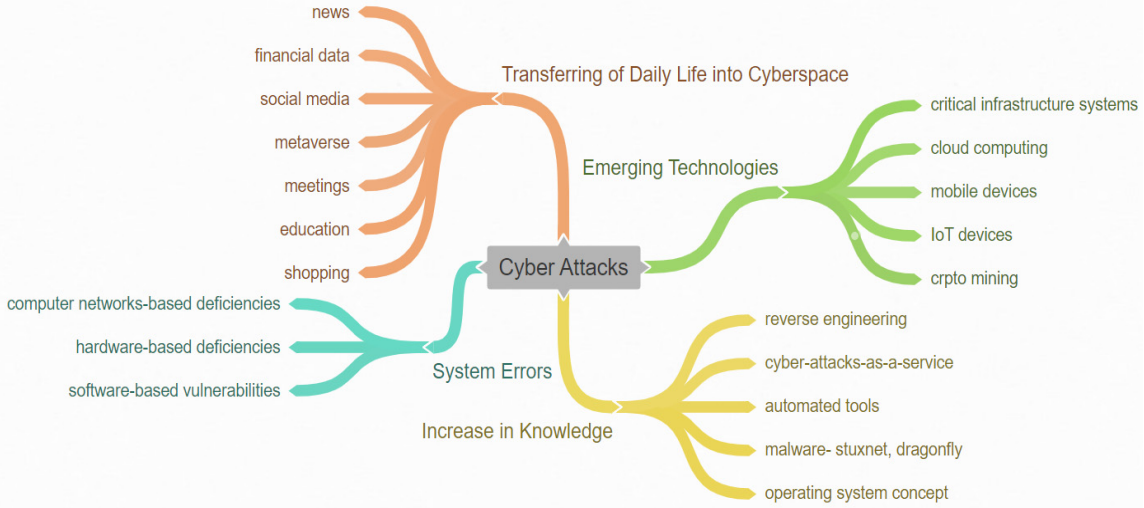

Figure 2. Main reasons for cyber attacks.

2.3.1. Causes Arising from Existing System Errors

The main reason for the rapid increase in cyberattacks is the structure of computer systems and communication networks. The vulnerabilities, deficiencies, and misconfigurations in hardware, software, and computer networks expose the systems to attacks that

hackers exploit. Due to the high number of software-based vulnerabilities and deficiencies in protocols in computer networks, the system becomes defenseless against cyberattacks. Additionally, users who lack knowledge about the digital environment and how to use computer systems also contribute to the causes of cyberattacks. The causes arising from existing system errors are classified into three groups: attacks caused by hardware deficiencies, attacks caused by software-based bugs, and attacks caused by vulnerabilities in computer networks.

1. **Attacks caused by hardware deficiencies:** Attacks initiated by hardware flaws and errors are more difficult to prevent because software-based tools are insufficient to detect and prevent hardware-related attacks [44]. Trojan horses are often the root cause of hardware attacks. These malicious software variants cause excessive use of computer resources, reduce performance, and cause the system to shut down by consuming excessive power supply [45]. Moreover, copying hardware parts illegally and obtaining untrusted components online create backdoors in the computer system.

The intertwining of hardware parts and the complexity of integrated circuits make it challenging to detect hardware-related vulnerabilities. A change in only one integrated circuit can affect many components and may go undetected for a long time [46]. Therefore, detecting and responding to cyber attacks using a well-designed hardware vulnerability is challenging. Some methods have been proposed to prevent cyber attacks caused by hardware flaws and errors. Tamper-proof hardware devices, hardware watermarking, and obfuscation can play a significant role in preventing these attacks [47].

2. **Attacks caused by software-based bugs:** Most cyber attacks are still driven by errors, vulnerabilities, and deficiencies in application software. These vulnerabilities and errors are increasing every day [48,49]. The leading causes of software-related vulnerabilities and errors can be listed as follows:
    a. Input validation errors;
    b. Problems with user access control;
    c. Incomplete or incorrect authentication;
    d. Migrations directory problem;
    e. Buffer overflow;
    f. Problems caused by Structured Query Language (SQL);
    g. Cross-site scripting (XSS);
    h. Using components with known vulnerabilities;
    i. Issues with web services and APIs;
    j. Improper software security testing.

Software is developed rapidly, but security tests are often inadequate in both the development and testing phases. Developer teams' lack of knowledge about secure software development processes exacerbates the problem. Using applications on different platforms and devices also creates vulnerabilities that increase software-related attacks. For instance, adding more data to a buffer than it can hold may cause unauthorized users to access the system or result in lost data [50]. SQL attacks can overload databases and lead to the theft of usernames, passwords, and credit card information.

While software updates are the most recommended method for fixing software-related errors and deficiencies, they do not always provide a solution. During software updates, errors and vulnerabilities are not eliminated; in some cases, new updates cause new problems. The most effective way to minimize software-based attacks is to produce an error-free program design and requirements before writing code in the software development process life cycle. For this reason, it is crucial for software developers to receive training in the secure software development process. Creating software quickly and trying to fix security vulnerabilities later is not the right approach. Therefore, security threats and attacks should be considered during software development, and all code blocks should be tested manually and automatically at every stage. For example, Microsoft made the use of security development life cycle (SDL) steps mandatory, significantly decreasing errors and

vulnerabilities in the software process. The Windows Vista operating system, developed by applying SDL, contains approximately 45% fewer errors and vulnerabilities than Windows XP, which was written without SDL [51].

3. **Attacks caused by vulnerabilities in computer networks:** During data transfer over the Internet, hackers can access, modify, or completely change the data. The main reason for such threats is using previously created computer network protocols and devices without any security concerns [44]. The vast majority of attacks against computer networks arise due to vulnerabilities in network protocols, such as Transmission Control Protocol (TCP), Internet Protocol (IP), Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS). For instance, since there is no structure to control the accuracy and confidentiality of packets while carrying them over the network using IP, information in the packets can be exposed and changed during transport. Similarly, since DNS responses are not verified, attackers can create fake servers, and users might connect to these counterfeit servers instead of the actual server. Attackers can also send excessive requests to DNS servers, making them unavailable for legitimate users. Moreover, attackers can capture information during data transport due to incomplete or incorrect configuration of network devices, including switches, routers, and wireless access points.

Existing protocol vulnerabilities must be reduced, new protocols must be added, and network devices must be configured correctly and thoroughly to protect data as they move across computer networks. Commonly used cyber security techniques to minimize network attacks can be listed as follows:

a. Use of encryption;
b. Use of access control list (ACL)l;
c. Use of virtualization and VLAN (Virtual LAN);
d. Use of firewall;
e. Use of intrusion detection, prevention, and protection systems (IDPS);
f. Use of web security appliance (WSA);
g. Use of email security appliance (ESA);
h. Use of virtual private network (VPN);
i. Use of transport layer security (TLS) and secure socket layer (SSL) protocols.

Although the data are secured to a certain degree in the network environment by using these techniques, they cannot be said to provide complete protection. Therefore, it is necessary to improve these techniques and propose new ones.

2.3.2. Causes Arising from Emerging Technologies

With the rapid development of technology, new devices and software are being added to the Internet environment every day, such as smartphones, tablets, Internet of Things (IoT) devices, and cloud technology. The generation of numerous application programs in a short time and the addition of new devices, including smartphones and IoT devices, to computer networks, increase the number of cyber attacks. Additionally, storing information belonging to different companies on the same physical structure in the cloud environment and having these environments managed and maintained by third parties also raise security concerns. The reasons arising from the development of new technologies can be listed as follows:

1. **Increasing number of smartphones:** The number of smartphones in use today is approximately 6 billion, and almost one out of every two people uses a smartphone. Personal data stored on these devices, the growing number of software applications developed for them, and the use of wireless networks for Internet access make these devices appealing targets for attackers. According to cyber security threat reports from Symantec [52] and McAfee [53], there has been a significant increase in the number of malicious software created for smartphones. Malware samples written

initially for traditional computers can be adapted for smartphone use with minor changes to the program code.

2. **Increasing number of IoT devices:** Smart devices, such as smart glasses, smart watches, smart parks, and automation systems, collectively known as the Internet of Things (IoT), are gradually being added to the Internet environment. The number of IoT-based Internet-connected devices is predicted to reach around 50 billion shortly. The large amount of data traffic generated by these devices will make it difficult to control the computer network. It can cause significant data loss in the event of a cyber attack. The rapid increase in the Internet of Things devices makes this an emerging cyber attack vector.
3. **Increasing usage of cloud computing**: Cloud computing has emerged as a new technology that has developed recently and serves according to user demand. Amazon, IBM cloud, Google, Rackspace, Microsoft, and Salesforce are widely known cloud computing service providers. The fact that it is easy to use, accessible from different devices and locations, and that the service provided is flexible and scalable according to requested demand increases the usage of this technology. In addition, the fact that processes that bring additional burdens, such as maintenance, repair, and updates, belong to cloud service providers also increases the demand for this technology. On the other hand, giving additional privileges to third parties raises security issues in the cloud environment. Problems related to cyber security in cloud environments generally arise for the following reasons:
    a. The companies and institutions requesting the service lose control over the data;
    b. Using the same physical resources for different companies;
    c. Security concerns regarding data storage in the cloud;
    d. Concerns arising from the use of virtual machines;
    e. Attacks that occur while data are being moved over the computer network.

While data are stored in the cloud environment, the user's control over the data is completely lost. In other words, users have no idea where their data are stored or what security measures are in place to protect them. As a result of multiple independent users sharing the same physical infrastructure, a user can threaten another user and access their data.

On the other hand, a virtual machine monitor (VMM) is a kind of middleware that allows the creation of several virtual machines on the same physical resources. Vulnerabilities have been identified against attacks, such as Xen, VMware, and Microsoft Hyper-V in many popular VMMs. For instance, the exposure on Xen allows the attacker to run arbitrary code by giving "root" authority [54]. Additionally, VMM cannot provide complete isolation between virtual machines. Therefore, the previously mentioned network attacks and vulnerabilities continue to pose a threat in the cloud computing environment. For such reasons, security concerns arise when storing data in the cloud. To reduce these concerns, cloud service providers and companies should work together and take necessary technological and managerial steps.

4. **Increase in the number of critical infrastructure systems:** Critical infrastructure is one of the most crucial systems a modern society needs to continue its daily operations without any problems. Energy production and distribution systems, financial services, communication systems, water and sewer systems, and health services can be given as examples of these systems. Severe disruption in these systems will affect society and daily life. According to studies conducted in recent years, it is seen that there has been an extreme increase in both the number and destructive effects of cyber attacks against critical infrastructure systems. Ensuring the security of critical infrastructure systems has severe difficulties due to structural complexity, geographical location, and the need for the Internet to operate the system efficiently. The reasons for the increase in cyber attacks on critical infrastructure systems can be listed as follows:
    a. Threats arising due to the nature of critical infrastructure systems;

b. Threats arising due to computer network usage during data transmission;
c. Threats arising from communication protocols used in SCADA systems;
d. Threats arising due to the 24/7 availability of critical infrastructure systems.

Critical infrastructure systems are complex in structure, consisting of many components not used in other systems. This complexity and uniqueness of features lead to security threats not present in other systems. Cyber attacks on critical infrastructure systems target corporate networks, SCADA centers, and remote substations. An attack on any of these systems can put the entire essential system at risk. For example, an attack on sensors located at substations can render remote terminal units either unavailable or entirely out of control. An attack on the SCADA center can allow third parties to take control of the system. In addition, communication protocols such as Modbus/TCP and DNP3 used in SCADA systems are vulnerable to several attacks. For example, data transmitted on these protocols are not encrypted, allowing unauthorized access and modification [55]. Ensuring the security of critical infrastructure systems is challenging due to their structural complexity, geographical location, and the need for the Internet to operate efficiently.

2.3.3. Reasons Arising from the Increase in Knowledge

With increased knowledge, launching an attack has become more accessible. It was tough to launch attacks on computer systems in the 1990s and early 2000s. Only experts with extensive knowledge and experience in computer systems could attack computer systems. In the last few years, it has become easier to initiate cyber attacks due to the widespread use of attack tools, the rapid spread of knowledge, and the easy detection of vulnerabilities in computer software and network protocols. Today, even ordinary people who do not have much knowledge about computer systems, known as "script kiddies", can launch attacks using cyber-attacks-as-a-service platforms. Most of these platforms are available on the Internet. Figure 3 compares the attack complexity with the attacker's technical knowledge [56,57]. As shown in Figure 3, although the complexity of the attacks increases over the years, the level of understanding of the attackers decreases.

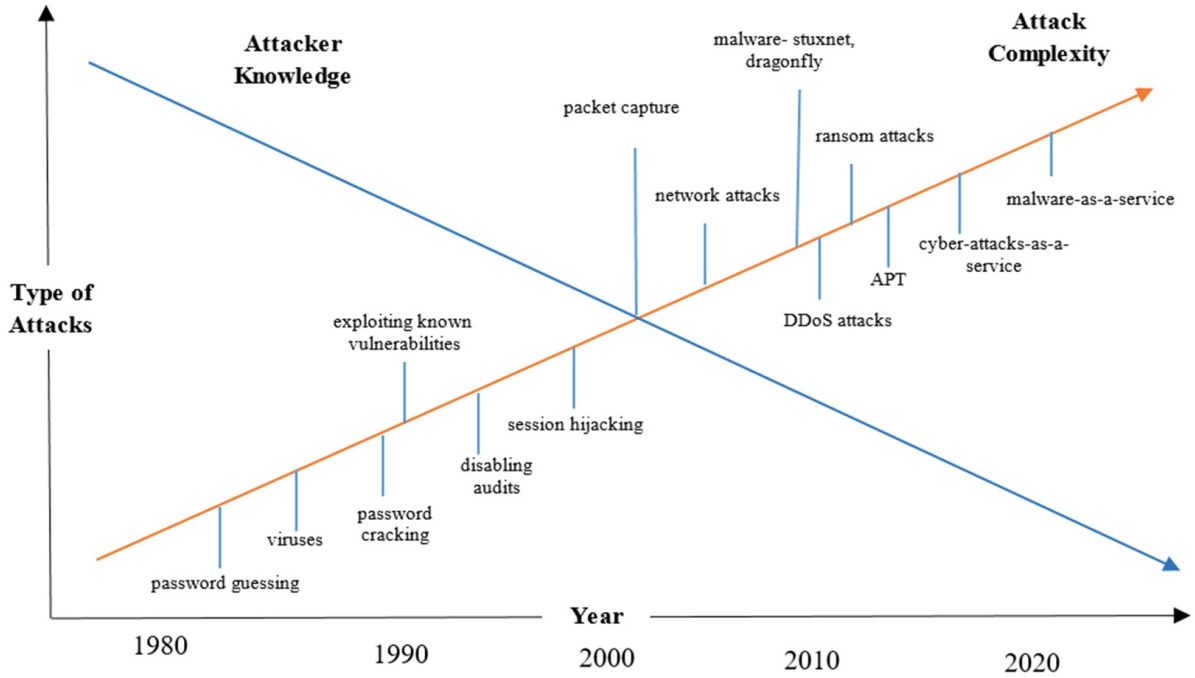

Figure 3. Technical knowledge of attackers versus attack complexity.

2.3.4. Transferring Daily Life into the Digital Environment

Social life has increasingly shifted to the virtual environment in recent years, and the COVID-19 pandemic has accelerated this trend. Nowadays, people of all ages spend a significant amount of time on the Internet, engaging in daily activities such as socializing and conducting business. In addition, many individuals begin their day by logging onto the Internet and continue to spend a large portion of their time online. The activities of daily life that have now been transferred to the Internet environment can be listed as follows:

1. The virtualization of social relations with social media environments;
2. Financial data and the virtualization of money;
3. The virtualization of business meetings;
4. The virtualization of education;
5. The virtualization of news;
6. The virtualization of politics;
7. The virtualization of shopping;
8. The virtualization of wars;
9. The virtualization of games.

The use of social media platforms, such as Twitter, Facebook, and Instagram, is rapidly increasing worldwide, with billions of users estimated to be using these platforms [58]. Many individuals spend a significant portion of their daily life on social media, which stores essential personal information about users, including their name, surname, date of birth, address, and place of residence. Image and video sharing have also become prevalent on these platforms. Social media companies store this user data in large data centers managed by third-party companies. However, while these data are transmitted over the network, they can be stolen, leaked from data centers, or used by managed companies for different purposes. Researchers have found that many social media users receive unsolicited emails (spam emails), and more than 50% of large institutions and organizations experience increased cyber attacks due to excessive information sharing by their employees on social media. Most malware variants in social media environments are spread through popular events, news, pictures, or videos [59,60]. Additionally, attackers can use inactive social media accounts or social engineering techniques to launch new attacks.

The virtualization of financial transactions and money has also increased due to the widespread use of bank cards and credit profits. Banking and stock market transactions are mainly carried out online using application programs. The money in bank accounts is virtual, consisting of mathematical numbers that are increased or decreased during online transactions. The use of virtual currency or cryptocurrencies in online transactions has also increased cyber attacks against these transactions. Millions of dollars are stolen annually by cyber criminals due to technical failures and personal errors during money transfers between accounts in virtual environments. Cyber attacks on cryptocurrencies have also increased, resulting in millions of dollars in yearly losses. For example, the Coincheck cryptocurrency exchange was attacked, resulting in approximately USD 550 million worth of cryptocurrencies being stolen in recent years [61,62]. Remote code execution attacks in recent years are also associated with crypto mining [63]. Virtualization has also impacted many areas, such as business meetings, education, shopping, games, wars, news, and politics.

2.3.5. The Attacks Have No Geographical Boundaries, Which Makes Detecting Attacks Challenging

Cyber attackers have the ability to attack 24/7 from any location in the world without any geographical boundaries. Attackers use specific techniques to hide their sites to avoid being caught during an attack. Furthermore, the absence of laws that deter cyber attacks among countries encourages cyber criminals during attacks. The ease of attacking the Internet, the lack of geographical boundaries, and the absence of legislation among countries regarding the punishment of cyber criminals can be cited as reasons for the increase in cyber attacks.

This section lists both technical and nontechnical reasons for the increase in cyber attacks. Cyber attacks are dynamic and occasionally alter their attack format and target audience, affecting all computer-based systems and the Internet environment. The shift of social life to the Internet environment raises the occurrence of cyber attacks and their destructive consequences. Errors and vulnerabilities in software, inadequacies in network protocols, increased number of devices connected to the network, and the complexity of critical systems increase cyber security risks. Furthermore, the virtualization of social life, excessive use of social networks, increased knowledge of attackers, and careless use of the Internet by users also increase security risks in the digital world.

3. Threats, Vulnerabilities, Exploits, and Attacks

With the development of the cyber security concept, the number of attacks, types of attacks, and damage they cause are also increasing. Hackers carry out attacks that target users, companies, and government institutions, causing great harm. These attacks usually include ransomware, phishing attacks, DDoS attacks, or mobile threats. This section of the study discusses cyber threats, security risks, vulnerabilities, and attacks in detail. Recommendations, precautions, and awareness strategies are also provided for each type of attack.

3.1. Threats

A cyber security threat is a malicious actor that gains unauthorized access to computer networks or another person's or organization's network to damage, disrupt, or steal data [64,65]. Commonly known threat types are described in detail, as follows (Figure 4).

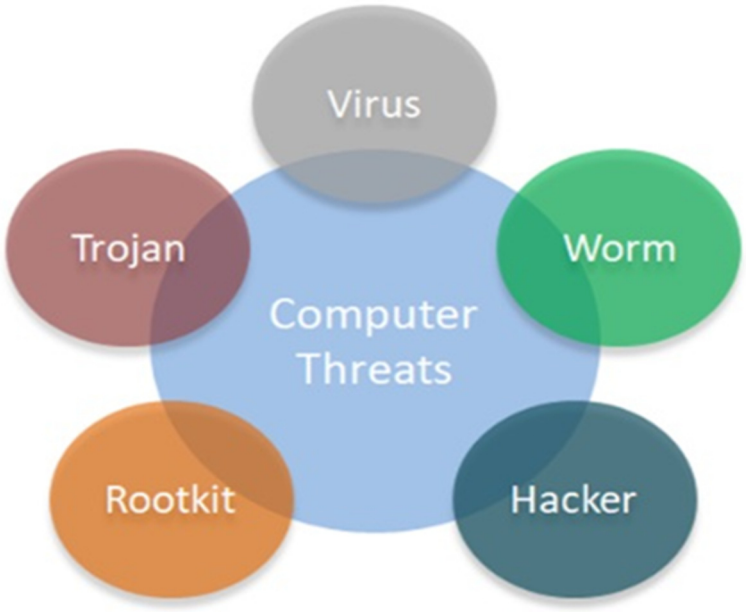

Figure 4. Common computer threats.

Computer viruses: A computer virus is a type of computer program that changes the way a computer works without a user's permission or knowledge and tries to hide in other files [66]. Although these programs can work alone, they generally work by nesting into other programs on the computer. Viruses try to copy themselves to other files after they succeed in running. Viruses need to be "run" to be active. Contrary to common opinion, the computer will not be infected when an infected CD, floppy disk, or flash drive is inserted into the computer—if there is no autorun file. The infected file should be run by the operating system or manually for the virus to become active.

Infectious files were originally only "program" files, often ending with ".exe, .com, or .pif" extensions. However, with the advancement of software technologies, the rise in

"executable" file types, and the evolution of operating systems, potentially dangerous file types have also increased. For example, files with the ".doc" extension, once known just as "text" files, have evolved into complex files in that the "executable" program can be placed with the development of office software. Likewise, files with the ".gif" extension, which are only seen as "images," have been a probable source of viruses by exploiting the vulnerabilities of popular operating systems.

Computer worms: Worms are malicious software with a more complex structure. They are usually spread using email attachments, various websites, and files shared over the network. When worms take over a system, they try to quickly deliver their source files to other users by using the user's data sources (such as an email address list) without the need for any further action by the user. In this way, they can reproduce themselves in large numbers [67]. While doing this, worms utilize users' bandwidth and network resources, and they can cause networks to crash, overload email servers, or slow down access to web resources. They have similar functions to viruses but are not user-run programs to infect programs. After a worm enters a system, often over a network connection or a downloaded file, it creates various copies of itself over a network. It spreads them to all poorly protected servers on the web and computers. The ideal solution to protect against worms is to install the latest version of the operating systems on the computer, chase and perform updates, and close the doors against external attacks using a personal firewall.

Trojan horses: On the other hand, malware called Trojan horses present themselves as useful program to users and cause them to be downloaded [68]. Trojan horses are malware that appear to be valid but are not. They become active due to running the program file to which they are added and spreading copies by users. They are not easy to detect like regular viruses and show their effects after infection. Trojan horses basically contain two files: The first is the file sent to the user. This file allows an attacker to access the user's computer by automatically opening a port on the computer. The attacker can access the user's computer by running the second file. Attackers can obtain personal information such as passwords, credit card info, and any other essential documents from the victim's system. Moreover, since Trojans leave backdoors in the design, attackers can easily install additional malware on the victim's system. Because Trojan malware is so diverse, it can only be avoided by employing an in-depth defense strategy. In addition, to reduce the security vulnerabilities of the systems, users need to regularly update all the software they use, not just their operating system.

Rootkits: A Rootkit is a kind of malware created to authorize hackers to enter and control the victim's device [69]. The majority of rootkits affect operating systems and software. However, some can also affect the hardware and software programs as well. Rootkits are experts at concealing their existence and remain active as long as they stay hidden. After obtaining access to computers, rootkits allow cyber criminals to steal financial and personal information, set up malware, or use devices as part of a botnet so that criminals can circulate spam and use devices for DDoS attacks. It is difficult to determine which files the rootkit actually changed, which module is loaded into the kernel, and which network service it would listen to and take action on with the appropriate command. However, at certain times, methods can be used, such as saving the eigenvalues of the most basic commands and possible rootkit infection points and checking them later.

Hackers and predators: Humans, not computers, create computer threats. The main difference between hackers and hunters is that hackers sacrifice others for their gain [70]. Hackers are informal users who attack systems to steal, change, or demolish data by installing malicious software without information or permission. These online hackers and predators often use phishing scams, spam, and other techniques to send malicious files to computers and compromise security. Anyone using a computer connected to the Internet must be sensitive to the threats posed by hackers and predators. Sometimes, employees and users threaten their organizations by not following and performing safe computer practices. Properly trained employees are the first line of defense against a cyberattack. Therefore, employees' lack of cyber security knowledge can pose one of the most significant

risks to an organization's network security. Hackers can try to access the computer and private information directly if there is no protection with a firewall. Predators, typically disguised as false identities, can expose sensitive personal and financial information, or worse. Therefore, quality firewall solutions and antivirus protection must be used to avoid falling victim to such malicious activities.

3.2. Risks

Technological developments bring along some negativity as well as innovations. In line with the needs of the digital age, institutions and organizations host their data in a distributed structure in different data centers and cloud environments. With corporate and personal data becoming more valuable, various risks threaten this order at many points [71]. In addition, cyber attackers are also developing their attack methods to get more benefits from computer-based systems. These activities, evaluated in various scenarios from data theft to ransomware attacks, are called "Cyber Risks." The most commonly known types of cyber risks are explained in detail in the following.

Spyware: Spyware software that collects data without the consent or knowledge of the computer user. Spyware is used to violate the privacy of personal information by recording the keys that the user presses on the keyboard, keeping track of the web pages viewed, scanning the data on the hard disk, and monitoring the searches made on the Internet [72]. As a result, illegal actions such as stealing people's email and bank passwords or creating "personal advertising" pop-ups, spam, and consuming network and system resources of the computer reduce the viewing speed of web pages or cause a general slowdown of the computer.

Spyware is often distinguished from viruses because it is not explicitly designed for illegal and direct harm to the user and because it is installed on the computer with the user's consent or as a result of their actions. Moreover, like viruses, spyware does not copy itself from one computer into another in any way. However, consent or approval for the installation is obtained without the user being explicitly informed about the activities of this malware on the computer. To be protected from this spyware, it is necessary to perform security measures such as not downloading files from intermediate sites, not connecting untrusted sources to devices, and not opening unknown emails.

Scareware: This is the name given to malicious computer software included in the malware class known as "Rogueware" [73]. It often scares users with unrealistic scenarios and encourages them to buy the software. Then, it is installed on the computer and claims that the malicious software will be cleaned, but the installation infects the device with a virus. In this way, the data on the computer are intercepted, and the computer's owner is prevented from accessing them.

The primary purpose of scareware software is to make money for its owner. When you log in to a website, a pop-up screen such as "x threats detected on your computer" appears, even though there is no virus on the computer. This pop-up not only says there is a virus on the computer but also suggests its own scareware software to get rid of viruses. The main purpose here is to scare the users and force them to buy the software with this fear. The vast majority of software called scareware cannot actually fulfill the functions they promise, and the only purpose is to get the user to pay. If scareware software is installed on the computer, there is no need to panic immediately, because, usually, scareware software can be found and deleted by logging into the Program, Add/Remove menu of the computer.

Joke Programs: A joke program is a standard program that generally has no malicious purpose. The primary purpose of these programs is to annoy or entertain the user [74]. Virus writers create joke programs to make fun of computer users, and the main purpose is not to harm them. However, some victims can panic and accidentally engage in activities that could damage data, such as drive formatting or file deletion. Since joke programs are ordinary, they do not damage other programs, systems, or data. Occasionally, these programs can temporarily deactivate devices such as a mouse or printer. However, the computer returns to its original state after a joke program ends or the user restarts it. While

joke programs often seem innocent, they can sometimes be costly for an institution or organization.

Ransomware: Ransomware is one of the most prominent types of cyber risks that make essential files, documents, applications, operating systems, networks, or servers inaccessible [75]. They are malware that can encrypt all files and documents on the network, including servers, from a single computer. After the ransomware infects the computer, victims are often asked to pay a ransom in cryptocurrency. In return, their data are promised. However, even if all files are decrypted by paying the ransom, it is difficult to be sure whether the criminals are keeping copies of the data. This means the information can be used in fraud or phishing attempts. They deceive people with a fake attachment or link. Malicious files are often disguised as ordinary documents (order confirmations, receipts, invoices, and notices) and appear to have been sent by a reputable company or institution. Downloading or trying to open one is enough to be infected by ransomware.

Hacking tools: Hacking is the deliberate modification of computer software or hardware outside architectural boundaries and design. A hacking tool is a program or utility designed to assist a hacker with hacking [76]. It can also be used proactively to protect a network or computer from hackers. Hacking tools have different capabilities designed to infiltrate systems. For example, Hacktool: Win32/Keygen is one of the most well-known hacking tools and is the codename of a fake tool that can generate phony activation keys or licenses for various software. The device itself is not malicious, but Hacktool: Win32/Keygen is often bundled with malware. Therefore, users who have installed (or infiltrated without their permission) Hacktool: Win32/Keygen are likely to have an infected computer. Many hacking tools are commonly used to gain unauthorized access to a computer to add worms, viruses, and Trojans. As a result, hacking tools can have serious consequences, such as loss of data, hijacking personal accounts, and theft of identity and savings.

Remote access: Remote access is an application that allows you to connect and manage your computer over the Internet, regardless of your location, and operate over particular protocols [77]. Although it sounds good, it is a method that carries many risks, because many people, institutions, and organizations fail to protect remote connection services from inappropriate access. An attacker will find vulnerable spots in a computer or network's security software to gain access to the machine or system. The leading causes of remote attacks are to view or steal data illegally; introduce viruses or other malware into another computer, network, or system; and damage the targeted computer or network. Other attacks that hackers can facilitate via remote access include email phishing, compromise of third-party providers, insider threats, social engineering, and the use of vulnerable applications to compromise systems. To protect against remote access attacks, VPNs with older and less secure protocols should be avoided. Multifactor authentication should also be mandatory for each VPN account. At the same time, at least two layers of security must be applied before any device can be managed remotely, and antivirus and antimalware programs must be installed and updated for protection.

3.3. Vulnerabilities

A vulnerability is a flaw within a product or system that can potentially permit an attacker to undermine the confidentiality, integrity, or availability of that product or system [78]. The various types of vulnerabilities are outlined briefly as follows.

Software vulnerabilities: Software vulnerabilities emerge when applications contain errors or bugs, which are seen by attackers as an opportunity to exploit these weaknesses to compromise the system. Buffer overflow and race conditions can be examples of attacks caused by software security vulnerabilities.

Firewall vulnerabilities: Firewalls serve as software and hardware safeguards that shield networks from attacks. A firewall vulnerability pertains to a mistake, deficiency, or faulty assumption made during the design, implementation, or configuration of the

firewall that can be exploited to launch attacks against the trusted network that the firewall is intended to safeguard.

TCP/IP vulnerabilities: These vulnerabilities belong to various layers of a network. These protocols may lack desired features in an unsecured network. ARP attacks and fragmentation attacks can be examples of attacks caused by TCP/IP vulnerabilities.

Wireless network vulnerabilities: Wireless Local Area Networks (LANs) encounter protocol-based attacks comparable to wired LANs. Insecure wireless access points can also become a potential threat, as they create an entry point for an attacker to gain unauthorized access to a personal or corporate network. Illustrative examples of these vulnerabilities include problems with the Service Set Identifier (SSID) and Wired Equivalent Privacy (WEP) issues.

Operating system vulnerabilities: These are security vulnerabilities in operating systems such as Windows, macOS, and Unix. The security of the applications running on it depends on the operating system's security. The slightest negligence of the system administrator can make operating systems vulnerable.

Web server: These vulnerabilities result from design and engineering errors or misapplication. Examples of attacks caused by web server vulnerabilities are sniffing and spoofing attacks.

3.4. Vulnerability Scanning Tools

These are tools that detect security vulnerabilities in devices and software in systems [79]. Like antivirus software that uses virus definition databases to determine the signatures of viruses, most vulnerability scanners trust vulnerability databases and scanning systems for specific vulnerabilities. These vulnerability databases can be obtained from reputable security testing labs or known databases used to identify vulnerabilities in software and hardware. As might be expected, the detection level of the scan tool depends on the vulnerability database that the tool uses. When choosing a vulnerability scanning tool, there are many features to consider, such as the variety of devices it can scan, the scanning method, and warning/reporting. Vulnerability scanning tools that are widely used today with these features are examined in this section.

Netsparker: Netsparker is an entirely accurate, automatic scanner that determines vulnerabilities in applications and APIs on the web. Netsparker heavily confirms defined vulnerabilities and proves they are genuine, not false positives. Therefore, there is no need to spend time manually confirming the defined vulnerabilities while finishing the scan. Windows software and an online service version of the tool are available [80].

Acunetix: Acunetix is a fully automated web vulnerability scanner. It detects over 4500 web application vulnerabilities, SQL Injections, and XSS. Then, it also provides a report about its scan. The Acunetix browser supports single-page applications with HTML5 and JavaScript, which allows the inspection of complex, authenticated applications. Furthermore, it makes use of sophisticated vulnerability management functionalities, ranks risks according to information via a unified and consolidated perspective, and combines scanner findings with additional tools and platforms [80].

Intruder: The Intruder is an advanced vulnerability scanner that performs proactive scans for newly released vulnerabilities [81]. It has conducted over 10,000 security checks in the past, covering Heartbleed and SQL Injection. Its integration with Slack and Jira allows development teams to stay updated when new issues arise, while AWS integration facilitates synchronization of IP addresses for scanning. The Intruder is a preferred choice for startups and midsize businesses, as it simplifies vulnerability management for small teams.

SolarWinds: The SolarWinds Network Configuration Manager offers network vulnerability detection capabilities. It includes features for monitoring, managing, and safeguarding network configurations. The tool sends notifications when configuration changes occur and performs ongoing checks to identify configurations that may render a device incompatible. Additionally, the software enables configuration backup to aid in monitoring changes.

Detailed information about configuration modifications and the login ID associated with them can also be obtained [82].

Apptrana: This is a web application vulnerability scanner that automates the detection and reporting of security vulnerabilities. It is used by over 1100 customers across 25+ countries worldwide. A proof-of-concept request is available to validate reported vulnerabilities and eliminate false positives. The same dashboard displays additional manual penetration tests and reports. The tool features a pause and resume function. Additionally, optional integration with Indusface WAF is provided to offer immediate virtual patching with zero false positives [83].

OpenVAS: OpenVAS is an open-source tool designed for centralized vulnerability scanning and management. It is available at no cost and is typically licensed under the GNU General Public License (GPL). The software is compatible with a range of operating systems. OpenVAS features a regularly updated scan engine with network vulnerability tests. It is a comprehensive vulnerability assessment tool used to identify security-related issues on servers and other network devices [84].

The Nexpose Community: Developed by Rapid7, the Nexpose vulnerability scanner is an open-source tool that performs network checks and vulnerability scans. It is employed to monitor vulnerability exposure in real time and stay informed of emerging threats using new data. Unlike many other vulnerability scanners that rank risks as high, medium, or low, Nexpose considers factors such as which malware kit is utilized and what benefits are derived from a vulnerability. It prioritizes security vulnerabilities and addresses them accordingly. The tool automatically identifies and scans new devices, assessing their vulnerabilities when they connect to the network. Additionally, Nexpose can be integrated with the Metasploit framework [85].

Nikto: Nikto is a widely favored open-source web scanner utilized for evaluating potential web server vulnerabilities and issues. It conducts thorough tests on web servers to identify hazardous programs or files, as well as to confirm that the server version is current and identify any issues impacting server operation. Nikto scans various protocols such as HTTP, HTTPS, and HTTPD. In addition, multiple server ports can be scanned using Nikto [86].

Microsoft Baseline Security Analyzer (MBSA): It is a tool designed to detect appropriate security status with Microsoft security recommendations and scan for security vulnerabilities on computers with MBSA Windows operating systems. Another feature of MBSA is that it can monitor all operating systems in the network. For this, the administrator user and password of the computer or computers to be scanned and on the computer where it is installed must also be the same. In this way, the vulnerabilities in the scan results of the computers on the entire network can be seen. The MBSA tool also performs the necessary HOTFIX check for IIS and SQL servers but not the operating system. HOTFIX is an additional package to fix bugs in software [87].

Wireshark: Wireshark is a globally recognized and extensively employed network protocol analyzer. It is utilized in diverse settings, including educational institutions, government agencies, and businesses, to conduct detailed examinations of networks. The tool possesses a distinctive capability to detect problems in real time and conduct analyses offline. It is compatible with several platforms, including Windows, Linux, Mac, and Solaris, and can explore numerous protocols in great detail. Wireshark is widely considered the most robust tool in the arsenal of security professionals [88].

3.5. Attacks

With the development of technology, the possibilities of accessing information have increased. However, the ease of access to information has also made it challenging to ensure information security. With today's information systems in all areas of life, the concept of cyber attacks has become more popular. These cyber attacks have spread over a wide area, from daily life to government institutions, the economy to commerce, and banks to hospitals. Common types of attacks are described below (Figure 5).

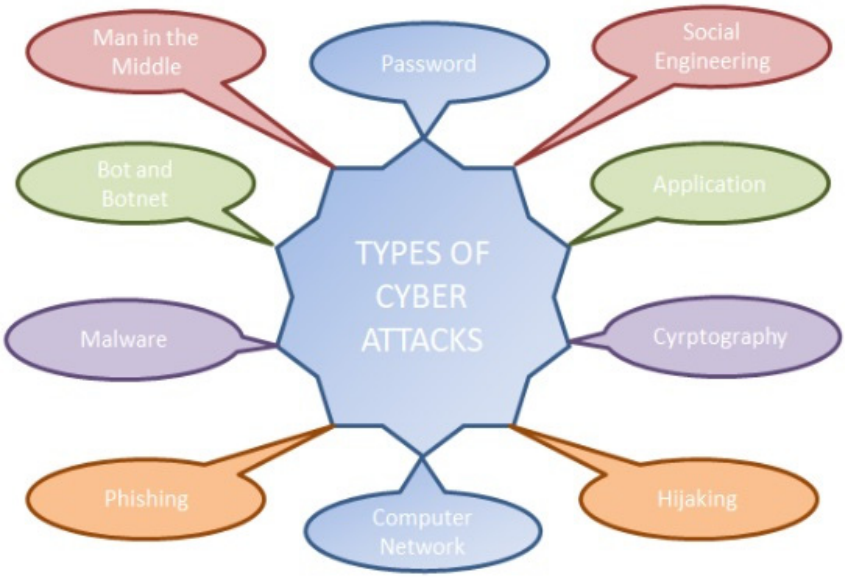

Figure 5. Common types of attacks.

Social engineering attacks: When considering cyber security, many believe in defending themselves against hackers who use technological vulnerabilities to attack data networks. However, there is another way to infiltrate organizations and networks which takes advantage of people's vulnerability. This method of tricking someone into revealing information or gaining access to data networks is known as "social engineering". In summary, social engineering is manipulating people to permit them to access or disclose information or data [89]. Social engineering, like most cyber attacks, aims to bypass the security measures of a person or organization. Anyone can be a victim of a social engineering attack. Still, the elderly with limited technical knowledge, those with little human interaction, and those prone to impulsive behavior are common targets. Personal/private information should not be shared to prevent possible attacks, people attempting to contact should be questioned, URL/address checks should be performed, and untrustworthy sources should be avoided.

Application attacks: An application attack involves cyber criminals gaining access to unauthorized domains. Attackers often start by looking at the application layer and looking for application vulnerabilities written in code. Although attacks target specific programming languages more than others, many applications representing various languages are attacked. Vulnerabilities exist in both proprietary code and open-source frameworks and libraries. Application vulnerabilities create opportunities for cyber criminals to exploit applications in production. These exploits target both proprietary code and open-source frameworks and libraries. Cyber criminals take advantage of different methods, such as vulnerabilities in code, vulnerabilities due to legacy certificates, and vulnerabilities due to a lack of authentication [90].

Cryptography attacks: Cryptography is a process that involves storing and transmitting data in a specific format to ensure that only the intended recipients can access and understand them. This is achieved through encryption, which involves converting plain text into cipher text, and decryption, which involves converting cipher text back into plain text. Cryptographic attacks occur when an attacker tries to compromise a cryptosystem by identifying weaknesses in the code, cipher, cryptographic protocol, or key management scheme. These attacks are classified as either passive or active. Passive attacks involve unauthorized access to information without disrupting the communication channel, while active attacks involve modifying or initiating an unauthorized transmission of information [91]. Passive attacks are often associated with stealing information, while active attacks involve changing data without permission. Both types of attacks can compromise the integrity and confidentiality of sensitive information.

Hijacking attacks: Hijacking attacks are a type of network security attack in which the attacker takes control of computer systems, software programs, and network communications [92]. Most cyber attacks rely on hijacking in some way, and hacking is regularly, if not always, illegal, with severe consequences for both the attacker and the victim. These attacks include airplane hijackers or taking control of an armored transport vehicle. There are many types of hijack attacks, and they are listed below:

- Browser hijacking;
- Session hijacking;
- Domain hijacking;
- Clipboard hijacking;
- Domain name system (DNS) hijacking;
- Internet protocol (IP) hijacking;
- Page hijacking.

Computer network attacks (CNAs): It is the process of manipulating, corrupting, rejecting, and destroying information in computers and computer networks in order to gain control of the computer/computer network [93]. With CNAs, systems can be shut down, data modified, and resources misused for botnets or any other action that compromises the integrity or availability of a system. The CNA relies on the data stream to execute the attack. For example, sending a code or instruction to a central processing unit that causes the computer's power supply to short circuit is a CNA. To perform a CNA, attackers gain access to the network and scout the network before taking action. Discovery allows to learn the network configuration and determine how best to carry out malicious activity.

Phishing attacks: Phishing is one of the most common cyber threats today. According to the world-accepted definition, phishing is "a type of online fraud that targets consumers by sending an email purporting to come from a known source" [94]. Scammers pretend to be Internet service providers, banks, stakeholder companies, or government agencies. These are attacks to obtain sensitive and confidential information, such as usernames, passwords, credit card information, and network credentials. They try to use social engineering as best as possible when manipulating personal information into disclosure, typically by asking victims to click on a harmful link or attachment via phone or email.

Attention and education are the keys to not being caught in phishing attacks. While many commonplace phishing attempts can be filtered out with email monitoring systems, employee email security training can also reduce the number of potential victims by raising awareness of phishing risk. At the same time, to avoid phishing attacks, it is essential to be wary of website pop-ups and ensure the URL starts with "HTTPS" and has a closed lock icon next to the address bar.

Malware attacks: Malware is the general name given to software designed to harm computer systems, steal information, or annoy users. Examples of this software are viruses, worms, Trojans, and rootkits. Although they are generally defined as software, they can sometimes be in the form of simple codes. Malware, sometimes called scumware, can be written in almost any programming or scripting language and carried in many file types. Malware can gather information and spy for a long time without alerting the infected computer system. In addition, it can be used to damage or sabotage the system it enters (such as Stuxnet), or it can be used to extort money or payments [95].

Bots and botnets: "Bot", short for robot, is a software program that performs repetitive, automated, and predefined tasks [96]. Bots often imitate or replace the behavior of human users. Because they are automatic, they work much faster than human users. They can perform useful functions such as customer service or indexing search engines or be used as malware to gain complete control over a computer. Malware bots and Internet bots can be programmed/hijacked to infiltrate user accounts, scan contact information, send spam, or perform other malicious actions.

The word botnet is derived from combining the words "robot" and "network." Botnets consist of a good deal of software agent programs. Each software agent program is controlled remotely. Botnets have the ability to act as a unit. A botnet is a set of Internet-

connected computers that communicate with similar machines to complete repetitive tasks and goals. Such networks are often used to send spam emails. A botnet is under the attacker's control and can be expressed as a network of thousands of zombie computers or even hundreds of thousands.

Password attacks: Password attacks are one of the most frequently used attack types in cyber attacks. Password attacks can be carried out against corporate targets as well as personal targets [97]. The aim is to harm the institution or individuals by seizing the passwords of any field that requires a password, such as social media networks, technologies, or software used by the person or institution. Generally, individuals or institutions prefer easy passwords to avoid forgetting them. In particular, social media users can share the password content they use in summary form on their pages. For example, on social media accounts, there is a lot of information, such as the team that the person supports, where they are from, date of birth, name of their spouse or partner, and relationship years. This information is essential for cyber attackers. Therefore, sharing this information facilitates the work of attackers who will carry out password attacks.

Man-in-the-middle attack: The man-in-the-middle attack is the oldest type of cyber attack, in which a malicious person is secretly involved in communication between two parties [98]. This attack allows the data transmitted by the victim to be read and even modified. The attacker achieves this by creating a secret, pseudofake connection between their and the victim's computers. Usually, the purpose of a man-in-the-middle attack is to obtain personal data, passwords, and bank information or impersonate one of the parties. These actions may include, unfortunately, changing login information or initiating a money transfer. Areas that provide free Wi-Fi are the most suitable areas for this attack to be carried out. The contents of unencrypted packets can be easily read. Attackers in Wi-Fi areas direct network traffic to pass over themselves. Thus, the traffic of the people on that network starts to flow through the attacker. The attacker who seizes this traffic can obtain personal data or passwords from here.

This section discusses well-known types of cyber threats, risks, vulnerabilities, and attacks in detail. Each has its own method of applications and target audiences. To prevent or protect computer-based systems from such threats, risks, and attacks, the following actions can be taken:

- Do not download or open programs from an unknown source;
- Never open unsafe emails or run attachments from them;
- Using licensed operating systems and software;
- Using Antivirus and Antispyware;
- Using a personal firewall;
- Avoid visiting suspicious websites whenever possible;
- Using virtual machines;
- Using strong passwords.

In summary, "security awareness" is the first line of defense to protect ourselves in a world of ever-evolving cyber threats and attacks. There are powerful security tools that can help, but acting consciously is the most critical step to protect your computer, information, and yourself.

4. Network Security

In this chapter, we present network security extensively. We classify network security based on network protocols, which are a set of rules and structures that control the data exchange among connected devices across networks. For this aspect, we first explain the Open Systems Interconnection (OSI) model and how network protocols work in Section 3.1. Then, we classify network protocols and security threats with these protocols in Section 3.2. Next, we present network protection devices and tools in Section 3.3. In the penultimate Section 3.4, we express Wireless Network Security.

4.1. The OSI Model

The majority of network protocols are structured based on the OSI model, which was announced by the International Organization for Standardization (ISO) in 1984. Therefore, it is crucial to understand the OSI model to describe the nuances of network protocols. Basically, the OSI model divides the communication process into seven layers. The layers are independent of each other, and each layer executes the tasks independently. The OSI model between the two devices is depicted in Figure 6. The OSI model is also grouped into two categories: Upper Layers and Lower Layers. The Upper Layers contain layers 5, 6, and 7, and the Lower Layers have layers 1, 2, 3, and 4, which manage application work. The Lower Layers contain layers 1, 2, 3, and 4 that execute transportation functions [99].

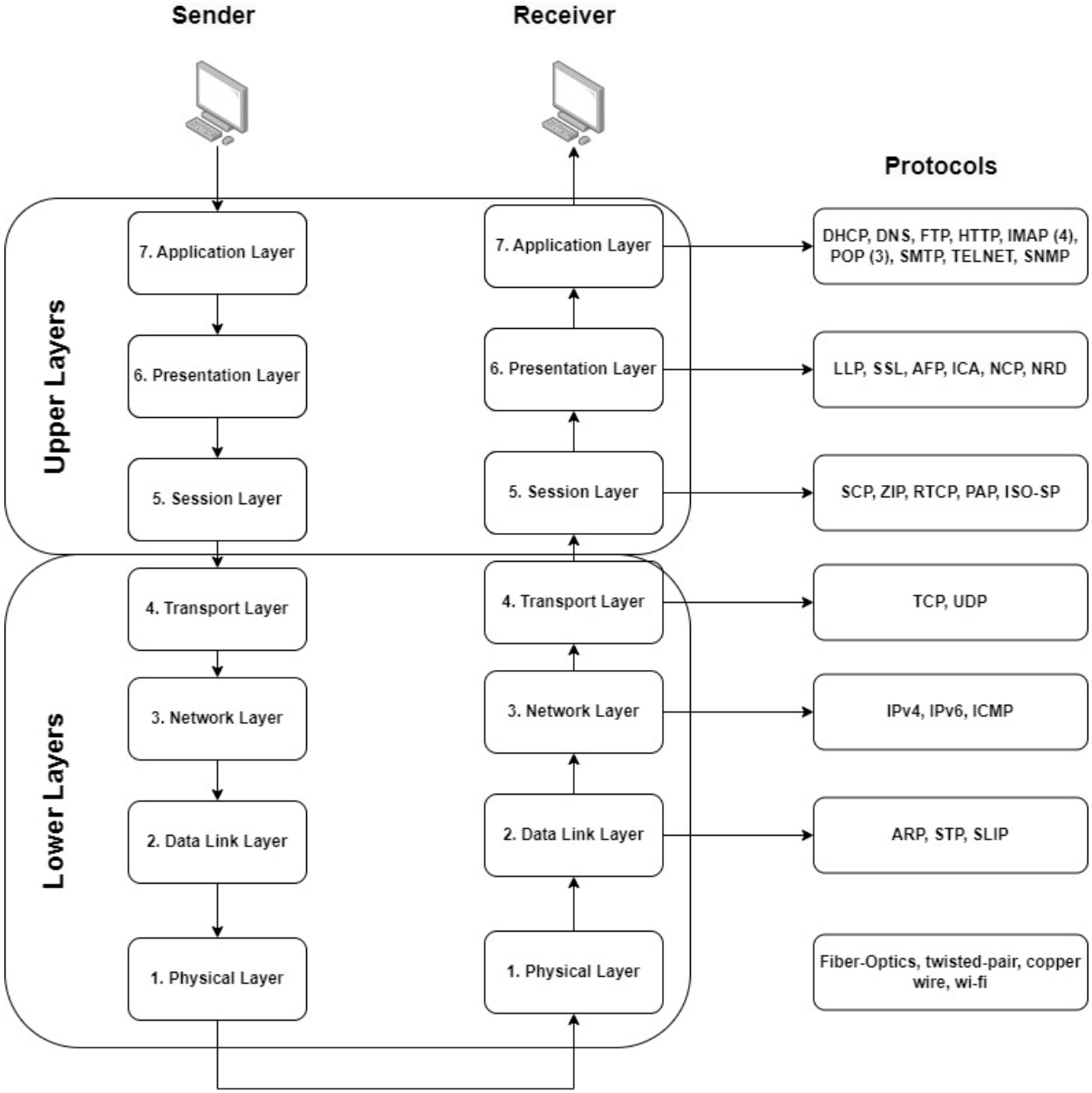

Figure 6. OSI model.

4.2. OSI Layers and Their Functionalities

We now classify and explain each layer and its functionalities with a top-down (from Layer 7 to Layer 1) approach.

4.2.1. Application Layer

Application layer protocols can be defined as how end-users pass messages to each other. Basically, an application layer defines the types of messages and the rules for the process of sending and responding to messages. Distinctly, the application layer is only a part of network protocols and network applications [100]. Some important application layer protocols are Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), Internet Message Access Protocol (4) (IMAP and IMAP4), Post Office Protocol (3) (POP and POP3), Simple Mail Transfer Protocol (SMTP), TELetype NETwork (TELNET), and Simple Network Management Protocol (SNMP).

Application Layer Protocols

– **Dynamic Host Configuration Protocol (DHCP):** IP addresses can be configured manually by a system administrator. When the number of hosts connected to the network increases, it could be hard to control IP address configuration manually. Therefore, there is a need to do it automatically [101]. DHCP is the protocol that allows the system to configure and distribute IP and other network configuration parameters in the system automatically [100–102]. The DHCP process consists of four steps (also known as DORA):
  - DHCP Discovery: DHCP client broadcasts to identify the DHCP server in the network;
  - DHCP Offer: DHCP server responds to the client (in a unicast manner) with an IP address and related configurations such as gateway address, DNS, and so on;
  - DHCP Request: DHCP client again broadcasts to the DHCP server to request configurations;
  - DHCP Ack: DHCP server sends an acknowledgment message to the client that it can use the network.

The security of the DHCP was not an important issue because of its simplicity, ease of use, and the small number of connected devices to the networks [103,104]. However, since the number of connected devices is increasing exponentially, DHCP security has become a critical criterion to consider [105]. The main reason for DHCP security issues is the lack of an authentication mechanism [106]. A malicious DHCP client can launch a starvation attack to prevent the IP address from being assigned to the network [97]. Furthermore, an attacker can use a rogue DHCP server to provide incorrect configuration information to network clients [102–109].

– **Domain Name System (DNS):** The Domain Name System (DNS) is responsible for translating a hostname into a computer-friendly IP address [110]. An IP address is an identification for computers, and finding a device on the Internet is necessary. The basic operations of DNS can be explained in eight steps. First, a client computer requests a domain name from a DNS resolver. This DNS resolver can be recursive or authoritative. Then, the resolver queries the DNS root name server. The root server responds to the resolver with a Top-Level Domain (TLD) such as .com, .org, .edu, etc. As soon as the resolver receives the TLD, it requests the related TLD server, which responds with the IP address of the domain's nameserver. The IP address of the nameserver is sent to the resolver after the resolver requests it from the nameserver. Finally, the DNS resolver responds to the client with the IP address of the requested domain [111,112].
– **File Transfer Protocol (FTP):** Basically, the File Transfer Protocol (FTP) is responsible for file transfers between connected heterogeneous computer systems [113]. However, the objectives of FTP are not limited to this. It boosts sharing of files, programs, and data. It also provides a way to use remote computers. In addition to these, it also acts as a shield that protects a user from variations and transfers data efficiently among hosts [114].

- **HyperText Transfer Protocol (HTTP):** As the foundation of the World Wide Web, HTTP is responsible for loading web pages using hypertext links. Since it is a protocol in the application layer, it runs on top of other layers and sends and receives information among connected computers. Clients request HyperText Markup Language (HTML) files, videos, scripts, photos, text, etc., from a server, usually via a web browser. Then, the server responds with the requested data to the client [100,115].
- **Email Protocols:** The Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP) are the standard protocols for email delivery over the Internet. The last versions of POP and IMAP are POP3 and IMAP4, respectively. Most email clients, such as Outlook and Gmail, use SMTP for email delivery between two parties. An SMTP server is responsible for pushing emails. Email clients connect to this server and communicate via it. When the user clicks the send button, the email client opens an SMTP connection to the server. Then, the SMTP server transfers data to the corresponding client via the Mail Transfer Agent (MTA). If the receiver uses the same client, the MTA directly sends a message. Otherwise, it uses the DNS protocol to reach the receiver's domain [116–118]. POP and IMAP are used to access electronic mailboxes. While POP stores all emails locally on the user's device, IMAP keeps them on the server. Therefore, IMAP provides mobility because users can check email from different devices [116,119].
- **TELetype NETwork (TELNET):** Telnet is a two-way text-based communication protocol that provides a two-way communication channel between two computers. The computers can be in a Local Area Network (LAN) as well as remote computers via Transmission Control Protocol (TCP) [120]. It is mainly used by users who need to use applications or data stored on a remote machine.
- **Simple Network Management Protocol (SNMP):** SNMP is a standard Internet protocol responsible for monitoring and managing network devices. The common devices that support SNMP are routers, terminal servers, hosts, and so on [121]. While the first implementation of SNMP, also called SNMPv1, only provides the architecture and framework, the later versions (SNMPv2c and SNMPv3) focus on performance and security [122,123].

Application Layer Attacks: There is a wide range of application-layer attacks, including DoS, DDoS, SMTP attacks, FTP bounce, insecure HTTP, browser hijacking, buffer overflow, malware attacks, data attacks, and so on [124,125]. Recently, application-layer DoS attacks have become very popular [125]. The most significant application-layer DoS attacks were reported in 2019 and continue to double every quarter of the year [125–128]. A DoS or DDoS attack is basically continuously sending forged requests to exhaust the IP address pool and bog down the server's responsiveness. DoS and DdoS attacks cause potential vulnerabilities and flaws, including DHCP starvation, Network Time Protocol (NTP) time-shifting/sticking, and slow HTTP DoS, as well as substantial computational performance and QoS degradation. An SMTP attack is a technique where the attacker gains unauthorized access to the client's mail, observes the mail addresses, and abuses them. An FTP bounce attack is similar to an SMTP attack in that the attacker can access ports using the victim's machine. Browser hijacking is a malware program the attacker uses to modify unauthorized web browser settings. A buffer overflow attack is a technique that aims to overwrite the memory of an application to damage files and expose private information. Insecure HTTP means that the HTTP data are not encrypted, which makes them vulnerable to attacks. Attackers use malware software to attack the victim. The most common malware attacks are adware, viruses, worms, Trojans, bots, and ransomware [129–132]. Security mechanisms such as cryptographic techniques, using security features in switches, traffic profiling, machine-learning-based techniques, path and server redundancy, monitoring traffic features, and comparing traffic profiles to prevent these attacks were studied in [124,126,133–137].

4.2.2. Presentation Layer

The sixth layer of the OSI model is called the presentation layer. This layer deals with the fields in the messages and the semantics of the fields in the messages exchanged between end-users. It is a bridge between the application and the transport layer and is responsible for data translation, encryption–decryption, and compression. Basically, the presentation layer translates messages from high-level language data to low-level language and vice-versa. Moreover, it encrypts the plain text message from the application layer and decrypts the encrypted data from the transport layer. In other words, it manages the encryption and decryption processes between senders and receivers. The layer also compresses data to reduce the number of bits in loss-tolerant data [100,138].

Presentation-layer protocols

Presentation-layer protocols include the Lightweight Presentation Protocol (LPP), Secure Socket Layer (SSL) protocol, Apple Filing Protocol (AFP), Independent Computing Architecture (ICA), NetWare Core Protocol (NCP), and Network Data Representation (NDR) [138,139].

Presentation-Layer Attacks

SSL is used to secure web services, including banking, online shopping, etc. The presentation-layer attacks involve malformed Secure Socket Layer (SSL), SSL Stripping, and Change Cipher Specification (CCS) manipulation attacks [140,141]. SSL stripping causes removing SSL data from a request message coming from the client and the opening of multiple ports for the corresponding server. A CCS manipulation attack is made by improper usage of CCS messages. Injecting a CCS message during an already opened session causes a passive session and failure of negotiation.

4.2.3. Session Layer

The session layer is the fifth layer of the OSI model. This layer manages data between the presentation layer and transport layer. It is responsible for enabling communication between two end-user applications, allowing the systems to communicate in the half- or full-duplex mode of communication, managing and allowing the process of adding checkpoints, managing communication sessions, and synchronizing information from different resources. It uses Remote Procedure Calls (RPCs) to implement services to control the functionalities mentioned above [115].

Session-Layer Protocols

The RPC protocol is mainly used in application environments in session-layer services. Other popular session-layer implementations include Session Control Protocol (SCP), Zone Information Protocol (ZIP), Real-time Transport Control Protocol (RTCP), Password Authentication Protocol (PAP), OSI session layer Protocol (ISO-SP, a.k.a. X.225), and so on [142].

Session-Layer Attacks

There are two main session-layer attacks: session hijacking and stealing session ID. We separate hijacking attacks into three groups: active, passive, and hybrid session hijacking, which carry out the same attacks differently. In an active session hijacking, an attacker attacks an active session. On the other hand, in passive session hijacking, an attacker locates themself between the user and the server. They send and receive packets between the server and the user, acting as a valid user and server. In hybrid session hijacking, an attacker uses active or passive session hijacking features based on the goal [143]. There are popular tools used for session hijackings, such as Wireshark, T-SightS, Hunt, and Hamster and ferret. For session ID stealing purposes, there are three popular ways. Sniffing: an attacker monitors the victim's network traffic and obtains the session ID from the unencrypted packets. Brute force, which is not a time-effective technique, means an attacker tries all combinations to figure out the session ID. Last but not least, cross-site scripting aims to steal session IDs by using the vulgarities of websites [143–145].

4.2.4. Transport Layer

The group of the first three layers mentioned above is called the Upper Layer. The transport layer is the layer between the Upper and Lower Layers. It is the fourth layer of the OSI model and the first layer of the Lower Layer group, including layers 4, 3, 2, and 1. It is responsible for delivering the complete messages between the end-users and providing acknowledgment of the data in case an error occurs. At the sender's side, the transport layer receives the formatted data from the upper layer, performs segmentation, implements required flow/error controls, inserts source–destination port numbers in the data header, and forwards the segmented data to the network layer. At the receiver side, the transport layer reassembles the segmented data, looks up the port number, and delivers the data to the related applications.

Transport-Layer Protocols

The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are in this layer, and they are critical protocols for the OSI model [100] [146,147]. While UDP is a connectionless protocol, TCP is the protocol that prioritizes data quality rather than speed.

Transport-Layer Attacks

In particular, this layer has three types of security threats: TCP flooding attack, UDP flooding attack, and TCP sequence prediction attack. The TCP flooding (a.k.a. TCP SYN) attack is the most common attack on the Internet. When a TCP connection is established between the sender and receiver computers, the sender sends the TCP Reset (TCP RST) packet to the receiving computer after ensuring the receiver is not listening. However, in a TCP SYN spoofing attack, the sender sends a TCP RST packet even if the receiver listens for the communication [148,149]. The UDP flooding attack is also a DDoS attack that targets weakening the performance of the victim's computer. The attacker spoofs the victim's IP address and sends UDP packets to affect the system of the victim [150,151]. Finally, a TCP sequence prediction attack is a way to send counterfeit packages to the victim's computer by predicting the sequence number that is used for identifying the packets in a TCP connection [152,153].

4.2.5. Network Layer

The network layer is one of the most complex layers in the OSI model [100]. This layer has two planes: the control and data planes. When a packet arrives at a router, it must be moved to the appropriate output link in the data plane, as illustrated in Figure 7.

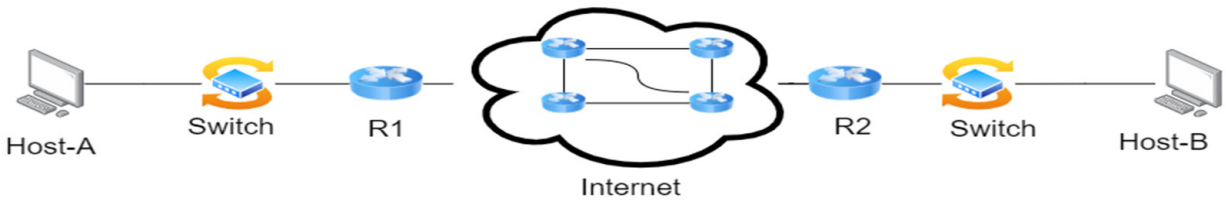

Figure 7. Representation of routing algorithm between sender and receiver in computer network.

Host-A sends a packet to Router1 (R1), and R1 must forward the packet to Host-B via Router2 (R2). This process, called forwarding, is covered in the data plane. Additionally, a router can block the forwarded packets if they are malicious or duplicated. Routing is the determined route or path that packets flow in from a sender to a receiver. The controller plane determines a path using a routing algorithm between the sender and receiver (for example, from Host-A to Host-B in Figure 7). There are two routing structures in the controller plane: static and dynamic routing. While static routing works better in small networks, dynamic routing will be more effective for many networks. In the Software-Defined Network (SDN) paradigm, the forwarding and routing system differs from the classical system [154]. In SDN, the controller layer is moved from the underlying network to a logically centralized controller responsible for finding a path and installing routing

rules on the underlying forwarding elements. However, in this study, we focus on the classical structure instead of SDN.

Network Layer Protocols

The well-known protocols in the network layer include Internet Protocol versions 4 and 6 (IPv4 and IPv6) and Internet Control Message Protocol (ICMP).

Network-Layer Attacks

The common network-layer attacks are Smurf attacks, IP spoofing attacks, and hijacking attacks. The Smurf attack is a type of Distributed Denial-of-Service (DDoS) attack. An attacker spoofs the IP address of a victim's computer and sends a forged Internet Control Message Protocol (ICMP) echo request to the computers in the same broadcast. The computers reply with an ICMP echo-reply and cause flooding of the victim computer [155,156]. An IP spoofing attack is a technique in which the attacker uses a trusted IP address to send packets to the server, and the server cannot identify the IP address of the attacker. As a result, the attacker discovers a way to access the server [157]. Finally, a hijacking attack disrupts a server–client session and establishes a new session between the attacker and the server [158].

4.2.6. Data Link Layer

The data link layer is the second layer of the OSI model. The protocols are run by nodes in this layer. Nodes can be hosts, routers, switches, or Wi-Fi access points. The communication between the nodes is done along the communication channels, also known as links. Data from the source host to the destination host are transferred over the links [100,159].

Data Link Layer Protocols

There are plenty of protocols in this layer, but we present the common ones, which are Address Resolution Protocol (ARP), Spanning Tree Protocol (STP), and Serial Line Internet Protocol (SLIP). ARP, which works on the network layer, is responsible for determining link-layer addresses such as MAC and IP addresses [160]. There are plenty of paths among devices on the Internet. To prevent a loop between the devices, STP exchanges Bridge Protocol Data Unit (BPDU) packets among the devices to detect loops and close the related bridge interface [161]. SLIP encapsulates the Internet Protocol that works over serial ports and modem connections [162].

Data-Link-Layer Attacks

Some common attacks in the data link layer are MAC attacks, STP attacks, and ARP poisoning attacks. MAC attacks (a.k.a. Content Access Memory (CAM) Table Flooding) force a switch to operate like a hub to forward the packets to all the ports. This causes flood from the table to switch. STP attacks use forged BPDU messages to change the Spanning Tree topology. Frequent topology changes may cause DoS attacks [161]. Although it operates on the network layer, ARP poisoning (MAC spoofing) is carried out in the data link layer. The devices on the Local Area Network keep the entries' IP address and related MAC address in a cache. When an attacker sends a gratuitous ARP (GARP) packet over the Internet to announce the combination of spoofed MAC and IP addresses, the devices update their cache. Therefore, the attacker can use this process (called ARP poisoning) to monitor traffic by forcing the gateway's traffic to flow over their switch [161,163].

4.2.7. Physical Layer

The last layer of the OSI model is the physical layer. In contrast to the data link layer, the physical layer moves the individual bits instead of entire frames within the frame between the nodes.

Physical Layer Protocols

The protocols in this layer depend on the material and the medium of the links, which can be fiber optics, twisted-pair copper wire, Wi-Fi, and so on.

Physical-Layer Attacks

Some common physical-layer attacks are wiretapping, jamming, and tampering. A jamming attack is an attack where a jamming node interferes with transmitting packets to reduce network performance and is a severe attack on Wireless Sensor Networks (WSNs) [164]. A wiretapping attack refers to an attacker connecting a third-party wire to the connecting wires, which allows the attacker to observe and analyze the flow of data in active and passive modes [165]. A tampering attack is an unauthorized act in which an attacker modifies a system or its components and data on the network.

4.3. Threats

Wireless communications infrastructures and services are increasing to meet proliferating demands [157–166]. Accordingly, the increasing number of wireless devices brings security threats such as cyber criminal activities, malicious attacks, data forging, identity theft, and so on [157]. Furthermore, these threats are increasing because of smartphone usage for online banking and personal accounts. Therefore, it is crucial to boost wireless communication security to prevent threats. This chapter briefly presents some wireless network attacks, then provides methods to secure wireless networks.

Wireless Security Attacks

A wireless network is a computer network that connects devices by using Radio Frequency (RF), as seen in Figure 8. Malicious association is one of the typical wireless network attacks. An attacker targets a company access point and makes the wireless network card of their cracked laptop look like a legitimate access point. When a user connects to this access point, the attacker can steal the user's password. In addition, the attacker can launch attacks on the wired network. An accidental association is an unintentional threat that an unauthorized user connects to a wireless access point of a close-distance company's network. Since the company's information is exposed, this can be considered a security issue [166–170].

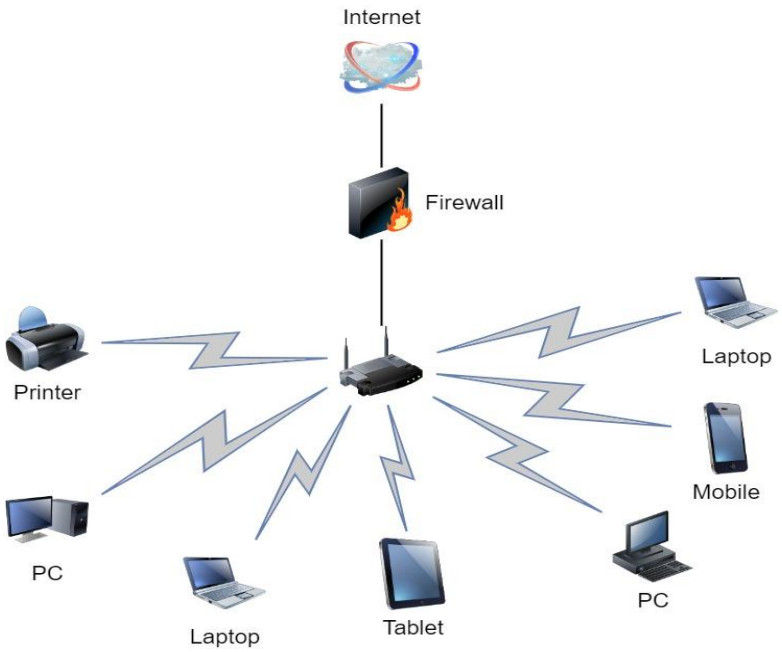

Figure 8. A sample of wireless networks.

Ad hoc networks are Peer-to-Peer (P2P) networks where clients are connected to each other wirelessly without using an access point. This type of network does not have enough protection, which may cause a significant number of threats [166–170]. Nontraditional networks such as Bluetooth devices can cause security risks because of weak security protection. An attacker can easily listen to the network traffic on these nontraditional networks, identify the MAC address, and exploit the network, which is called MAC

spoofing [73–76]. The Caffe Latte attack is a method that targets the WEP security protocol. The attacker obtains the WEP key using ARP requests to send a flood of encrypted ARP responses [166–170]. The above-mentioned network security attacks, such as man-in-the-middle, Denial of Service (DoS), and network injection, are also security threats to wireless networks [157].

Securing Wireless Networks

Encryption is one of the most effective ways to protect wireless networks. Therefore, a built-in encryption mechanism produces wireless routers and access points. Using antivirus, firewall, and antispyware software and updating them frequently is essential for wireless network protection. The routers come with a default identifier and password. Attackers know the default identifiers that can be used to access the network. Therefore, changing the default identifier and password to unique and strong ones is crucial. In addition, the identifier broadcasting should be turned off for the sake of network security. Each computer has its own Media Access Control (MAC) address that the computer uses when connected to the network. Wireless routers can be set to allow specific MAC addresses to access the network. However, this method is insufficient to secure the network perfectly since attackers can mimic MAC addresses. Last but not least, educating users about the importance of network security and routinizing the usage of protection methods is quite critical to reducing attacks and threats [157,166–170].

Securing switches is a crucial technique for the sake of network security. Switches can be protected by keeping them locked up, disabling unused ports, filtering MAC address tables, checking/controlling duplicate MAC addresses, providing unicast flood protection, and updating switches frequently [171]. Securing routers is also an important technique to protect users from threats. To do that, the user must change the router password and SSID from default to unique ones, encrypt Wi-Fi, turn off WPS and UPnP, use a password-protected guest network, control port forwarding, and periodically check for new firmware [172].

5. Evaluation of Cyber Security Vulnerabilities, Threats, Attacks, Solutions, and Future Challenges

This section discusses cyber security threats, attacks, possible solutions, and future research directions. Figure 9 shows the security solutions applied in the cyber security domain. Basically, solutions are divided into two main categories: technical and nontechnical. The nontechnical solutions can be listed as physical and administrative. The area protection, computing devices' physical security, data center disaster recovery plan, and the location of the backups are crucial when preserving physical security. Administrative-based management and adjustments are other essential concepts in nontechnical solutions. Policies, procedures, standards, risk assessment, vendor management, assigned responsibilities, and training are other important concepts when dealing with cyber attacks. Even if cyber security specialists create the most powerful protection system, adequate security will not be provided if the users of this system are not adequately trained. Thus, nontechnical solutions are as important as technical solutions. Technical solutions are divided into three groups: technologies and platforms, used tools, and applying AI and data science. The substantial technologies and platforms are given in Figure 9. Cryptography protects the data's integrity and confidentiality when stored on disk and in transit. Access control restricts access to the data, which increases security while decreasing the possibility of remote attack as well as privilege escalation. Big data allows for analyzing a large amount of data in order to discover unknown patterns as well as malicious features of attacks.

Emerging technologies such as blockchain, virtualization, and big data are also starting to be widely used in cyber security. For example, blockchain technology helps to validate the consistency of the data, as well as detect some complex attacks. Virtualization techniques separate software applications from the hardware components, which increases the software usability and decreases the cost, while reducing the downtime in case of cyber

attacks. Proactive threat management, advanced data security, scalability, high availability, and efficient data recovery are all features of the cloud computing platform.

Various well-known tools and protocols help to detect, prevent, and decrease the number of attacks (Figure 9). ACLs (Access control lists) can filter the packets based on the source IP addresses, ports, and protocols. Firewalls also filter the packages based on predefined rules. ACLs and firewalls help to reduce DDoS attacks. IDSs and IPSs are used to detect intrusions based on the signatures or anomalies in computer networks. VPNs, IPsec, TLS, and SSL technologies and protocols are used to protect data's confidentiality and integrity when transmitted across the network. The WSA and ESA protect the web servers and email servers, respectively. Antivirus scanners detect malware-related attacks in the end hosts. Vulnerability scanners help to detect and classify the vulnerabilities that systems have. They find the vulnerabilities before the attackers and give chances to patch the discovered vulnerabilities. To effectively protect computer systems, all the tools mentioned above, protocols, and technologies (Figure 9) need to be used in each layer. Additionally, new attack detection systems that use statistics, probability, data mining, and machine learning techniques are needed.

The attack surface and strategies evolve over time, decreasing the efficiency and feasibility of current detection systems. New solutions can be added to the existing ones or new systems designed to combat more intelligent attacks. Statistics, probability, data mining, and machine learning techniques can be used in this respect. Statistics is a scientific method that analyzes, interprets, and uncovers patterns in data. Probability is the technique that identifies the chance of an event occurring. Data mining is a method that discovers and extracts unknown patterns in large datasets. It intersects with statistics, machine learning, and computer science. Machine learning techniques allow computers to learn without being explicitly programmed. In other words, ML techniques describe the data algorithmically. Statistics and probability-based solutions have been used for many years in cyber security. However, data mining and ML techniques have become popular in the cyber security domain in recent years [173]. The new data mining and ML techniques help to add new features to the existing attack detection systems. In addition, these innovative technologies make detection systems more intelligent against recent cyber attacks.

ML-based techniques are varied, including regression, probabilistic, distance-based learning, decision trees, dimensionality reduction algorithms, and boosting–bagging algorithms applicable in cyber security. These ML-based techniques help to scan for data breaches and vulnerabilities in computer systems and communication networks. They provide fast analysis for large amounts of data and adjust it without domain expert input. Additionally, ML methods significantly improve threat detection accuracy and enhance network efficiency using heuristic techniques. Specifically, ML techniques are applicable in a wide range of areas in cyberspace. These application areas can be summarized as follows:

- Malware detection [174];
- Spam identification;
- Fraud detection [175];
- Malicious JavaScript detection;
- Anomaly detection [176,177];
- Malware classification [178];
- Risk classification;
- DNS classification;
- Phishing detection [179];
- Leakage detection;
- Hidden channel detection;
- Botnet detection;
- DDoS detection [180–182];
- Zero-day detection;
- APTs detection;
- Social media attacks detection;

- Vulnerability detection;
- Cryptographic attack detection.

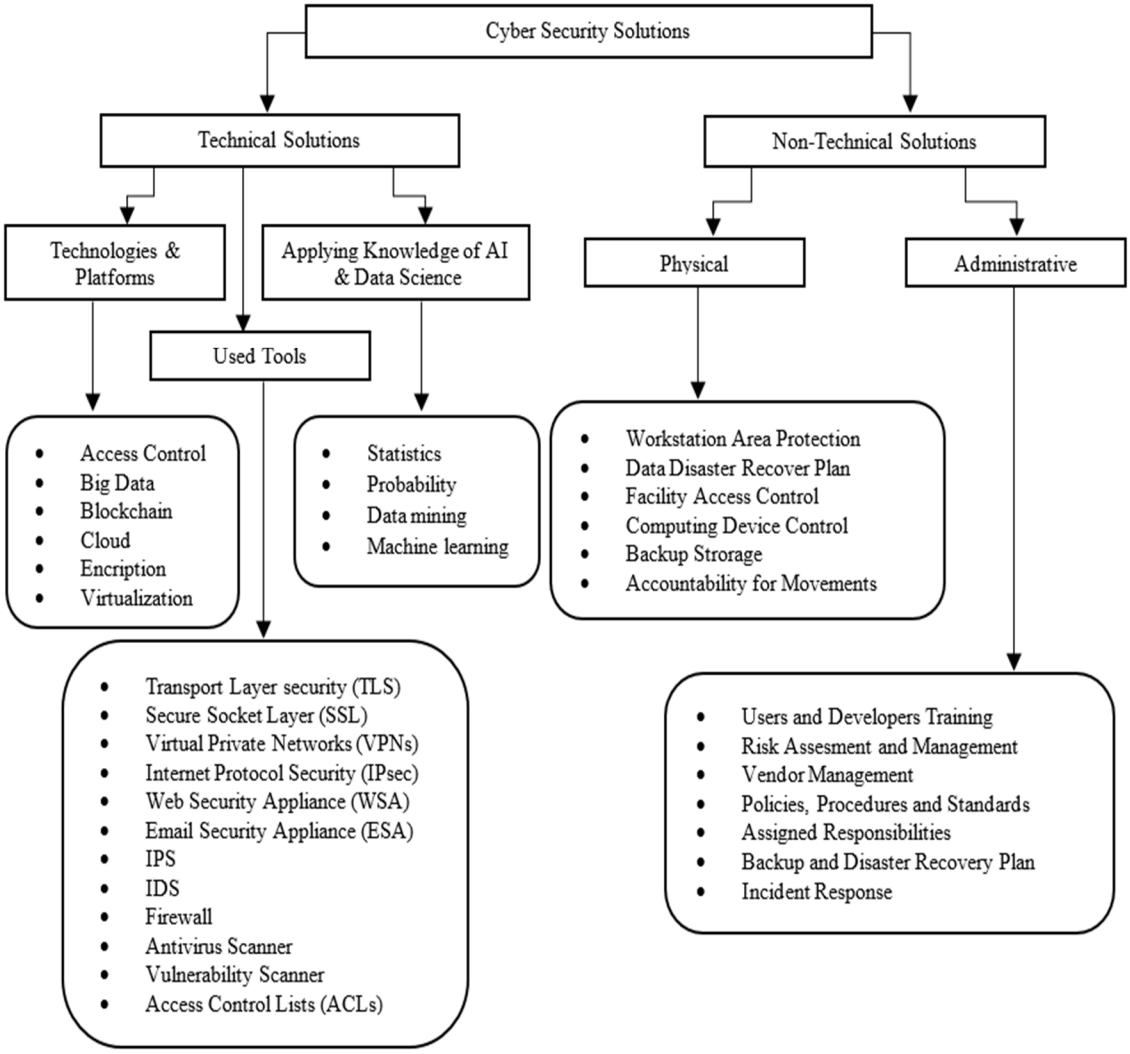

Figure 9. Represent the technical and non-technical cyber security solutions.

Even though there are several advances to detecting attacks in the digital world, there are still key challenges to identifying attacks in the cyber security domain. These challenges can be listed as follows:

- It takes a lot of time to design a secure system;
- It is not easy to create, store, and distribute confidential information;
- Security is often an afterthought;
- Security is often seen as a barrier;
- Security professionals must identify and fix all vulnerabilities—an attacker only needs to find one;
- Security often turns into a human issue;
- Detecting and preventing unknown attacks are challenging;
- The complexity of the attacks is increasing;
- Attacks are becoming automated by using cyber-attacks-as-a-service;
- Intelligent attacks bypass the detection systems;
- ML-based algorithms assume the data;
- ML-based algorithms are prone to bias;
- ML-based algorithms cannot handle outliers all the time;

- ML-based attacks are increasing;
- Classifying millions of network connections is a challenging task;
- Dealing with high-dimensional data is cumbersome;
- The data preprocessing step is complex because of multiple data formats;
- Creating contextual features is tough;
- Applying domain knowledge for automated analysis is difficult;
- Not enough consistent and up-to-date datasets are available to test the proposed methods in cyber security;
- The protection of multiple components is a challenging task;
- The attack vector is complex;
- Insider attacks;
- Outdated hardware;
- Software vulnerabilities are increasing;
- Loss of control over the data;
- Cloud-based attacks are increasing;
- IoT-based threats are expanding [183];
- Ransomware attacks are becoming more complicated;
- Social engineering techniques are evolving.

6. Conclusions

This comprehensive review paper summarizes cyber security problems and solutions based on recent technological advances. In order to provide solid and detailed information about cyber security, we divided cyber security issues into three extensive sections: cyber security fundamentals; threats, vulnerabilities, exploits, and attacks; and network security level by level. This division is critical for understanding the main components of cyber security and for providing holistic solutions to security problems.

In the cyber security fundamentals section, technical and nontechnical reasons that cause the increase in cyber attacks are listed. Cyber attacks are dynamic and affect all computer-based systems and the Internet environment by changing the attack format and target audience occasionally. The transfer of social life to the Internet environment increases cyber attacks and their destructive effects. Errors and vulnerabilities in software, the inadequacy of network protocols, the number of devices added to the network, and the complexity of critical systems all increase cyber security risks. Furthermore, the virtualization of social life, excessive use of social networks, attackers' increased knowledge, and users' careless Internet usage also raise security risks in the digital world.

The main components of attack strategies, which exploit the system and third-party software vulnerabilities, are explained in the section on threats, exploits, exploits, and attacks section. Cyber attackers use well-prepared malicious code blocks to exploit vulnerabilities in computer-based systems. Common malware (viruses, worms, rootkits, ransomware, etc.), hacking tools, application attacks, access attacks, cryptography attacks, and APTs (Advanced Persistent Threats) can be listed as common threats and attacks in the cyber security domain. Recently, cyber-attacks-as-a-service tools have become available for those who want to create cyber attacks. This increases the number of attacks and makes detection processes more challenging.

Each layer's common attacks and potential solutions are presented to comprehend network security fully. The attacks generally target a certain layer's protocols to succeed. Network attacks can be categorized based on layer, namely as physical-layer attacks (sniffing), data-link-layer attacks (spoofing: MAC, ARP, etc.), network-layer attacks (man-in-the-middle), transport-layer attacks (reconnaissance), session-layer attacks (hijacking), presentation-layer attacks (phishing), and application-layer attacks (exploits). The main reasons for the success of attacks arise from vulnerabilities in computer network protocols and the misconfiguration of network devices. These protocols can be listed as ARP, DNS, DHCP, FTP, ICMP, IP, TCP, UDP, etc. For instance, when packets are transmitted over the network using the IP protocol, there is no structure to control the accuracy and

confidentiality of these packets. Hence, the information in the packets can be exposed and changed during packet transmission. In the same way, since DNS responses are not verified, users connect to servers created by the attackers instead of the actual server. Existing protocol vulnerabilities must be reduced, new protocols must be added, and network devices must be configured correctly and completely to protect data as they move across computer networks.

To protect the computer-based system from attackers effectively, individuals, organizations, software developers, and countries must collaborate to provide extensive protection. In this context, the solutions can be categorized into technical and nontechnical. When dealing with cyber attacks, administrative-based management, policies, standards, procedures, risk assessment, vendor management, assigned responsibilities, and training are critical nontechnical concepts. Even if cyber security specialists create the most well-designed protection system, adequate security will not be provided if the users of this system are not adequately trained.

Technical solutions, on the other hand, use technological advances and science to create smart applications to deal with attackers. Technical solutions can be divided into three groups: technologies and platforms, used tools, and applying artificial intelligence and data science. Cryptography protects the integrity and confidentiality of data. Access control restricts access to data, which increases the level of security. Big data allows for analyzing a large amount of data in order to discover unknown patterns as well as malicious features of attacks. Virtualization techniques separate software applications from the hardware components, which increases the software usability and decreases the cost, while reducing the downtime in case of cyber attacks. The cloud computing platform provides proactive threat management, advanced data security, scalability, high availability, and efficient data recovery. Blockchain technology assists in validating the consistency of the data, as well as detecting some complex attacks. Statistical methods help to interpret and uncover patterns in data. Data mining discovers and extracts unknown patterns in large datasets. The ML techniques help to add new features to the existing attack detection systems. Additionally, these innovative ML technologies have improved detection systems' intelligence in the face of recent cyber attacks.

Even though the mentioned technical advances significantly improve the ability to scan for data breaches, find vulnerabilities in computer systems and communication networks, and enhance the accuracy of attack detection systems, there are still some challenges to effectively detecting new and complex cyber attacks. These challenges are that the complexity of the attacks is increasing; attacks are becoming automated by cyber-attacks-as-a-service; intelligent attacks bypass the detection systems; ML-based algorithms make assumptions about the data, which contain bias; classifying millions of network connections is challenging; dealing with high-dimensional data is cumbersome; the protection of multiple components is rugged; and security often turns into a human issue.

Author Contributions: Conceptualization, Ö.A. and M.O.-O.; methodology, Ö.A., M.O.-O., A.A.Y., E.A. and S.S.A.; formal analysis, E.A.; investigation, M.O.-O.; resources, Ö.A.; writing—original draft preparation, Ö.A., M.O.-O., A.A.Y., E.A. and S.S.A.; writing—review and editing, Ö.A., M.O.-O., A.A.Y., E.A. and S.S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data were not used in this study.

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

References

1. Pan, J.; Paul, S.; Jain, R. A survey of the research on future internet architectures. *IEEE Commun. Mag.* **2011**, *49*, 26–36. [CrossRef]
2. Safa, N.S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. *Comput. Secur.* **2016**, *56*, 70–82. [CrossRef]
3. Von Solms, R.; van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
4. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cyber security. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [CrossRef]

5. Wang, W.; Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
6. Papp, D.; Ma, Z.; Buttyan, L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In Proceedings of the 2015 13th Annual Conference on Privacy, Security and Trust, Izmir, Turkey, 21–23 July 2015; pp. 145–152.
7. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **2021**, *21*, 115–158. [CrossRef] [PubMed]
8. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
9. Kaur, J.; Ramkumar, K.R. The recent trends in cyber security: A review. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 5766–5781. [CrossRef]
10. Maglaras, L.A.; Kim, K.-H.; Janicke, H.; Ferrag, M.A.; Rallis, S.; Fragkou, P.; Maglaras, A.; Cruz, T.J. Cyber security of critical infrastructures. *ICT Express* **2018**, *4*, 42–45. [CrossRef]
11. Waseem, M.; Khan, M.A.; Goudarzi, A.; Fahad, S.; Sajjad, I.A.; Siano, P. Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies* **2023**, *16*, 820. [CrossRef]
12. Khan, M.A.; Saleh, A.M.; Waseem, M.; Sajjad, I.A. Artificial Intelligence Enabled Demand Response: Prospects and Challenges in Smart Grid Environment. *IEEE Access* **2023**, *11*, 1477–1505. [CrossRef]
13. Dasgupta, D.; Akhtar, Z.; Sen, S. Machine learning in cyber security: A comprehensive survey. *J. Def. Model. Simul. Appl. Methodol. Technol.* **2020**, *19*, 57–106.
14. Denning, D.E.R. *Cryptography and Data Security*; Addison-Wesley: Boston, MA, USA, 1982; p. 112.
15. Blackley, J.A.; Peltier, T.R.; Peltier, J. *Information Security Fundamentals*; Auerbach Publications: Boca Raton, FL, USA, 2004. [CrossRef]
16. Cole, E. *Network Security Bible*; John Wiley & Sons: Hoboken, NJ, USA, 2011; p. 768.
17. Aslan, O.; Yilmaz, A.A. A New Malware Classification Framework Based on Deep Learning Algorithms. *IEEE Access* **2021**, *9*, 87936–87951. [CrossRef]
18. Cyber-Security.Degree. Available online: https://cyber-security.degree/resources/history-of-cyber-security/ (accessed on 1 January 2023).
19. Wikipedia. List of Security Hacking Incidents. Available online: https://en.wikipedia.org/wiki/List_of_security_hacking_incidents (accessed on 1 January 2023).
20. Avast Blog. Available online: https://blog.avast.com/history-of-cybersecurity-avast (accessed on 1 January 2023).
21. Wikipedia. Creeper and Reaper. Available online: https://en.wikipedia.org/wiki/Creeper_and_Reaper (accessed on 1 January 2023).
22. Russell, D.; Gangemi, S.; Gangemi, G.T., Sr. *Computer Security Basics*; O'Reilly Associates, Inc.: Sebastopol, NY, USA, 1991.
23. Lehtinen, R.; Gangemi, G.T., Sr. *Computer Security Basics: Computer Security*; O'Reilly Media, Inc.: Sebastopol, NY, USA, 2006.
24. Wikipedia. Markus Hess. Available online: https://en.wikipedia.org/wiki/Markus_Hess (accessed on 1 January 2023).
25. Popularmechanics. A. Digital Spies: The Alarming Rise of Electronic Espionage. Pop. Mech. Available online: https://www.popularmechanics.com/technology/security/how-to/a7488/digital-spies-the-alarming-rise-of-electronic-espionage/ (accessed on 1 January 2023).
26. Aslan, O.; Ozkan-Okay, M.; Gupta, D. Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment. *IEEE Access* **2021**, *9*, 83252–83271. [CrossRef]
27. Center For Internet Security: The Mirai Botnet–Threats and Mitigations. Available online: https://www.cisecurity.org/blog/the-mirai-botnet-threats-and-mitigations/ (accessed on 1 January 2023).
28. Kaspersky. Available online: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (accessed on 1 January 2023).
29. CSO: Ransomware. Available online: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html (accessed on 1 January 2023).
30. Trendmicro. Available online: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware (accessed on 1 January 2023).
31. Cyware. Available online: https://cyware.com/research-and-analysis/covidlock-android-ransomware-spreading-amid-covid-19-epidemic-4a5b (accessed on 1 January 2023).
32. Manky, D. Cybercrime as a service: A very modern business. *Comput. Fraud. Secur.* **2013**, *2013*, 9–13. [CrossRef]
33. Aslan, Ö.; Samet, R. A Comprehensive Review on Malware Detection Approaches. *IEEE Access* **2020**, *8*, 6249–6271. [CrossRef]
34. Aslan, Ö.; Samet, R.; Tanrıöver, Ö.Ö. Using a Subtractive Center Behavioral Model to Detect Malware. *Secur. Commun. Netw.* **2020**, *2020*, 7501894. [CrossRef]
35. Whitman, M.E.; Mattord, H.J. *Principles of information security*; Cengage Learning: Boston, MA, USA, 2011; pp. 1–27.
36. AlMadahkah, A.M. Big data in computer cyber security systems. *Int. J. Comput. Sci. Netw. Secur. IJCSNS* **2016**, *16*, 56–65.
37. Schumacher, H.J.; Ghosh, S.; Lee, T.S. Top Secret Traffic and the Public ATM Network Infrastructure. *Inf. Syst. Secur.* **1999**, *7*, 27–45. [CrossRef]
38. Puttaswamy, K.P.N.; Kruegel, C.; Zhao, B.Y. Silverline: Toward data confidentiality in storage-intensive cloud applications. In Proceedings of the 2nd ACM Symposium on Cloud Computing, Cascais, Portugal, 26–28 October 2011.

39. Metz, C. AAA protocols: Authentication, authorization, and accounting for the Internet. *IEEE Internet Comput.* **1999**, *3*, 75–79. [CrossRef]
40. Paolini, A.; Scardaci, D.; Liampotis, N.; Spinoso, V.; Grenier, B.; Chen, Y. Authentication, Authorization, and Accounting. *Towards Interoper. Res. Infrastruct. Environ. Earth Sci.* **2020**, *12003*, 247–271. [CrossRef]
41. Sivathanu, G.; Wright, C.P.; Zadok, E. Ensuring data integrity in storage: Techniques and applications. In Proceedings of the 2005 ACM Workshop on Storage Security and Survivability, Fairfax, VA, USA, 11 November 2005.
42. Pipino, L.; Strong, D.; Richard, Y.W. Process-embedded data integrity. *J. Database Manag.* **2004**, *15*, 87–103.
43. Whitman, M.E.; Mattord, H.J. *Management of Information Security*; Cengage Learning: Boston, MA, USA, 2013; pp. 27–35.
44. Aslan, Ö. Analysis and detection of malware based on behaviors. PhD Thesis, University of Ankara, Ankara, Turkey, 2020.
45. Karri, R.; Rajendran, J.; Rosenfeld, K.; Tehranipoor, M. Trustworthy Hardware: Identifying and Classifying Hardware Trojans. *Computer* **2010**, *43*, 39–46. [CrossRef]
46. Weforum. Available online: https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/ (accessed on 1 January 2023).
47. Tehranipoor, M.; Wang, C. *Introduction to Hardware Security and Trust*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011.
48. McGraw, G. Building secure software: Better than protecting bad software. *IEEE Softw.* **2002**, *19*, 57–58. [CrossRef]
49. Aslan, Ö. How to decrease cyber threats by reducing software vulnerabilities and bugs. In Proceedings of the 1st International Mediterranean Science and Engineering Congress, Çukurova University, Adana, Turkey, 26–28 October 2016; pp. 639–646.
50. Aslan, O.; Samet, R. Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs. In Proceedings of the IEEE 2017 International Conference on Cyberworlds, Chester, UK, 20–22 September 2017; pp. 222–225. [CrossRef]
51. Techsurface. Available online: http://techsurface.com/2010/01/microsoft-security-development-lifecycle-sdl.html (accessed on 1 January 2023).
52. Broadcom. Available online: https://docs.broadcom.com/docs/istr-21-2016-en/ (accessed on 1 January 2023).
53. Mcafee. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf (accessed on 1 January 2023).
54. Padhy, R.P.; Manas, R.P.; Suresh, C.S. Cloud computing: Security issues and research challenges. *Int. J. Comput. Sci. Inf. Technol. Secur.* **2011**, *1*, 136–146.
55. Alcaraz, C.; Zeadally, S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 53–66. [CrossRef]
56. Lipso, H.F. *Tracking, and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*; Carnegie-Mellon University: Pittsburgh, PA, USA, 2002.
57. Ramirez, J.H.P. An Anomaly Behavior Analysis Methodology for the Internet of Things: Design, Analysis, and Evaluation. PhD Thesis, The University of Arizona, Tucson, AZ, USA, 2017.
58. Alcaraz, C.; Sherali, Z. Critical control system protection in the 21st century. *Computer* **2013**, *10*, 74–83. [CrossRef]
59. Trend Micro. Available online: http://blog.trendmicro.com/trendlabs-security-intelligence/operation-woolen-goldfish-when-kittens-go-phishing/ (accessed on 1 January 2023).
60. Info Security Group. Available online: http://www.infosecurity-magazine.com/news/potao-trojan-served-up-by-russian/ (accessed on 1 January 2023).
61. Litefinance. Available online: https://www.litefinance.com/blog/for-professionals/cryptocurrency-exchange-hacks-history-causes-and-effects/ (accessed on 1 January 2023).
62. BBC: News. Available online: https://www.bbc.com/news/world-asia-42845505 (accessed on 1 January 2023).
63. VARONIS. Available online: https://www.varonis.com/blog/cybersecurity-statistics/ (accessed on 1 January 2023).
64. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]
65. Jouini, M.; Rabai, L.B.A.; Ben Aissa, A. Classification of Security Threats in Information Systems. *Procedia Comput. Sci.* **2014**, *32*, 489–496. [CrossRef]
66. Khan, I. An introduction to computer viruses: Problems and solutions. *Libr. Hi Tech News* **2012**, *29*, 8–12. [CrossRef]
67. Rajesh, B.; Reddy, Y.J.; Reddy, B.D.K. A survey paper on malicious computer worms. *Int. J. Adv. Res. Comput. Sci. Technol.* **2015**, *3*, 161–167.
68. Jaiswal, M. Computer Viruses: Principles of Exertion, Occurrence, and Awareness. *Int. J. Creat. Res. Thoughts* **2017**, *5*, 648–651.
69. Bickford, J.; O'Hare, R.; Baliga, A.; Ganapathy, V.; Iftode, L. Rootkits on smartphones: Attacks, implications, and opportunities. In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, Annapolis, MD, USA, 22–23 February 2010; pp. 49–54.
70. Patil, S.; Jangra, A.; Bhale, M.; Raina, A.; Kulkarni, P. Ethical hacking: The need for cyber security. In Proceedings of the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, Chennai, India, 21–22 September 2017; pp. 1602–1606.
71. Dahbur, K.; Mohammad, B.; Tarakji, A.B. A survey of risks, threats, and vulnerabilities in cloud computing. In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications, Amman, Jordan, 18–20 April 2011; pp. 1–6.

72. Javaheri, D.; Hosseinzadeh, M.; Rahmani, A.M. Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines. *IEEE Access* **2018**, *6*, 78321–78332. [CrossRef]
73. Chen, R.; Li, Y.; Fang, W. Android malware identification based on traffic analysis. *Int. Conf. Artif. Intell. Secur.* **2019**, *11632*, 293–303.
74. Wadhwa, A.; Arora, N. A Review on Cyber Crime: Major Threats and Solutions. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 2217–2221.
75. Al-Rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Comput. Secur.* **2018**, *74*, 144–166. [CrossRef]
76. Pham, D.V.; Syed, A.; Mohammad, A.; Halgamuge, M.N. Threat analysis of portable hack tools from USB storage devices and protection solutions. In Proceedings of the 2010 International Conference on Information and Emerging Technologies, Karachi, Pakistan, 14–16 June 2010; pp. 1–5. [CrossRef]
77. Clausen, H.; Grov, G.; Sabate, M.; Aspinall, D. Better Anomaly Detection for Access Attacks Using Deep Bidirectional LSTMs. In Proceedings of the International Conference on Machine Learning for Networking, Paris, France, 24–26 November 2020; pp. 1–18. [CrossRef]
78. Humayun, M.; Niazi, M.; Jhanjhi, N.; Alshayeb, M.; Mahmood, S. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
79. Tundis, A.; Mazurczyk, W.; Mühlhäuser, M. A review of network vulnerabilities scanning tools: Types, capabilities and functioning. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 1–10.
80. Joshi, C.; Singh, U.K. Security testing and assessment of vulnerability scanners in quest of current information security landscape. *Int. J. Comput. Appl.* **2016**, *145*, 1–7. [CrossRef]
81. Wang, Y.; Yang, J. Ethical hacking and network defense: Choose your best network vulnerability scanning tool. In Proceedings of the 2017 31st International Conference on Advanced Information Networking and Applications Workshops, Taipei, Taiwan, 27–29 March 2017; pp. 110–113.
82. Peisert, S.; Schneier, B.; Okhravi, H.; Massacci, F.; Benzel, T.; Landwehr, C.; Mannan, M.; Mirkovic, J.; Prakash, A.; Michael, J.B. Perspectives on the SolarWinds Incident. *IEEE Secur. Priv.* **2021**, *19*, 7–13. [CrossRef]
83. Páez, C.; Michel, M. *Application Security Testing Tools STUDY and Proposal*; Universitat Oberta de Catalunya: Barcelona, Spain, 2021; pp. 1–53.
84. Rahalkar, S. *Quick Start Guide to Penetration Testing*; Apress: Berkeley, CA, USA, 2019. [CrossRef]
85. Roldán-Molina, G.; Almache-Cueva, M.; Silva-Rabadão, C.; Yevseyeva, I.; Basto-Fernandes, V. A comparison of cyber security risk analysis tools. *Procedia Comput. Sci.* **2017**, *121*, 568–575. [CrossRef]
86. Karangle, N.; Mishra, A.K.; Khan, D.A. Comparison of Nikto and Uniscan for measuring URL vulnerability. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies, Kanpur, India, 6–8 July 2019; pp. 1–6. [CrossRef]
87. Pattanavichai, S. Comparison for network security scanner tools between GFI LanGuard and Microsoft Baseline Security Analyzer (MBSA). In Proceedings of the 2017 15th International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, 22–24 November 2017; pp. 1–7. [CrossRef]
88. Ndatinya, V.; Xiao, Z.; Manepalli, V.R.; Meng, K.; Xiao, Y. Network forensics analysis using Wireshark. *Int. J. Secur. Netw.* **2015**, *10*, 91–106. [CrossRef]
89. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
90. Al-Khurafi, O.B.; Al-Ahmad, M.A. Survey of web application vulnerability attacks. In Proceedings of the 2015 4th International Conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, Malaysia, 8–10 December 2015; pp. 154–158.
91. Pavlenko, A.; Buzdalov, M.; Ulyantsev, V. Fitness comparison by statistical testing in construction of SAT-based guess-and-determine cryptographic attacks. In Proceedings of the Genetic and Evolutionary Computation Conference, Prague, Czech Republic, 13–17 July 2019; pp. 312–320. [CrossRef]
92. Vimal, S.; Kalaivani, L.; Kaliappan, M. Collaborative approach on mitigating spectrum sensing data hijack attack and dynamic spectrum allocation based on CASG modeling in wireless cognitive radio networks. *Clust. Comput.* **2017**, *22*, 10491–10501. [CrossRef]
93. Pawar, M.V.; Anuradha, J. Network Security and Types of Attacks in Network. *Procedia Comput. Sci.* **2015**, *48*, 503–506. [CrossRef]
94. Basit, A.; Zafar, M.; Liu, X.; Javed, A.R.; Jalil, Z.; Kifayat, K. A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommun. Syst.* **2020**, *76*, 139–154. [CrossRef] [PubMed]
95. Kramer, S.; Bradfield, J.C. A general definition of malware. *J. Comput. Virol.* **2010**, *6*, 105–114. [CrossRef]
96. Eslahi, M.; Salleh, R.; Anuar, N.B. Bots and botnets: An overview of characteristics, detection and challenges. In Proceedings of the 2012 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, 23–25 November 2012; pp. 349–354.
97. Raza, M.; Iqbal, M.; Sharif, M.; Haider, W. A survey of password attacks and comparative analysis on methods for secure authentication. *World Appl. Sci. J.* **2012**, *19*, 439–444.

98. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [CrossRef]
99. Zimmermann, H. OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection. *IEEE Trans. Commun.* **1980**, *28*, 425–432. [CrossRef]
100. Kurose, J.F.; Ross, K.W. *Computer Networking: A Top Down Approach*, 7th ed.; Pearson Publishers: Upper Saddle River, NJ, USA, 2012.
101. Think Security: DHCP Starvation—Quick and Dirty. Available online: http://think-security.com/dhcpstarvation-quick-and-dirty/ (accessed on 1 January 2023).
102. Syed, S.; Khuhawar, F.; Talpur, S. Machine Learning Approach for Classification of DHCP DoS Attacks in NIDS. In Proceedings of the 2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), Charlotte, NC, USA, 10–12 October 2021; pp. 143–146.
103. Droms, R. *Dynamic Host Configuration Protocol (RFC 2131)*; IETF: Fremont, CA, USA, 1997.
104. Alexander, S.; Droms, R. *DHCP Options and BOOTP Vendor Extensions (RFC 2132)*; IETF: Fremont, CA, USA, 1997.
105. Internetlivestats. Available online: https://www.internetlivestats.com/ (accessed on 1 January 2023).
106. Dinu, D.D.; Togan, M.; Bica, I. On DHCP Security. *Proc. Rom. Acad. Ser. A Math. Phys. Tech. Sci. Inf. Sci.* **2017**, *18*, 403–412.
107. Younes, O.S. A Secure DHCP Protocol to Mitigate LAN Attacks. *J. Comput. Commun.* **2016**, *4*, 39–50. [CrossRef]
108. Tripathi, N.; Hubballi, N. A probabilistic anomaly detection scheme to detect DHCP starvation attacks. In Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, Bangalore, India, 6–8 November 2016; pp. 1–6.
109. Droms, R.; Arbaugh, W. *Authentication for DHCP Messages(RFC 3118)*; IETF: Fremont, CA, USA, 2001.
110. RFC 1035: Domain Names—Implementation and Specification. Available online: https://datatracker.ietf.org/doc/html/rfc1035 (accessed on 1 January 2023).
111. Cloudflare. Available online: https://www.cloudflare.com/learning/dns/what-is-dns/ (accessed on 1 January 2023).
112. Lyu, M.; Gharakheili, H.H.; Sivaraman, V.A. Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques. *arXiv* **2022**, arXiv:2201.00900. [CrossRef]
113. Gien, M. A File Transfer Protocol (FTP). *Comput. Netw.* **1978**, *2*, 312–319. [CrossRef]
114. Postel, J.; Reynolds, J.K. *File Transfer Protocol (RFC0959)*; IETF: Fremont, CA, USA, 1985.
115. Koksal, O.; Tekinerdogan, B. Feature-Driven Domain Analysis of Session Layer Protocols of Internet of Things. In Proceedings of the 2017 IEEE International Congress on Internet of Things, Linz, Austria, 22–25 October 2017; pp. 105–112. [CrossRef]
116. Goralski, W. *The Illustrated Network: How TCP/IP Works in a Modern Network*; Morgan Kaufmann: Burlington, MA, USA, 2017.
117. Postmark. Available online: https://postmarkapp.com/guides/everything-you-need-to-know-about-smtp (accessed on 1 January 2023).
118. Abdulkadhim, E.G.; Hayder, M.A. Survey of E-mail Classification: Review and Open Issues. *Iraqi J. Comput. Inform.* **2020**, *46*, 17–23.
119. Makeuseof. Available online: https://www.makeuseof.com/tag/pop-vs-imap/ (accessed on 1 January 2023).
120. Cerf V., G. On heterogeneous computing. *Commun. ACM* **2021**, *64*, 9. [CrossRef]
121. Harrington, D.; Presuhn, R.; Wijnen, B. *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (RFC 3411)*; IETF: Fremont, CA, USA, 2002.
122. Hong, L.; Yang, H. The security mechanism of SNMPv3 and implementation based on SNMP++. In Proceedings of the 2013 International Conference on Communications, Circuits and Systems, Mumbai, India, 4–5 April 2013; pp. 109–111.
123. Juniper. Available online: https://www.juniper.net/documentation/software/junos-security/junos-security10.2/mib-srx5600-srx5800-service-gateway/topic-21511.html (accessed on 1 January 2023).
124. Peng, Y.; Xie, F.; Zhao, W.; Wang, D.; Han, X.; Lu, T.; Li, Z. Analysis of security threats and vulnerability for cyber-physical systems. In Proceedings of the 2013 3rd International Conference on Computer Science and Network Technology, Dalian, China, 12–13 October 2013; pp. 50–55.
125. Tripathi, N.; Hubballi, N. Application Layer Denial-of-Service Attacks and Defense Mechanisms: A Survey. *ACM Comput. Surv.* **2021**, *54*, 1–33. [CrossRef]
126. Imperva: Global DDoS Threat Landscape Quarter 4. Available online: https://www.incapsula.com/ddos-report/ddos-report-q4-2017.html (accessed on 1 January 2023).
127. Imperva: Slowloris. Available online: https://www.imperva.com/learn/application-security/slowloris/ (accessed on 1 January 2023).
128. Imperva: 2019 Global DDoS Threat Landscape Report. Available online: https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/ (accessed on 1 January 2023).
129. Cambiaso, E.; Papaleo, G.; Chiola, G.; Aiello, M. Slow DoS Attacks: Definition and Categorisation. *Int. J. Trust Manag. Comput. Commun.* **2013**, *3*, 300–319. [CrossRef]
130. Gonzalez, H.; Gosselin-Lavigne, M.A.; Stakhanova, N.; Ghorbani, A.A. The Impact of Application-Layer Denial-of-Service Attacks. In *Case Studies in Secure Computing: Achievements and Trends*; CRC Press Taylor and Francis: Boca Raton, FL, USA, 2014.
131. Mantas, G.; Stakhanova, N.; Gonzalez, H.; Jazi, H.H.; Ghorbani, A.A. Application-layer denial of service attacks: Taxonomy and survey. *Int. J. Inf. Comput. Secur.* **2015**, *7*, 216–239. [CrossRef]

132. Singh, K.; Singh, P.; Kumar, K. User Behaviour Analytics-based Classification of Application Layer HTTP-GET Flood Attacks. *J. Netw. Comput. Appl.* **2018**, *112*, 97–114. [CrossRef]
133. Dietzel, C.; Smaragdakis, G.; Wichtlhuber, M.; Feldmann, A. Stellar: Network Attack Mitigation using Advanced Blackholing. In Proceedings of the International Conference on emerging Networking EXperiments and Technologies, Roma, Italy, 6–9 December 2018; pp. 152–164.
134. Hubballi, N.; Tripathi, N. A closer look into DHCP starvation attack in wireless networks. *Comput. Secur.* **2017**, *65*, 387–404. [CrossRef]
135. Malhotra, A.; Van Gundy, M.; Varia, M.; Kennedy, H.; Gardner, J.; Goldberg, S. The Security of NTP's Datagram Protocol. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kinabalu, Malaysia, 10–14 February 2017; pp. 405–423.
136. Tripathi, N.; Hubballi, N. Detecting stealth DHCP starvation attack using machine learning approach. *J. Comput. Virol. Hacking Tech.* **2017**, *14*, 233–244. [CrossRef]
137. Tripathi, N.; Hubballi, N. Slow rate denial of service attacks against HTTP/2 and detection. *Comput. Secur.* **2018**, *72*, 255–272. [CrossRef]
138. Hollis, L. OSI presentation layer activities. *Proc. IEEE* **1983**, *71*, 1401–1403. [CrossRef]
139. Roberts, R.M. *Networking Fundamentals Course Outline & Text Materials*; Wilcox Publisher: Tinley Park, IL, USA, 2005.
140. Kumar, G. Denial of service attacks–An updated perspective. *Syst. Sci. Control Eng.* **2016**, *4*, 285–294. [CrossRef]
141. Keerthi, V.K. Taxonomy of SSL/TLS attacks. *Int. J. Comput. Netw. Inf. Secur.* **2016**, *8*, 15–24.
142. OSI-model. Available online: https://osi-model.com/session-layer/ (accessed on 1 January 2023).
143. Baitha, A.K.; Vinod, S. Session hijacking and prevention technique. *Int. J. Eng. Technol.* **2018**, *7*, 1939–1988.
144. Jain, V.; Sahu, D.R.; Tomar, D.S. Session Hijacking: Threat Analysis and Countermeasures. *Int. Conf. Futur. Trends Comput. Anal. Knowl. Manag.* **2015**, *1*, 1–6.
145. Burgers, W.; Verdult, R.; Van Eekelen, M. Prevent Session Hijacking by Binding the Session to the Cryptographic Network Credentials. In Proceedings of the Nordic Conference on Secure IT Systems, Reykjavik, Iceland, 30 November–2 December 2013; Volume 8208, pp. 33–50. [CrossRef]
146. Maltz, D.A.; Bhagwat, P. MSOCKS: An architecture for transport layer mobility. In Proceedings of the IEEE INFOCOM'98, the Conference on Computer Communications. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies 1998, San Francisco, CA, USA, 29 March–2 April 1998; Volume 3, pp. 1037–1045.
147. Welzl, M.; Islam, S.; Gundersen, M.; Fischer, A.; Kosek, M.; Shreedhar, T.; Bajpai, V.; Chiariotti, F.; Deshpande, A.A.; Giordani, M.; et al. Transport Layer Innovations for Future Networks. *IEEE Commun. Mag.* **2021**, *59*, 14–15.
148. Schuba, C.L.; Krsul, I.V.; Kuhn, M.G.; Spafford, E.H.; Sundaram, A.; Zamboni, D. Analysis of a denial of service attack on TCP. In ıN. In Proceedings of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 4–7 May 1997; pp. 208–223.
149. Eddy, W. *TCP SYN Flooding Attacks and Common Mitigations(RFC 4987)*; IETF: Fremont, CA, USA, 2007.
150. Pandey, A.; Saini, J.R. Attacks & Defense Mechanisms for TCP/IP Based Protocols. *Int. J. Eng. Innov. Res.* **2014**, *3*, 17–23.
151. Sula, E. A review of Network Layer and Transport Layer Attacks on Wireless Networks. *Int. J. Mod. Eng. Res.* **2018**, *8*, 23–27.
152. Qian, Z.; Mao, Z.M.; Xie, Y. Collaborative TCP sequence number inference attack: How to crack sequence number under a second. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; pp. 593–604.
153. Bellovin, S.M. Security problems in the TCP/IP protocol suite. *ACM SIGCOMM Comput. Commun. Rev.* **1989**, *19*, 32–48. [CrossRef]
154. Akin, E.; Korkmaz, T. Comparison of Routing Algorithms with Static and Dynamic Link Cost in Software Defined Networking (SDN). *IEEE Access* **2019**, *7*, 148629–148644. [CrossRef]
155. Sajjad, F. *Denial of Service–The Smurf Attack*; School of Computer Science University of Windsor: London, UK, 2009.
156. Bouyeddou, B.; Harrou, F.; Sun, Y.; Kadri, B. Detection of smurf flooding attacks using Kullback-Leibler-based scheme. In Proceedings of the 2018 4th International Conference on Computer and Technology Applications, Istanbul, Turkey, 3–5 May 2018; pp. 11–15.
157. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
158. Manivannan, S.S.; Sathiyamoorthy, E. A Prevention Model for Session Hijack Attacks in Wireless Networks Using Strong and Encrypted Session ID. *Cybern. Inf. Technol.* **2014**, *14*, 46–60. [CrossRef]
159. FederalRegister. Session Co. IT5 Tx. 225. ORGANIZATION. Available online: https://archives.federalregister.gov/issue_slice/1994/6/13/30386-30446.pdf (accessed on 1 January 2023).
160. David, C.P. *An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware (RFC 826)*; IETF: Fremont, CA, USA, 1982.
161. Mahmood, S.; Mohsin, S.M.; Akber, S.M. Network security issues of data link layer: An overview. In Proceedings of the 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies, Sukkur, Pakistan, 29–30 January 2020; pp. 1–6.
162. Stevens, W.R. *TCP/IP Illustrated, Volume 1: The Protocols*; Addison Wesley: Boston, MA, USA, 1994; ISBN 0-201-63346-9.

163. Tripathi, N.; Mehtre, B.M. Analysis of various ARP poisoning mitigation techniques: A comparison. In Proceedings of the 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies, Kanyakumari, India, 10–11 July 2014; pp. 125–132.
164. Liu, G. Jamming Attacks and Countermeasures in Wireless Area Networks. PhD Thesis, Hong Kong Polytechnic University, Hong Kong, China, 2012.
165. Deka, G.C. *Handbook of Research on Securing Cloud-Based Databases with Biometric Applications*; IGI Global: Hershey, PA, USA, 2014.
166. Aliu, O.G.; Imran, A.; Imran, M.A.; Evans, B. A Survey of Self Organisation in Future Cellular Networks. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 336–361. [CrossRef]
167. ElSawy, H.; Hossain, E.; Haenggi, M. Stochastic Geometry for Modeling, Analysis, and Design of Multi-Tier and Cognitive Cellular Wireless Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 996–1019. [CrossRef]
168. Choi, M.K.; Robles, R.J.; Hong, C.H.; Kim, T.H. Wireless network security: Vulnerabilities, threats and countermeasures. *Int. J. Multimed. Ubiquitous Eng.* **2008**, *3*, 77–86.
169. Kavianpour, A.; Anderson, M.C. An overview of wireless network security. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 24–26 June 2017; pp. 306–309.
170. Stallings, W.; Brown, L.; Bauer, M.D.; Howard, M. *Computer Security: Principles and Practice*; Pearson: Upper Saddle River, NJ, USA, 2012.
171. The Cyber security Man: Switch Security. Available online: https://thecybersecurityman.com/2018/01/30/switch-security/ (accessed on 1 January 2023).
172. Routersecurity.org. Available online: https://routersecurity.org/ (accessed on 1 January 2023).
173. Houichi, M.; Jaidi, F.; Bouhoula, A. A Systematic Approach for IoT Cyber-Attacks Detection in Smart Cities Using Machine Learning Techniques. In Proceedings of the International Conference on Advanced Information Networking and Applications, Toronto, ON, Canada, 12–14 May 2021; pp. 215–228. [CrossRef]
174. Shah, S.S.H.; Ahmad, A.R.; Jamil, N.; Khan, A.U.R. Memory Forensics-Based Malware Detection Using Computer Vision and Machine Learning. *Electronics* **2022**, *11*, 2579. [CrossRef]
175. Malik, E.F.; Khaw, K.W.; Belaton, B.; Wong, W.P.; Chew, X. Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture. *Mathematics* **2022**, *10*, 1480. [CrossRef]
176. Hu, X.; Xie, C.; Fan, Z.; Duan, Q.; Zhang, D.; Jiang, L.; Wei, X.; Hong, D.; Li, G.; Zeng, X.; et al. Hyperspectral Anomaly Detection Using Deep Learning: A Review. *Remote. Sens.* **2022**, *14*, 1973. [CrossRef]
177. Gadal, S.; Mokhtar, R.; Abdelhaq, M.; Alsaqour, R.; Ali, E.S.; Saeed, R. Machine Learning-Based Anomaly Detection Using K-Mean Array and Sequential Minimal Optimization. *Electronics* **2022**, *11*, 2158. [CrossRef]
178. Akhtar, M.S.; Feng, T. Malware Analysis and Detection Using Machine Learning Algorithms. *Symmetry* **2022**, *14*, 2304. [CrossRef]
179. Mughaid, A.; AlZu'bi, S.; Hnaif, A.; Taamneh, S.; Alnajjar, A.; Abu Elsoud, E. An intelligent cyber security phishing detection system using deep learning techniques. *Clust. Comput.* **2022**, *25*, 3819–3828. [CrossRef]
180. Alashhab, A.A.; Zahid, M.S.M.; Azim, M.A.; Daha, M.Y.; Isyaku, B.; Ali, S. A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks. *Symmetry* **2022**, *14*, 1563. [CrossRef]
181. Saghezchi, F.B.; Mantas, G.; Violas, M.A.; Duarte, A.M.D.O.; Rodriguez, J. Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs. *Electronics* **2022**, *11*, 602. [CrossRef]
182. Almaraz-Rivera, J.G.; Perez-Diaz, J.A.; Cantoral-Ceballos, J.A. Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models. *Sensors* **2022**, *22*, 3367. [CrossRef]
183. Goudarzi, A.; Ghayoor, F.; Waseem, M.; Fahad, S.; Traore, I. A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies* **2022**, *15*, 6984. [CrossRef]