Review

Wireless Technology Security and Privacy: A Comprehensive Study

Hamza Azam , Micheal Tan , Lim Tik Pin , Muhammad Afiq Syahmi , Antony Liew Wen Qian , Huang Jingyan , Muhammad Fuhad Uddin , Siva Raja Sindiramutty *

Posted Date: 9 November 2023

doi: 10.20944/preprints202311.0664.v1

Keywords: Intrusion Prevention System (IPS); Intrusion Detection System (IDS); Intrusion Detection and Presentation System (IDPS); Deep Packet Inspection (DPI); Network-Based Prevention System (NIPS)

Review

Wireless Technology Security and Privacy: A Comprehensive Study

Hamza Azam [1], Micheal Tan [1], Lim Tik Pin, Muhammad Afiq Syahmi [1], Antony Liew Wen Qian, Huang Jingyan [3], Muhammad Fuhad Uddin [2] and Siva Raja Sindiramutty [1]

[1] Schools of Computer Science Taylor's University**;** hamzazam00@gmail.com ; michaelyinhan.tan@sd.taylors.edu.my; 331961@sd.taylors.edu.my; afiqsyahmi.muhammadzulhilmi@sd.taylors.edu.my;0321885@sd.taylors.edu.my ; 676562216@qq.com; mohammedfuhad1@gmail.com; siva.sindiramutty@taylors.edu.my

[2] Seneca College, School of Software Design & Data Science, Canada

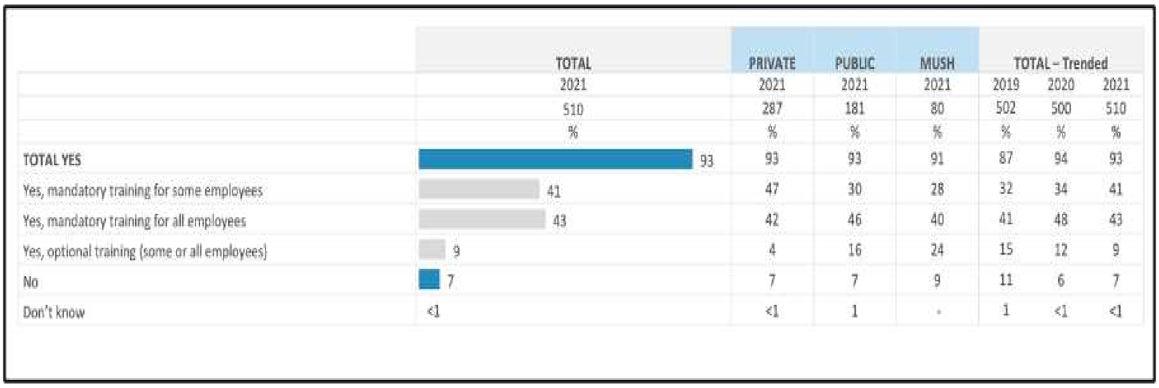
[3] International Business School, Dongbei University of Finance and Economics, China

Abstract: Since the advent of the Internet, there has been a significant shift from wired to wireless communication between devices. The volume of data transmitted has surged, primarily driven by the exponential growth of network services, Internet of Things (IoT) devices, and online users. This trend became especially pronounced with the onset of the COVID-19 pandemic, as the Internet's role and significance expanded dramatically. People began to spend more time online, engaging in activities like e-learning, remote work, and online shopping. Concurrently, concerns about the security of wireless communication channels have escalated. As more data is stored and transmitted over the Internet, cybercriminals are actively seeking unauthorized access to it to further their malicious objectives. Through a comprehensive literature review in the realm of wireless network security and privacy, it has become evident that several factors render these networks susceptible to vulnerabilities. The aim of this paper is to shed light on the major and common security and privacy challenges faced by existing wireless networks. Additionally, it seeks to demonstrate the array of techniques available to mitigate these issues. Ultimately, this paper will culminate in an in-depth analysis of cybersecurity measures to address the issues in wireless networks.

Keywords: Intrusion Prevention System (IPS); Intrusion Detection System (IDS); Intrusion Detection and Presentation System (IDPS); Deep Packet Inspection (DPI); Network-Based Prevention System (NIPS)

INTRODUCTION

With the ever-advancing field of computer science and technology, which includes cloud computing, big data, and artificial intelligence, and the relentless progress of global information sharing, Internet technology has become an indispensable driving force for societal advancement [1] [51] [68]. The onset of the COVID-19 pandemic initiated a significant transformation across all industries, ushering in the era of widespread Work-From-Home (WFH) arrangements. To facilitate these changes, industries now rely heavily on dependable wireless communication channels, involving both hardware like laptops and software applications such as Zoom. This has led to a surge in demand for such communication channels worldwide. However, this shift is not without its challenges and drawbacks. Wireless communication networks are increasingly responsible for transmitting sensitive data [52] [69]. Since wireless transmissions are broadcast, the data being sent is vulnerable to eavesdropping [3] [70]. With the transition to remote work, the security landscape for businesses expanded, introducing new threats as organizations needed to secure not only their office environments but also individual employees working from home during the pandemic. This has made maintaining cybersecurity costly and challenging, especially for smaller firms [53][71]. Cyberattacks have evolved significantly since the emergence of computers in the late 1980s, evolving in tandem with the progress of information technology. According to Figure 1.0 [4], 93 percent of businesses have implemented cybersecurity training, but there's a split, with some companies making training mandatory for all employees (43% of the 93 percent), while others offer it as an optional resource.



	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2021	2021	2021	2021	2019	2020	2021
	510	287	181	80	502	500	510
	%	%	%	%	%	%	%
TOTAL YES	93	93	93	91	87	94	93
Yes, mandatory training for some employees	41	47	30	28	32	34	41
Yes, mandatory training for all employees	43	42	46	40	41	48	43
Yes, optional training (some or all employees)	9	4	16	24	15	12	9
No	7	7	7	9	11	6	7
Don't know	<1	<1	1	-	1	<1	<1

Figure 1. Does your organization conduct cybersecurity awareness training for its employee? [4].

According to Figure 1.0 [4], it's concerning that some organizations still treat cybersecurity training as optional when it should be considered essential. Among the 93 percent, 41 percent only make it mandatory for selected employees. The truth is, cyberattacks can target anyone, regardless of their position, be it a CEO or an IT support staff member. One example of such an attack involved cybercriminals infecting a company's computers with malware and using a keylogger to steal banking passwords [5] [72]. A keylogger is software that silently records keystrokes and sends the data to a hacker [54] [73]. They can then use this information to access bank accounts. This situation could have been prevented with mandatory cybersecurity training for all employees. In this case [5] [74], the malicious software was delivered and installed by cybercriminals through email. Therefore, it's crucial for employees to receive education on email security and be aware of potential email risks, including keyloggers, social engineering attacks, and phishing attempts, among others. Due to the pandemic, many people worldwide are working from home, and online video conferencing applications like Zoom and Microsoft Teams have seen a surge in users. However, this increased usage has also led to more vulnerabilities and attacks [56]. For example, Zoom fell victim to a credential stuffing attack due to its recent user growth. Researchers from IntSights discovered various databases with Zoom credentials, some containing hundreds and others hundreds of thousands [6] [75]. They gathered this information from various online crime forums and dark web shops that stored usernames and passwords stolen in cyberattacks dating back to 2013. Notably, Zoom did not cross-check registration usernames and passwords with known compromised account credentials, which allowed attackers to access Zoom user accounts. This attack resulted in the announcement of the sale of 500,000 stolen Zoom passwords on the dark web in early April 2020 [6] [76]. Blockchain technology offers a potential solution to these issues. With blockchain, secure sharing, examination, and storage of digital data become more accessible. Moreover, data transmitted can be encrypted using cryptography, as will be explained in more detail later in this paper.

In summary, the objective of this paper is to provide a comprehensive assessment of security and privacy issues in wireless networks, aiming to develop enhanced security methods for IT systems and showcase the utility of blockchain technology [1] [77] in the realm of network security. This paper critically examines the security and privacy challenges within wireless networks, with the intention of highlighting the importance of individual cybersecurity awareness and promoting societal security.

Definition of Wireless Technology

Wireless technology, which enables the transmission of data without the need for a physical medium, has become a pervasive feature, creating a globally interconnected experience across devices such as phones, laptops, and Internet of Things (IoT) devices, all reliant on this technology.

Over the course of more than 30 years, wireless technology has undergone significant evolution, giving rise to systems like 5G, Bluetooth, Wi-Fi, and other innovations. Some of these systems have spearheaded revolutionary advancements, including high-speed optical communications, multiple-input multiple-output (MIMO), and orthogonal frequency-division multiplexing (OFDM) transmission technologies, all aimed at providing more reliable and faster communications [61] [78]. These wireless mediums make use of radio frequencies across various wavelengths and frequencies, employing diverse tools and techniques to transmit data in the form of radio waves into the open. Tools like Wi-Fi chipsets, now affordable and user-friendly, have played a pivotal role in driving this evolution in wireless technology [61] [79]. As these tools and techniques continue to become more accessible and cost-effective, the demand for channels of data transmission escalates, aligning with the increasing applications for such technology.

Application Of Wireless Technology and Its Benefits

Numerous industries have embraced wireless technology to streamline processes, enhance efficiency, and simplify communication in various environments. For instance, tasks that traditionally required sending physical mail or messengers can now be easily accomplished through email or phone calls, all made possible by wireless technology. This shift allows individuals and organizations to focus on more challenging tasks that necessitate manual intervention. Wireless technology finds applications in a wide range of fields, including virtual/augmented reality (VR/AR), autonomous driving, Internet of Things (IoT), wireless backhaul (a replacement for optical fiber installations), and even emerging applications that are yet to be conceived, all of which demand higher bandwidth and reduced latency [62] [80]. The versatility of wireless technology continues to grow with technological advancements, offering a multitude of benefits. These advantages include increased mobility, enabling access to information and the exchange of data without the need for physical connections to a medium. Scalability is another key benefit, as the cost of ownership decreases over time, making wireless technology a cost-effective and efficient solution for data transmission. Additionally, the flexibility to configure wireless technology to meet specific needs and the ease of installation contribute to its appeal. Wireless systems offer extended reach without the requirement for cabling, further enhancing their utility [63] [81]. All these factors contribute to ongoing efforts dedicated to advancing the field of wireless technology.

Importance of Protecting Wireless Technology

The rapid growth of wireless technology brings forth legitimate concerns about the security and privacy of continuously transmitted data. With various applications come various security considerations. Wireless technology often plays a critical role in authenticating internet services, a process necessary to confirm the identity of users seeking access to these services. Authentication is typically accomplished through factors such as passwords, personal identification numbers, or biometrics, among others. Alongside authentication, there is the concept of authorization, where different systems are configured with various authorization levels, granting users different degrees of access [64]. In systems that combine authentication and authorization, a considerable volume of data is frequently relayed, encompassing various types that require encryption for protection. Encryption adds a layer of complexity that makes it more challenging for unauthorized individuals to access the data without proper authorization and authentication. Despite these security measures, numerous methods have been developed to exploit vulnerabilities and gain access to data, potentially causing significant harm to data owners. Therefore, safeguarding wireless technology is of paramount importance to establish robust, secure systems that can thwart potentially damage.

Scope of the paper

The scope of this comprehensive study is to delve into the multifaceted domain of wireless technology security and privacy, addressing critical issues, challenges, and solutions. Wireless technology, which includes various forms of wireless communication such as Wi-Fi, Bluetooth, cellular networks, and more, has become an integral part of our daily lives. It offers tremendous benefits in terms of convenience, mobility, and connectivity, revolutionizing the way we communicate, access information, and interact with the digital world. In this paper, we aim to define wireless technology and elucidate its diverse applications, emphasizing the advantages it brings to individuals and organizations. Simultaneously, we underscore the imperative need for protecting wireless networks and the data they transmit, as vulnerabilities in this domain can lead to significant breaches of security and privacy. Our paper explores the security and privacy challenges associated with wireless technology, covering issues like denial-of-service attacks, unauthorized access through piggybacking and wardriving, identity theft, data breaches, and eavesdropping, among others. To provide a comprehensive analysis, we review existing literature, categorizing security and privacy issues in wireless networks, and then propose a unique solution framework. Our study will consider research questions that arise in this context, detailing the methodology used for data collection and analysis. We will focus on search strategies, including keywords and source selection, and clearly define inclusion and exclusion criteria for the research materials. By the end of this paper, readers will gain a profound understanding of the security and privacy landscape in wireless technology. They will also be introduced to innovative solutions and recommendations to mitigate these risks. This paper ultimately seeks to empower individuals, businesses, and policymakers with the knowledge and tools needed to safeguard their wireless environments, ensuring a secure and private digital experience in an increasingly interconnected world.

RELATED RESEARCH BACKGROUND

A) Security and Privacy Issues of Wireless Networks

I. Denial of Service (DoS)

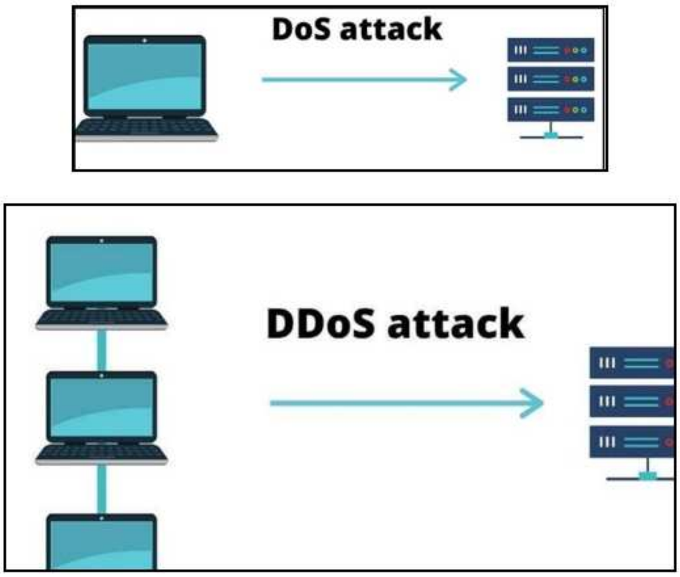


Figure 2. Architecture of DoS Attacks.

From the time of their initial discovery to the present day, there are two primary types of Denial-of-Service (DoS) attacks. The key difference between these two kinds of attacks lies in the number of computers or devices used to execute the attack, which can involve a single device or multiple devices. An attack that employs only one computer to disrupt the target system is known as a Denial of Service (DoS) attack. Conversely, an attack that utilizes more than one computer or device to disrupt the target system is referred to as a Distributed Denial of Service (DDoS) attack. In a Denial-of-Service attack, the source device sends an overwhelming volume of unnecessary data to the target device, such as network gateways, network switches, routers, network access points, and more, with the intention of causing disruption on the target network [13,65]. These disruptions can result in prolonged network downtime, network crashes, and slowed network responses, as the target network or devices struggle to process the inundation of incoming requests. DoS attacks occur frequently, with an increasing rate of incidents, affecting thousands to millions of individuals. The ease of launching DoS attacks, coupled with their minimal requirement for specialized knowledge, contributes to their prevalence [14,66]. It's worth noting that DoS attacks can be initiated through wireless networks as well as the World Wide Web [15,16], which means that even public networks are at risk of being targeted and compromised by DoS attacks [17,67]. The table below provides a historical overview of DoS cases in past years.

Table 1. 0: Overview of DoS cases in past years.

Victim	Year	Severity	Description of DDoS/DoS Attack
Amazon	2020	2.3 Tbps*, **world's largest**DDoS Attack in record.	In February 2020, AWS was targeted by its owncustomer where they launched a full-scale DDoS attack against AWS. The transmission speed of the attack had reached a new record of the previous DDoS attacks. Luckily AWS' intrusion prevention system known as AWS Shield had automatically intercepted the attack and prevented the largest system down ever from happening.
GitHub	2018	1.3 Tbps*, recorded **third largest** DDoS attacks. Where includes shocking 126.9Million of packets per second.	In February 2018, GitHub suffered a DDoS attack andcaused a 20-minute of downtime. According to the IPSreport, the recorded speed of the attack is 1.3 Terabytes per second and up to 127 million of internetpackets were sent every second.
GitHub	2018	1.7 Tbps*, the **second largest**scale of DDoS recorded past.	2018 is not a good year for GitHub as they suffered another DDoS attack within a month after the last DDoS attack. The source of the attack is from a clientthat is hosted by a network company called NETSCOUT. And thanks to the reliable IPS of GitHub, the severity of the DDoS has been mitigated.
BBC	2015	600 Gbps**, biggest DDoS attack recorded in 2015. And longest service downtime.	In December 2015, the pioneer news broadcasting company BBC suffered a DDoS attack from a group of hackers called the "New World Hacking". A speed of 600 Gigabytes per second attack was launched andcaused BBC a shocking 3 hours of downtime. And theattack was launched by using a system pressure testing tool known as "BangStresser".

* *Terabytes per second; ** Gigabytes per second.*

II. Piggybacking and Wardriving

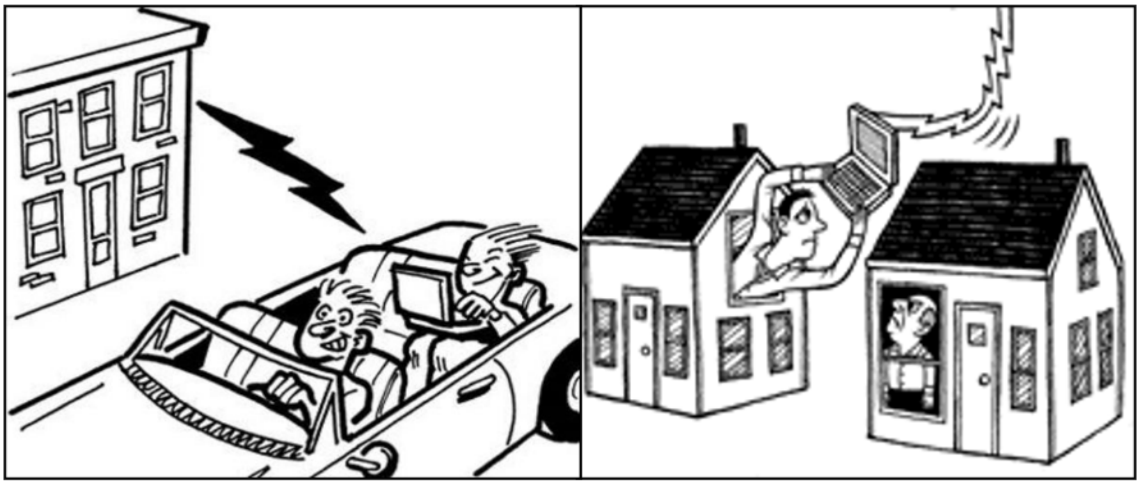


Figure 3. Wi-Fi Piggybacking and Wardriving.

The concept of network/wireless piggybacking shares similarities with real-life piggybacking, albeit in different forms. While physical piggybacking is typically harmless, network/wireless piggybacking can pose potential risks to wireless network owners, as it is considered illegal [14&15]. To delve deeper into the subjects of piggybacking and wardriving, it's essential to understand the workings of Wi-Fi. Wi-Fi operates by transmitting signals through radio waves, and there are limited effective means to confine these waves within the confines of residential properties. Consequently, it's not uncommon to discover neighboring Wi-Fi SSIDs appearing on our devices [26]. Certain individuals engage in Wi-Fi piggybacking by successfully guessing the password that protects a network. This activity is commonly referred to as network intrusion. Once they breach the network's defenses, these individuals gain unauthorized access to and can potentially steal sensitive data connected within the local area network. Furthermore, there is another form of piggybacking, where attackers roam specific areas, such as residential neighborhoods, in vehicles equipped with network antennas to detect available Wi-Fi signals. This practice is known as wardriving [27]. Wardriving attackers typically attempt to infiltrate networks either by guessing Wi-Fi passwords or by connecting to unsecured networks [28]. Unsecured networks encompass public networks, school networks, and similar types. Once access is granted, attackers can obtain information from all devices connected to the local area network, mirroring the risks associated with piggybacking [29]. Notably, larger-scale victims of wardriving attacks include public networks and home networks lacking password protection. Figure 3 shows example of Wi-Fi Piggybacking and Wardriving.

III. Spoofing and Keylogging

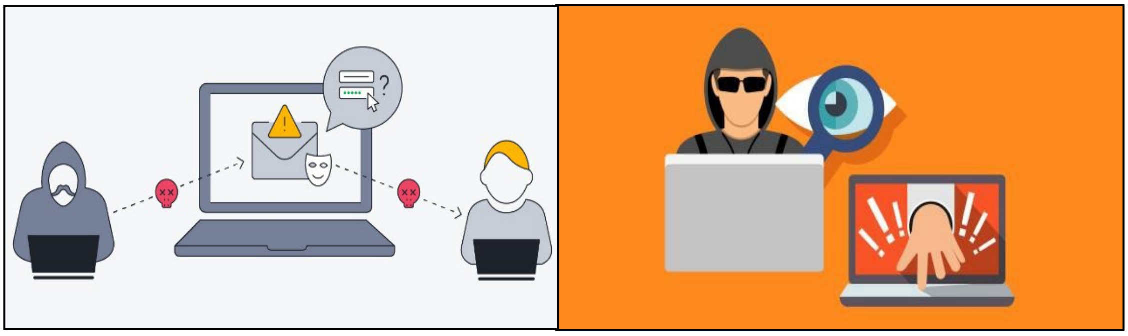


Figure 4. Keylogging and Spoofing.

Spoofing constitutes a criminal activity in which attackers adopt the guise of everyday tools that users frequently employ. These deceptive tools encompass emails, fraudulent phone calls, and websites that closely mimic legitimate ones. Additionally, attackers may impersonate service providers, including servers such as DNS servers and web servers. The advent of wireless networks has ushered in a transformation in the realm of spoofing, shifting from traditional physical connections, such as internet cable network connections, to wireless network connections. This evolution encompasses Wi-Fi spoofing, Near Field Communication (NFC) spoofing, Wireless Local Area Network (WLAN) spoofing, and more.

Wireless network spoofing offers attackers an easier route to infiltrate victims' networks and access valuable data and information, surpassing the methods of traditional spoofing [23]. Simultaneously, it intensifies the potential for inbound attacks on networks and poses greater risks to users. In addition to spoofing, keylogging activities have also evolved in tandem with the evolution of network connections [28 & 29]. Keylogging, also known as "keystroke logging" involves attackers embedding scripts to log every keystroke made by the victim.These logged keystrokes may include crucial information like passwords, credit card details, and identification numbers [21 & 22]. Given the escalating security concerns in wireless networks, attackers can integrate keylogging attacks with the aforementioned security issues, such as conducting "live keylogging" while piggybacking or wardriving victims' wireless networks to immediately capture keystroke information.

IV. Rogue Access Points

Rogue Access Points, also known as rogue routers, are devices intentionally set up by malicious individuals to deceive wireless network users. These criminals configure a rogue router to replicate the Service Set Identifier (SSID) of a legitimate Wi-Fi network [30]. To an unsuspecting user, the Wi-Fi SSID they see on their devices appears identical (refer to the image below) [31]. Users often assume that this SSID might belong to a different Wi-Fi band, like the 5 Gigahertz or 2.4 Gigahertz band, and may connect to either SSID without much thought. However, the danger lies in the fact that these rogue access points may not provide encrypted data transmission between the host and the connected clients, thus raising the risk of falling victim to phishing attacks and other internet-related security issues [32].

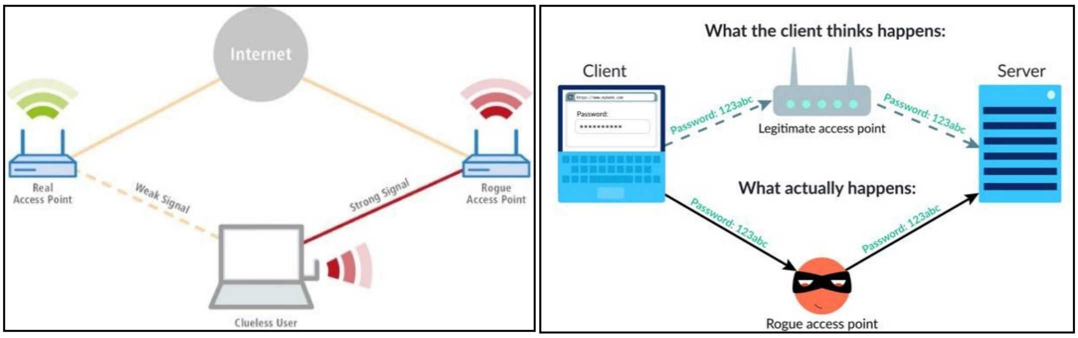
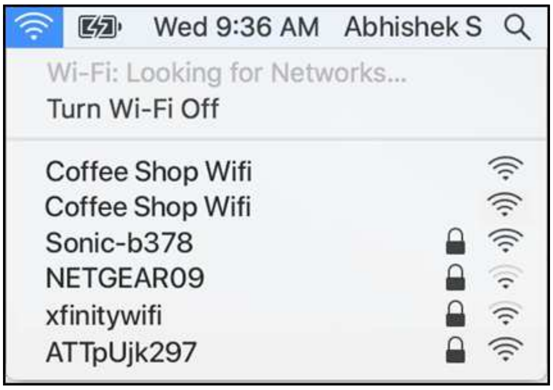


Figure 5. Rogue Access Points.



Wed 9:36 AM Abhishek S

Wi-Fi: Looking for Networks...

Turn Wi-Fi Off

Coffee Shop Wifi
Coffee Shop Wifi
Sonic-b378
NETGEAR09
xfinitywifi
ATTpUjk297

Figure 6. Image X.X Rogue Wi-Fi SSIDs (CofeeShop Wifi).

In the event that the user unknowingly connects to the rogue access point, which is controlled by the malicious attacker, they become vulnerable to various forms of attacks without their awareness. All of their internet traffic passes through the attacker's devices before reaching the intended server, and the server's responses likewise pass through the attacker's equipment. This implies that every piece of data, every packet, transmitted between the user and the server effectively passes through the prying eyes of the attacker. As a result, the attacker gains the ability to monitor and intercept all personal and sensitive information belonging to the victim. This, in turn, can lead to substantial losses and significant privacy breaches for the victim. Table 2 below shows the report about attacks on wireless teachnology.

Table 2. Report of type of treat from year 2016 - 2019.

Ref No	Year	Threat	Description
[13]	2016	Denial of Service	Discusses the effects of Denial of Service attacks towards a network

[14]	2017	Denial of Service	Discusses the process and the requirements inorder to launch a Denial of Service attack towards a wireless network
[15]	2015	Denial of Service	Discusses the how Wireless Networks act as a catalyst for Denial of Service attack
[16]	2021	Denial of Service	Discusses the how Wireless Networks act as a catalyst for Denial of Service attack
[17]	2013	Denial of Service	Discusses the wireless network types that are more vulnerable to Denial of Service attacks
[18]	2015	Keylogging	Discusses how Keylogging methods evolve from wired to wireless network connection.
[19]	2015	Keylogging	Discusses how Keylogging methods evolve from wired to wireless network connection.
[20]	2011	Keylogging	Discusses the method of Keylogging during an attack
[21]	2017	Keylogging	Discusses the information that are retrieved/stolen from the Keylogging attacks
[22]	2009	Keylogging	Discusses the information that are retrieved/stolenfrom the keylogging attacks and how wireless networks are making Keylogging easier
[23]	2011	Spoofing	Discusses the Wireless Network Connections that might be at risk of Spoofing Attacks
[24]	2019	Piggybacking	Discusses the legal aspects of Piggybacking an unknown wireless network
[25]	2009	Piggybacking	Discusses the legal aspects of Piggybacking an unknown wireless network
[26]	2017	Piggybacking	Discusses the reason on why is Piggybacking a thing and what are the reasons of Piggybacking
[27]	2011	Piggybacking & Wardriving	Discusses the similarities of Piggybacking and Wardriving and what kind of wireless network is potentially targeted
[28]	2017	Piggybacking & Wardriving	Discusses on why are Public Networks more prone to Piggybacking and Wardriving
[29]	2015	Wardriving	Discusses the consequences if the wireless network security is not well-configurated
[30]	2019	Rogue Access Point	Discusses the similarities of Legitimate Wi-Fi network and the Rogue Access Point network andhow they work in real-life
[31]	2019	Rogue Access Point	Discusses on how does a Rouge Access Point works and how attackers benefit from it
[32]	2019	Rogue Access Point	Discusses the consequences and other risks of Rogue Access Point

B) Privacy Issues in Wireless Network

I. Identity Theft

Identity theft is a pressing privacy concern in today's digital age, where much of our personal lives has migrated to the online realm [33] [86]. This malicious act involves the illicit acquisition of an individual's personal information without their consent, often for nefarious purposes, such as financial gain or damaging the victim's reputation [34]. The increasing reliance on electronic storage for sensitive data, including personal and financial information, accessible through wireless networks, has heightened the vulnerability to unauthorized access [37]. In this digital landscape, identity theft primarily occurs as a result of cyberattacks, with eavesdropping being a notable method employed by cybercriminals to exploit security weaknesses and access sensitive personal information. Eavesdropping involves intercepting communications or data transmission to surreptitiously collect information. Cybercriminals can employ various techniques, like packet sniffing, to intercept data transmitted over unsecured networks, thus gaining access to sensitive information, such as login credentials or financial details. As individuals continue to conduct personal and financial transactions online, this vulnerability remains a significant threat [33] [87–93].

Moreover, with the proliferation of social media, online banking, and e-commerce, people share vast amounts of personal data online, inadvertently providing cybercriminals with a treasure trove of information to exploit. As a result, the risk of identity theft remains substantial in the digital age. To mitigate this threat, individuals must exercise caution when sharing personal information online and regularly update their online security measures. Employing strong, unique passwords and using two-factor authentication can add an extra layer of protection. Organizations and service providers must also play a critical role in enhancing cybersecurity to safeguard the personal data entrusted to them, as the consequences of identity theft can be financially and emotionally devastating [33]. As the digital landscape continues to evolve, it is imperative for both individuals and institutions to remain vigilant in the battle against identity theft.

II. Data Breach

Data breaches have become an increasingly common and concerning occurrence in today's digital landscape, affecting a wide range of organizations and individuals. These incidents involve the unauthorized theft of personal information, often resulting in significant harm and damages. Stolen data from such breaches can encompass various sensitive categories, including financial data (e.g., credit card numbers and bank account information), trade secrets, personally identifiable data (PID), and business-related information [37][82]. While data breaches may share some similarities with identity theft, their key distinguishing factor lies in the extent of the damage they cause. Data breaches are typically more harmful than identity theft due to the sheer volume and variety of sensitive information exposed. The consequences of a data breach can be far-reaching, impacting not only the individuals whose data is compromised but also the organizations responsible for safeguarding that information. The severity of this issue is underscored by the fact that some countries have implemented data breach notification laws. These regulations obligate companies to report data breach incidents to relevant authorities and affected individuals, enhancing transparency and accountability in the face of such breaches [38] [94–97]. Several prominent companies have unfortunately fallen victim to significant data breach incidents, underscoring the widespread nature of this problem. These breaches have highlighted vulnerabilities in the digital security infrastructure, reminding organizations and individuals alike of the need for robust cybersecurity measures to protect against data breaches. In conclusion, data breaches are a growing concern, affecting individuals and organizations with potentially devastating consequences. The increasing frequency of these incidents emphasizes the importance of implementing strong cybersecurity measures and adhering to data breach notification laws to mitigate the risks associated with such breaches [36].

Table 3. Privacy issue case.

Company	Year	Affected	Description
Yahoo!	2013-14	3B accounts	In September 2016, Yahoo revealed the company's largest data breach to date. All of the email addresseswere taken, along with their true names, phone numbers, passwords, and birth dates.
LinkedIn	2012 & 2016	165M accounts	LinkedIn stated that the credentials of 165 million members were stolen and exposed on a Russian hacker website. The information

			was sold for only 5-bitcoins (almost $2000) by the hacker. LinkedIn had finally reset all of the account passwords.
Zynga	2019	218M accounts	A Pakistani hacker claimed to have hacked the accounts of all 218 million players. Later, Zynga admitted that all user information, including user ids and passwords, had been taken. This entire event took place entirely on the Facebook gaming platform.
Adobe	2013	153M accounts	Hackers acquired over 150 million user login credentials, credit card records, and company data bases. As a result, Adobe agreed to pay $1 million to customers for breaching the Customer Records Act.

There are several attacks that can cause identity theft and data breaches. This report will discuss two attacks, eavesdropping and phishing, including the way it works.

III. Eavesdropping

Eavesdropping is a well-known passive attack in the realm of cybersecurity, earning its name due to its non-disruptive nature, which doesn't impede network and communication operations [39] [85]. This type of attack hinges on attackers covertly intercepting communications between two legitimate users without their awareness or consent [40]. The inherent passivity of eavesdropping makes it a stealthy threat, as victims often remain oblivious to the intrusion, rendering it a potent danger to privacy. Eavesdropping poses a significant risk to the security of personal and confidential information, as it involves the theft or interception of sensitive data. Such breaches often occur when individuals connect to networks where traffic is inadequately secured or encrypted. Attackers exploit the vulnerabilities in unsecured traffic, making it relatively easy to carry out eavesdropping attacks. Notably, wireless networks are particularly susceptible to this type of assault due to the unique characteristics of the wireless medium. Although encryption schemes are available at the upper layers of the network stack, they may not be universally effective, primarily due to hardware limitations such as constraints on node power [41]. These limitations can leave wireless networks vulnerable to eavesdropping, making it crucial for users to be aware of the security measures in place within a given network. Employing robust encryption and security protocols is essential for safeguarding against eavesdropping, especially in the context of wireless networks. In summary, eavesdropping is a passive yet stealthy attack that jeopardizes the privacy and confidentiality of digital communications. Its prevalence is accentuated in unsecured or inadequately encrypted network environments, with wireless networks being particularly susceptible. To mitigate this threat, it is imperative for users to be vigilant about the security of the networks they connect to and employ encryption measures that can withstand the challenges posed by eavesdroppers [41].

IV. Phishing

Phishing has long been a significant security concern, with no definitive solution in place [42]. This type of attack revolves around deceiving victims into trusting the attacker, who often impersonates a trustworthy person or organization to obtain confidential information. Phishing attacks are frequently carried out through email (email spoofing), wherein malicious code or links are embedded in the email content, directing victims to a pre-defined malicious website and prompting them to enter their credentials [43,44] [83]. Notably, nearly half of phishing sites employ the HTTPS protocol, a ploy aimed at making them appear legitimate [45]. The most common targets of phishing attacks include bank account numbers, credit card information, internet banking credentials, usernames, and passwords [46][84].

There are various types of phishing attacks:

1. Email Phishing: This is the most prevalent form of phishing, wherein attackers send rushed emails to victims, often claiming that their accounts have been compromised and

urging immediate action. The goal is to trick victims into performing specific actions, such as clicking on malicious links that lead to fake login pages. When victims enter their credentials, their personal information is transmitted to the attackers [46].

2. Spear Phishing: This type of phishing necessitates thorough research to gather information about the victim. The research might involve gathering data from social media, such as the victim's name, friends, and locations. Armed with this information, attackers pose as a trusted contact and attempt to obtain confidential information through email or other messaging tools [46].
3. Evil Twin Phishing: In this type of phishing, attackers set up a counterfeit Wi-Fi network that directs users to a phishing site when they connect to it. Once on the phishing site, victims are prompted to provide personal information, including login credentials. With access to these credentials, attackers can infiltrate the network, monitor unencrypted traffic, and devise strategies to steal valuable data or information [47].
4. Clone Phishing: This form of phishing involves using a genuine email to create a nearly identical email that is then sent from a spoofed email account closely resembling the original sender. Links in the email are typically replaced with malicious ones. Since it replicates an existing email, clone phishing stands out from other forms of phishing due to its higher precision [48].

Table 4. Privacy issue.

Ref No	Year	Domain	Description
[33]	2017	Identity Theft	Discusses the identity theft detection in the mobile social networks
[34]	2016	Identity Theft	Discusses the process of discovering identity theft in wireless networks
[35]	2019	Identity Theft	Discusses the type of identity theft and the protection strategies
[36]	2018	Data Breach	Discusses the analysis and visualization of a data breach, including the insights
[37]	2021	Data Breach	Discusses the Wi-Fi risks and the data breach, along with the measures to tackle the incident
[38]	2019	Data Breach	Discusses the analysis of issues in the data breach notification
[39]	2018	Eavesdropping	Discusses the issues in the mobile wireless networks, including the brief analysis of the issues
[40]	2016	Eavesdropping	Discusses the eavesdropping attack as a major threat in the wireless networks
[41]	2017	Eavesdropping	Discusses the protection in the eavesdropping attack using a novel anti-eavesdropping scheme
[42]	2018	Phishing	Discusses the phishing as a major threat, the challenges, and the solution
[43]	2021	Phishing	Discusses the phishing acts as an attack to hack

			wireless networks credentials
[44]	2018	Phishing	Discusses the detection of phishing, how to differentiate between real email and phishing email
[45]	2020	Phishing	Discusses the benchmarking and evaluation of detecting the phishing
[46]	2019	Phishing	Discusses the overview of phishing, along with the types and the countermeasures strategy
[47]	2021	Phishing	Discusses the review of a phishing attack in the internet of things as well as the countermeasures ofthe attack
[48]	2019	Phishing	Discusses the phishing attack in the blockchain projects as well as the protection of the attack

RESEARCH METHODOLOGY

This section delves into the research methodologies employed in the creation of this research survey. Our research approach for this paper draws inspiration from the methods used in [7] and [8]. The primary aim of this research survey is to offer readers a comprehensive guide to the latest developments in security and privacy, particularly concerning the issues within wireless networks. To accomplish this objective, we have established a set of guidelines to be adhered to when conducting in-depth research within this specific subject area. The methodologies and guidelines utilized in this research survey will be elaborated upon in the following subsections.

A. Research questions

The formulation of research questions serves to keep the research focused within the defined subject area, reducing the risk of straying from the intended domain. Research questions also play a pivotal role in facilitating the efficient retrieval of essential information, as they serve as the cornerstone upon which the research is built. The research questions crafted for this survey and the rationale behind them can be found in Table 5.

Search strategy

An effective search strategy is a crucial element in all types of research. In this research survey, we have meticulously designed the research strategy to ensure that the search phase is conducted efficiently, resulting in more effective overall research [49]. This strategy employs two main techniques, namely, the use of keywords and the selection of sources. Both of these techniques are explained in detail below.

1. Keywords

We have defined specific keywords for each of the research questions to streamline the search process and enhance efficiency. These keywords are listed in Table 1 alongside the corresponding questions they are associated with. The connection between keywords and questions is indicated through the use of Boolean operators, which assist in specifying conditions within keywords or search strings.

Table 5. Research Question and Keywords.

Research Question	Keywords
What are the security and privacy issues in wireless networks?	“Security Issues” Wireless Networks” OR “Privacy Issues” Wireless Networks”
Security Issues	
What to know about Denial of Service or Distributed Denial of Service?	“Denial of Service”
What to know about Wireless Piggybacking and	“Piggybacking” AND “Wardriving”

Wardriving?	
What to know about Spoofing and Keylogging?	“Spoofing” AND “Keylogging”
What to know about Rogue Access Points?	“Rogue Access Points”
Privacy Issues	
What to know about Identity Theft?	“Identity Theft”
What to know about Data Breach?	“Data Breach”
What to know about Eavesdropping?	“Eavesdropping”
What to know about Phishing?	“Phishing”

2. Search documentation and Selection of sources

To elevate the quality and efficiency of our research, we have meticulously assessed and restricted our sources to those that are pertinent and encompass a broad spectrum of papers related to our subject area. Many of these electronic repositories are equipped with robust search engines that aid in generating more precise results using our search strings and keywords [50]. Table 6 provides an in-depth overview of our search strategy and documents these searches, including key information such as the date of access, the number of results retrieved, and more.

Table 6. Source selection and search documentation.

Source	Date Accessed	# of results retrieved without filter	# of results with filter (by years)
Security Issues			
Google Scholar	15 Nov, 2021	28,039	17,648
Semantics Scholar	15 Nov, 2021	16,485	7,438
IEEE Explore	15 Nov, 2021	5,578	2,914
Science Direct	15 Nov, 2021	3,891	1,596
Springer	15 Nov, 2021	10,396	6,365
Privacy Issues			
IEEE Explore	13 Nov, 2021	5,758	2,574
Science Direct	13 Nov, 2021	1,591	884
Springer	13 Nov, 2021	17,164	8,694

3. Inclusion and exclusion criteria

The establishment of inclusion and exclusion criteria simplifies the decision-making process by providing clear guidelines that dictate whether a document should be included or excluded. Every paper retrieved from the search results using the search string or keywords was subject to a thorough evaluation, and its eligibility was assessed based on the criteria outlined below. These inclusion and exclusion criteria are detailed as follows:

a. Inclusion criteria

i. The research paper must be published during or after the year 2016.

ii. Only papers written in the English language are included.

iii. Publications relevant to the discussion topic were considered.

b. Exclusion criteria

i. All publications before 2016 are excluded.

ii. All papers that do not answer any of the research questions have been excluded.

iii. Papers with less than four pages of length were excluded.

4. In-Depth Discussion and Summary

In this section, we delve into the in-depth findings and provide a summary of the results obtained in our research. Before embarking on this study, our team meticulously selected the topics to address and established stringent guidelines to ensure the precision and accuracy of the information gathered, keeping it aligned with the core objectives of our research. Based on our findings, it is apparent that privacy and security enhancement are not always a top priority for individuals and organizations.

One of the primary topics we explored was Denial of Service (DoS) attacks. From our research, it is evident that no organization, regardless of its size or prominence, is immune to Distributed Denial of Service (DDoS) or DoS attacks [57]. Even organizations as substantial as Amazon, GitHub, and BBC, faced with their advanced IT capabilities, are not entirely impervious to such threats. The critical point of consideration is how these organizations respond to and mitigate these attacks. For example, GitHub, a platform with over 73 million developers, initially experienced a 20-minute downtime during a DDoS attack. However, they subsequently prepared and successfully defended against a similar attack with the help of a reliable Intrusion Prevention System. In contrast, Amazon managed to withstand the largest DDoS attack in history, with a severity of 2.3 Terabytes per second, without incurring any losses. These instances underscore the importance of proactive preparation for various forms of cyberattacks, including Denial of Service attacks.

Turning our attention to privacy challenges, the COVID-19 pandemic has brought about a surge in remote work and increased reliance on unsecured networks. This situation has presented a ripe opportunity for cybercriminals, as the lack of robust privacy protection and lax cybersecurity practices render users more vulnerable to attacks, including phishing and eavesdropping [58]. To illustrate the real-world consequences of these vulnerabilities, consider a major data breach on a gaming platform. In 2019, Zynga, one of the largest browser gaming platforms on Facebook, fell victim to a hack by a Pakistani attacker. Personal information, passwords, and user IDs of over 218 million players were compromised. The breach targeted a popular Zynga puzzle game and granted the hacker access to the database of 218 million users. This incident serves as a stark reminder that no organization or individual is immune to cyberattacks, and it can happen to anyone. Even a gaming platform can be targeted, highlighting the value of user information across diverse platforms. These findings emphasize the need for vigilance and preparedness in the face of potential cyber threats, as valuable information is at stake across all sectors and platforms.

5. Unique solution for the issues/challenges

There is no one-size-fits-all method for safeguarding a wireless network, as various vulnerabilities require diverse approaches for mitigation and prevention [59]. Technology has undoubtedly brought many advantages, such as increased access to communication and knowledge, but it has also led to a surge in cyberattacks and malicious activities [60]. Protecting data from unauthorized access, theft, destruction, and other forms of cybercrime has become paramount. However, many users remain unaware of the risks they face when it comes to online security and privacy. Furthermore, there are numerous forms of cyberattacks, each with its own objectives and sources, necessitating a variety of solutions to address them.

Blockchain technology holds the potential to enhance encryption and authentication security. It can protect privacy by enabling users to use aliases to conceal their true identities [1]. While its primary application is currently in authenticating bitcoin transactions, blockchain technology can be applied to various areas, including cybersecurity. Companies are increasingly contending with ransomware attacks and data breaches daily, with even critical events like presidential elections being vulnerable to such attacks [9]. Additionally, the introduction of 5G networks is expected to significantly increase download speeds, providing more opportunities for hackers to exploit security vulnerabilities [10] and access data illegally. In addressing these challenges, blockchain can offer a superior alternative to current end-to-end encryption for securing user data. By implementing decentralized data storage, sensitive information can be protected, making it considerably more challenging for hackers to breach data storage systems. Employing this technology can substantially reduce privacy issues such as data breaches, which currently occur every 14 seconds according to the 2020 Official Annual Cybercrime Report (ACR) [9][11].

Moreover, with the increasing demand for Internet of Things (IoT) devices, hackers might gain access to smart homes via edge devices like smart switches if these IoT devices have weak security measures [10]. This can be achieved through Denial-of-Service (DoS) or Distributed Denial of Service (DDoS) attacks. Blockchain technology can be used to secure such systems by decentralizing the management of these systems or individual devices [10]. A decentralized system can help reduce DDoS attacks by decentralizing Domain Name System (DNS) entries [9][10]. Beyond DDoS attacks, patch updates may contain malicious data that grants access to all connected IoT devices. Therefore, blockchain technology can be used to verify patches, installers, and firmware updates, ensuring that IoT devices are regularly updated to prevent hackers from exploiting security flaws in the current version. Furthermore, blockchain technology can also protect data from illegal access during transmission by utilizing encryption [10].

On the other hand, raising awareness about the importance of cybersecurity should be a top priority. Educating individuals about cybersecurity, prevalent cyber threats, and how to avoid them is essential. As the saying goes, "prevention is better than cure" by Desiderius Erasmus. There are various methods to raise cybersecurity awareness. Social media, like TikTok, has been shown to influence social media users, as information and trends can spread quickly due to the large user base [12]. By utilizing social media, organizations and individuals can effectively raise awareness about cybersecurity. Moreover, employees, especially those in non-IT departments, should participate in cybersecurity workshops to learn about common tactics and strategies employed by fraudsters. This knowledge can help employees identify whether an email is legitimate or fraudulent. Additionally, according to the 2020 Official Annual Cybercrime Report, cybercrime is projected to cost the world $6 trillion by 2021 [11]. Therefore, the long-term benefits of sending employees to workshops outweigh the costs, especially in terms of potential savings from recovering after a cyberattack.

CONCLUSION

Throughout the course of our research, our team has come to the realization that privacy and security issues related to wireless networks are escalating at an alarming rate. Despite the world's continuous progress into a new era of ever-changing technology, cybersecurity remains undervalued and inadequately prioritized, when in fact, it should be at the forefront to ensure individuals' safety and protection from malicious attacks. With cybercriminals and technology both evolving rapidly, it is crucial that everyone takes responsibility for their own security before indulging in the benefits of new technologies and features. From the reports and findings we've collected in our research, it is evident that many organizations and individuals fail to recognize the significance of cybersecurity. Even as cybercriminals continue to refine their hacking techniques and strategies, we firmly believe that, by fostering a community committed to the right principles and recognizing the paramount importance of cybersecurity, we can collectively work towards achieving more secure and protected systems.

REFERENCES

1. L. Chen et al., *A Survey: Machine Learning Based Security Analytics Approaches and Applications of Blockchain in Network Security*, 1st ed. IEEE, 2020, pp. 17-21. [Accessed 14 November 2021].
2. A. Kavianpour and M. Anderson, *An Overview of Wireless Network Security*, 1st ed. IEEE, 2017, pp. 306-309. [Accessed 14 November 2021].
3. D. Da Costa and H. Yang, *Grand Challenges in Wireless Communications*, 1st ed. Frontiers in Communications and Networks, 2020, pp. 1-4. [Accessed 14 November 2021].
4. *PERCEPTIONS AND ATTITUDES OF CANADIAN ORGANIZATIONS TOWARD CYBERSECURITY*, 1st ed. The Strategic Counsel, 2021, pp. 6-62. [Accessed 14 November 2021].
5. "A Construction Company Gets Hammered by A Keylogger", *NIST*, 2020. [Online]. Available: https://www.nist.gov/system/files/documents/2020/09/30/Cybersecurity-Case-2.pdf. [Accessed 14 November 2021].
6. D. Winder, "Zoom Gets Stuffed: Here's How Hackers Got Hold Of 500,000 Passwords", *Forbes*, 2020. [Online]. Available: https://www.forbes.com/sites/daveywinder/2020/04/28/zoom- gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/?sh=8d943235cdc4. [Accessed:14- Nov- 2021].
7. A. Ioannou, I. Tussyadiah, G. Miller, S. Li, and M. Weick, "Privacy nudges for disclosure of personal information: A systematic literature review and meta-analysis," *PLOS ONE*, vol. 16, no.8, p. e0256822, Aug. 2021, doi: 10.1371/journal.pone.0256822. [Accessed 14 November 2021].
8. A. Algarni, "A Survey and Classification of Security and Privacy Research in Smart HealthcareSystems," *IEEE Access*, vol. 7, pp. 101879–101894, 2019, doi: 10.1109/access.2019.2930962. [Accessed 14 November 2021].
9. J. Legrand, "The Future Use Cases of Blockchain for Cybersecurity", Cm-alliance.com, 2020.[Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of- blockchain-for-cybersecurity. [Accessed: 14- Nov- 2021].
10. S. SINGH, "Potential Use Cases of Blockchain Technology for Cybersecurity | ITBE", IT Business Edge, 2021. [Online]. Available: https://www.itbusinessedge.com/security/potential- use-cases-of-blockchain-technology-for-cybersecurity/. [Accessed: 14- Nov- 2021].
11. "The 2020 Official Annual Cybercrime Report - Herjavec Group", Herjavec Group, 2020. [Online]. Available: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/. [Accessed: 14- Nov- 2021].

12. A. Moncur-Beer, "TikTok: the impact it has on our society | Glebe Report", Glebereport.ca, 2021. [Online]. Available: https://www.glebereport.ca/tiktok-the-impact-it-has-on-our-society/. [Accessed: 14- Nov- 2021].
13. J. Ioannidis and S. Steven, "Implementing Pushback: Router-Based Defense Against DDoS Attacks", *Network and Distributed System Security Symposium: NDSS '02*, 2021 [Accessed 17 November 2021].
14. P. Henry and Hui Luo, "WiFi: what's next?", *IEEE Communications Magazine*, vol. 40, no. 12, pp. 66-72, 2016. Available: 10.1109/mcom.2002.1106162 [Accessed 17 November 2021].
15. R. Deshmukh and K. Devadkar, "Understanding DDoS Attack & its Effect in Cloud Environment", *Procedia Computer Science*, vol. 49, pp. 202-210, 2016. Available: 10.1016/j.procs.2015.04.245 [Accessed 17 November 2021].
16. C. Zhang, "Impact of Defending Strategy Decision on DDoS Attack", *Complexity*, vol. 2021, pp. 1-11, 2021. Available: 10.1155/2021/6694383 [Accessed 17 November 2021].
17. S. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, 2018. Available: 10.1109/surv.2013.031413.00127 [Accessed 15 November 2021].
18. R. Rahim, H. Nurdiyanto, A. Saleh A, D. Abdullah, D. Hartama and D. Napitupulu, "Keylogger Applicationto Monitoring Users Activity with Exact String Matching Algorithm", *Journal of Physics: Conference Series*, vol. 954, p. 012008, 2018. Available: 10.1088/1742-6596/954/1/012008 [Accessed 17 November 2021].
19. Venkatesh R. and Sekhar R. K. User Activity Monitoring Using Keylogger Asia Journal of Information Technology 15 4758-4762. 2017. [Accessed 15 November 2021].
20. A. Sodiya, O. Folorunso, P. Komolafe and O. Ogunderu, "Preventing Authentication Systems From Keylogging Attack", Journal of Information Privacy and Security, vol. 7, no. 2, pp. 3-27, 2016. [Accessed 15 November 2021].
21. S. Shinde and U. Wanaskar, "Keylogging: A Malicious Attack", *International Journal of Advanced Researchin Computer and Communication Engineering*, vol. 5, no. 6, pp. 285-289, 2021 [Accessed 16 November 2021].
22. S. Sagiroglu and G. Canbek, "Keyloggers", *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 10- 17, 2016. Available: 10.1109/mts.2009.934159 [Accessed 17 November 2021].
23. P. Ramesh, D. Bhaskari and C. -, "A Comprehensive Analysis of Spoofing", *International Journal of Advanced Computer Science and Applications*, vol. 1, no. 6, 2016. Available: 10.14569/ijacsa.2010.010623 [Accessed 17 November 2021].
24. Lee. E, "WiFi Piggybacking – Is It Legal?", Lee & Poh Partnetship. 2019. Available:https://lpplaw.my/wifi-piggybacking-is-it-legal-2/. [Accessed 15 November 2021].
25. G. Guillot, Trespassing Through Cyberspace: Should Wireless Piggybacking Constitute a Crime or Tort Under Louisiana Law?, 69 La. L. Rev. (2009). Available: https://digitalcommons.law.lsu.edu/lalrev/vol69/iss2/6. [Accessed 15 November 2021].
26. H. Lee, J. Kim and S. Cho, "A Delay-Based Piggyback Scheme in IEEE 802.11", *2017 IEEE Wireless Communications and Networking Conference*, 2017. Available: 10.1109/wcnc.2007.87 [Accessed 17 November 2021].
27. S. Kaul, R. Yates and M. Gruteser, "On Piggybacking in Vehicular Networks", *2011 IEEE Global Telecommunications Conference - GLOBECOM 2016*, 2016. Available: 10.1109/glocom.2011.6134181 [Accessed 15 November 2021].
28. N. Chandler and W. Fenlon, "How to Detect if Someone's Stealing Your WiFi" (2017). HowStuffWorks.com. Available: https://electronics.howstuffworks.com/how-to-tech/how-to- detect-stealing-wifi.htm. [Accessed 15 November 2021].
29. P. Sapiezynski, R. Gatej, A. Mislove, and S. Lehmann. Opportunities and Challenges in Crowdsourced Wardriving. CCS.NEU.edu, 2016 [Accessed 15 November 2021].
30. R. Jang, J. Kang, A. Mohaisen and D. Nyang, "Catch Me If You Can: Rogue Access Point Detection Using Intentional Channel Interference", *IEEE Transactions on Mobile Computing*, vol. 19, no. 5, pp. 1056-1071, 2020. Available: 10.1109/tmc.2019.2903052 [Accessed 17 November 2021].
31. Y. Song, C. Yang and G. Gu, "Who is peeping at your passwords at Starbucks?; To catch an evil twin access point", *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, 2010. Available: 10.1109/dsn.2010.5544302 [Accessed 15 November 2021].
32. R. Beyah and A. Venkataraman, "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions", *IEEE Security & Privacy Magazine*, vol. 9, no. 5, pp. 56-61, 2016. Available: 10.1109/msp.2011.75. [Accessed 15 November 2021].
33. C. Wang, B. Yang and J. Luo, "Identity Theft Detection in Mobile Social Networks Using Behavioral Semantics", *IEEE International Conference on Smart Computing (SMARTCOMP)*, 2017. Available: 10.1109/smartcomp.2017.7947016 [Accessed 14 November 2021].

34. D. Vivek and V. Persis, "Discovering Identity Theft (Spoofing) Using the Spatial Correlation of Received Signal Strength in Wireless Networks", *International Journal and Magazine of Engineering, Technology, Management & Research*, vol. 3, no. 6, pp. 527-532, 2016. [Accessed13 November 2021].
35. R. Labong, "Identity Theft Protection Strategies: A Literature Review", *Journal of Academic Research*, vol. 4, no. 2, pp. 1-12, 2019. [Accessed 14 November 2021].
36. L. Liu, Y. Wang and Y. Zhou, "Understanding Data Breach: A Visualization Aspect", *LectureNotes in Computer Science*, pp. 884-890, 2018. Available: 10.1007/978-3-319-94268-1_81[Accessed 14 November 2021].
37. R. Kamurthi, S. Chopra and R. Sharma, "Confrontation- Wi-Fi Risks and Data Breach", *International Conference on Emerging Smart Computing and Informatics (ESCI)*, pp. 633-638, 2021. Available: 10.1109/esci50559.2021.939704 [Accessed 14 November 2021].
38. Y. Zou, S. Danino, K. Sun and F. Schaub, "You 'Might' Be Affected: An Empirical Analysis ofReadability and Usability Issues in Data Breach Notifications", *CHI Conference on HumanFactors in Computing Systems*, vol. 194, pp. 1-14, 2019. Available: 10.1145/3290605.3300424 [Accessed 14 November 2021].
39. S. Bendale and J. Prasad, "Security Threats and Challenges in Future Mobile Wireless Networks", *Global Conference on Wireless Computing and Networking (GCWCN)*, pp. 146-150, 2018. Available: 10.1109/gcwcn.2018.8668635 [Accessed 13 November 2021].
40. H. Dai, H. Wang, H. Xiao, X. Li and Q. Wang, "On Eavesdropping Attacks in Wireless Networks", *IEEE International Conference on Computational Science and Engineering*, pp. 138-141, 2016. Available: 10.1109/cse-euc-dcabes.2016.173 [Accessed 13 November 2021].
41. X. Li, H. Dai, Q. Wang and A. Vasilakos, "AE-Shelter: An Novel Anti-Eavesdropping Schemein Wireless Networks", *IEEE International Conference on Communications (ICC)*, 2017. Available: 10.1109/icc.2017.7996847 [Accessed 14 November 2021].
42. [42]I. Vayansky and S. Kumar, "Phishing – challenges and solutions", *Computer Fraud & Security*,vol. 2018, no. 1, pp. 15-20, 2018. Available: 10.1016/s1361-3723(18)30007-1 [Accessed 13 November 2021].
43. H. Musthyala and N. Reddy, "Hacking wireless network credentials by performing phishing attack using Python Scripting", *5th International Conference on Intelligent Computing and ControlSystems (ICICCS)*, pp. 248-253, 2021. Available: 10.1109/iciccs51141.2021.9432 [Accessed 13November 2021].
44. M. Baykara and Z. Gürel, "Detection of phishing attacks", *6th International Symposium on Digital Forensic and Security (ISDFS)*, 2018. Available: 10.1109/isdfs.2018.8355389 [Accessed 14 November 2021].
45. A. El Aassal, S. Baki, A. Das and R. Verma, "An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs", *IEEE Access*, vol. 8, pp. 22170-22192, 2020. Available: 10.1109/access.2020.2969780 [Accessed 14 November 2021].
46. A. Muntode and S. Parwe, "An Overview on Phishing- its types and Countermeasures", *International Journal of Engineering Research and*, vol. 8, no. 12, pp. 545- 548, 2019. Available: 10.17577/ijertv8is120260 [Accessed 13 November 2021].
47. A. Sadiq et al., "A review of phishing attacks and countermeasures for internet of things- based smart business applications in industry 4.0", *Human Behavior and Emerging Technologies*,pp. 1-11, 2021. Available: 10.1002/hbe2.301 [Accessed 14 November 2021].
48. A. Andryukhin, "Phishing Attacks and Preventions in Blockchain Based Projects", *International Conference on Engineering Technologies and Computer Science (EnT)*, pp. 15-19, 2019. Available: 10.1109/ent.2019.00008 [Accessed 14 November 2021].
49. A. Hassan *et al.*, "A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency," *Journal of Cyber Security*, vol. 2, no. 1, pp. 1–17, 2020 [Accessed 16 November 2021].
50. B. Liao, Y. Ali, S. Nazir, L. He and H. Khan, "Security Analysis of IoT Devices by Using MobileComputing: A Systematic Literature Review", *IEEE Access*, vol. 8, pp. 120331-120350, 2020. Available: 10.1109/access.2020.3006358 [Accessed 17 November 2021].
51. Q. JIANG and L. HOU, "Research on the Influence of Science and Technology Advancementand Social Progress on the Ideological and Political Education Work in Colleges and Universities", *4th International Conference on Humanities Science and Society Development*, vol.328, pp. 87-90, 2019. [Accessed 17 November 2021].
52. A. Burg, A. Chattopadhyay and K. Lam, "Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things", *Proceedings of the IEEE*, vol. 106, no. 1, pp. 38-60, 2018. Available: 10.1109/jproc.2017.2780172 [Accessed 17 November 2021].
53. S. Kabanda, M. Tanner and C. Kent, "Exploring SME cybersecurity practices in developing countries", *Journal of Organizational Computing and Electronic Commerce*, vol. 28, no. 3, pp. 269-282, 2018. Available: 10.1080/10919392.2018.1484598 [Accessed 17 November 2021].
54. R. Rahim, H. Nurdiyanto, A. Saleh A, D. Abdullah, D. Hartama and D. Napitupulu, "KeyloggerApplication to Monitoring Users Activity with Exact String Matching Algorithm", *Journal of Physics:Conference Series*, vol. 954, p. 012008, 2018. Available: 10.1088/1742-6596/954/1/012008[Accessed 17 November 2021].

55. M. Ilayaraja, K. Shankar and G. Devika, "A Modified Symmetric Key Cryptography Method for Secure Data Transmission", *International Journal of Pure and Applied Mathematics*, vol. 116,no. 10, pp. 301-308, 2017. [Accessed 17 November 2021].
56. B. Pranggono and A. Arabo, "COVID -19 pandemic cybersecurity issues", *Internet Technology Letters*, vol. 4, no. 2, 2020. Available: 10.1002/itl2.247 [Accessed 17 November 2021].
57. C. Townsley, "Are businesses getting complacent when it comes to DDoS mitigation?", *Network Security*, vol. 2018, no. 6, pp. 6-9, 2018. Available: 10.1016/s1353- 4858(18)30054-0 [Accessed 17 November 2021].
58. K. Okereafor and P. Manny, "UNDERSTANDING CYBERSECURITY CHALLENGES OF TELECOMMUTING AND VIDEO CONFERENCING APPLICATIONS IN THE COVID-19 PANDEMIC", *International Journal in IT & Engineering (IJITE)*, vol. 8, no. 6, pp. 13-23, 2020 [Accessed 17 November 2021].
59. B. Bhushan and G. Sahoo, "Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks", *Wireless Personal Communications*, vol. 98, no. 2, pp. 2037-2077, 2017. Available: 10.1007/s11277-017-4962-0 [Accessed 17 November 2021].
60. L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems", *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16-32, 2020. Available: 10.1109/jiot.2019.2948888 [Accessed 17 November 2021].
61. Atzeni, D., Bacciu, D., Mazzei, D., & Prencipe, G. (2022). A Systematic Review of Wi-Fi and Machine Learning Integration with Topic Modeling Techniques. Sensors, 22(13), 4925. https://doi.org/10.3390/s22134925 [Accessed 11 October 11, 2023]
62. T. S. Rappaport et al., "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond," in IEEE Access, vol. 7, pp. 78729-78757, 2019, doi: 10.1109/ACCESS.2019.2921522.
63. LaBrie, G. (2017). *6 Benefits of Wireless Networking + Wireless Networking Solutions*. Wei.com. https://blog.wei.com/6-benefits-of-wireless-networking-wireless-networking-solutions
64. Rathod, T., Jadav, N. K., Alshehri, M. D., Tanwar, S., Sharma, R., Felseghi, R. A., & Raboaca, M. S. (2022). Blockchain for Future Wireless Networks: A Decade Survey. Sensors, 22(11), 4182. https://doi.org/10.3390/s22114182
65. S. Muzafar, N. Z. Jhanjhi, N. A. Khan, and F. Ashfaq, “DDOS attack detection approaches in on software defined network,” *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, Nov. 2022, doi: 10.1109/macs56771.2022.10022653.
66. S. Muzafar and N. Z. Jhanjhi, “DDoS attacks on software defined Network: Challenges and issues,” *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, Feb. 2022, doi: 10.1109/icbats54253.2022.9780662.
67. R. Gopi *et al.*, “Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things,” *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 26739–26757, Feb. 2021, doi: 10.1007/s11042-021-10640-6.
68. S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain, and M. Humayun, “Performance Enhancement in Wireless Body Area Networks with Secure Communication,” *Wireless Personal Communications*, vol. 116, no. 1, pp. 1–22, Aug. 2020, doi: 10.1007/s11277-020-07702-7.
69. K. N. Kumar, S. Verma, Kavita, N. Z. Jhanjhi, and M. Talib, “A Survey of The Design and Security Mechanisms of The Wireless Networks and Mobile Ad-Hoc Networks,” *IOP Conference Series*, vol. 993, p. 012063, Dec. 2020, doi: 10.1088/1757-899x/993/1/012063.
70. V. Ponnusamy, L. T. Jung, T. Ramachandran, and N. Z. Jhanjhi, “Bio-inspired energy scavenging in wireless ad hoc network,” *2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT)*, Apr. 2017, doi: 10.1109/icieect.2017.7916600.
71. V. Ponnusamy, N. Z. Jhanjhi, T. J. Low, and A. H. M. Amin, *Biologically-Inspired Energy Harvesting through Wireless Sensor Technologies*. 2016. doi: 10.4018/978-1-4666-9792-8.
72. N. Z. Jhanjhi, L. T. Jung, and V. Ponnusamy, “Application of Self-Healing in wireless sensor network,” in *Advances in environmental engineering and green technologies book series*, 2016, pp. 217–233. doi: 10.4018/978-1-4666-9792-8.ch011.
73. N. Z. Jhanjhi, T. J. Low, and T. A. Alghamdi, “Enhancing routing energy efficiency of Wireless Sensor Networks,” *ICACT Transactions on Advanced Communications Technology*, Jul. 2015, doi: 10.1109/icact.2015.7224928.
74. T. Jabeen, I. Jabeen, H. Ashraf, N. Z. Jhanjhi, A. Yassine, and M. S. Hossain, “An intelligent healthcare system using IoT in wireless sensor network,” *Sensors*, vol. 23, no. 11, p. 5055, May 2023, doi: 10.3390/s23115055.
75. S. K. Chaurasiya, A. Biswas, A. Nayyar, N. Z. Jhanjhi, and R. Banerjee, “DEICA: A differential evolution-based improved clustering algorithm for IoT-based heterogeneous wireless sensor networks,” *International Journal of Communication Systems*, vol. 36, no. 5, Jan. 2023, doi: 10.1002/dac.5420.

76. H. Ashraf, F. Khan, U. Ihsan, F. Al-Quayed, N. Z. Jhanjhi, and M. Humayun, “MABPD: Mobile Agent-Based Prevention and Black Hole Attack Detection in Wireless Sensor Networks,” *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, Mar. 2023, doi: 10.1109/icbats57792.2023.10111277.
77. M. U. Hanif *et al.*, “AI-Based wormhole attack detection techniques in wireless sensor networks,” *Electronics*, vol. 11, no. 15, p. 2324, Jul. 2022, doi: 10.3390/electronics11152324.
78. Q. W. Ahmed *et al.*, “AI-Based Resource Allocation Techniques in Wireless Sensor Internet of Things Networks in Energy Efficiency with Data Optimization,” *Electronics*, vol. 11, no. 13, p. 2071, Jul. 2022, doi: 10.3390/electronics11132071.
79. L. Dash *et al.*, “A Data Aggregation Approach Exploiting Spatial and Temporal Correlation among Sensor Data in Wireless Sensor Networks,” *Electronics*, vol. 11, no. 7, p. 989, Mar. 2022, doi: 10.3390/electronics11070989.
80. M. S. Dawood, N. Z. Jhanjhi, A. R. Khan, and M. Salih, “Designing of energy efficient routing protocol for Wireless Sensor Network (WSN) Using Location Aware (LA) Algorithm,” *Journal of Information & Communication Technology JICT*, vol. 3, no. 2, p. 15, Jan. 2009, [Online]. Available: http://jms.ilmauniversity.edu.pk/index.php/JICT/article/view/583
81. V. Ponnusamy, Y. Aun, N. Z. Jhanjhi, M. Humayun, and M. F. Almufareh, “IoT wireless intrusion detection and network Traffic Analysis,” *Computer Systems Science and Engineering*, vol. 40, no. 3, pp. 865–879, Jan. 2022, doi: 10.32604/csse.2022.018801.
82. A. A. Teoh, N. B. A. Ghani, M. Ahmad, N. Z. Jhanjhi, M. A. AlZain, and M. Masud, “Organizational data breach: Building conscious care behavior in incident response,” *Computer Systems Science and Engineering*, vol. 40, no. 2, pp. 505–515, Jan. 2022, doi: 10.32604/csse.2022.018468.
83. A. A. Ubing, S. K. B. Jasmi, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, “Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, Jan. 2019, doi: 10.14569/ijacsa.2019.0100133.
84. İ. Ali, N. Z. Jhanjhi, and A. Laraib, “Cybersecurity and blockchain usage in contemporary business,” in *Advances in information security, privacy, and ethics book series*, 2022, pp. 49–64. doi: 10.4018/978-1-6684-5284-4.ch003.
85. A. Khan, N. Z. Jhanjhi, and M. Humayun, “The role of cybersecurity in smart cities,” in *Chapman and Hall/CRC eBooks*, 2022, pp. 195–208. doi: 10.1201/9781003203087-9.
86. M. Humayun, N. Z. Jhanjhi, M. Talib, M. H. Shah, and G. Suseendran, “Cybersecurity for data science: issues, opportunities, and challenges,” in *Lecture notes in networks and systems*, 2021, pp. 435–444. doi: 10.1007/978-981-16-3153-5_46.
87. Adeyemo Victor Elijah, Azween Abdullah, NZ JhanJhi, Mahadevan Supramaniam and Balogun Abdullateef O, “Ensemble and Deep-Learning Methods for Two-Class and Multi-Attack Anomaly Intrusion Detection: An Empirical Study” International Journal of Advanced Computer Science and Applications (IJACSA), 10(9), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100969
88. K. Hussain, S. J. Hussain, N. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-4, doi: 10.1109/ICCISci.2019.8716416.
89. Gaur, L., Singh, G., Solanki, A., Jhanjhi, N. Z., Bhatia, U., Sharma, S., ... & Kim, W. (2021). Disposition of youth in predicting sustainable development goals using the neuro-fuzzy and random forest algorithms. Human-Centric Computing and Information Sciences, 11, NA.
90. Kumar, T., Pandey, B., Mussavi, S. H. A., & Zaman, N. (2015). CTHS based energy efficient thermal aware image ALU design on FPGA. Wireless Personal Communications, 85, 671-696.
91. Lim, M., Abdullah, A., & Jhanjhi, N. Z. (2021). Performance optimization of criminal network hidden link prediction model with deep reinforcement learning. Journal of King Saud University-Computer and Information Sciences, 33(10), 1202-1210.
92. Gaur, L., Afaq, A., Solanki, A., Singh, G., Sharma, S., Jhanjhi, N. Z., ... & Le, D. N. (2021). Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels. Computers and Electrical Engineering, 95, 107374.
93. Gouda, W., Sama, N. U., Al-Waakid, G., Humayun, M., & Jhanjhi, N. Z. (2022, June). Detection of skin cancer based on skin lesion images using deep learning. In Healthcare (Vol. 10, No. 7, p. 1183). MDPI.
94. Nanglia, S., Ahmad, M., Khan, F. A., & Jhanjhi, N. Z. (2022). An enhanced Predictive heterogeneous ensemble model for breast cancer prediction. Biomedical Signal Processing and Control, 72, 103279.
95. Diwaker, C., Tomar, P., Solanki, A., Nayyar, A., Jhanjhi, N. Z., Abdullah, A., & Supramaniam, M. (2019). A new model for predicting component-based software reliability using soft computing. IEEE Access, 7, 147191-147203.

96. Hussain, S. J., Ahmed, U., Liaquat, H., Mir, S., Jhanjhi, N. Z., & Humayun, M. (2019, April). IMIAD: intelligent malware identification for android platform. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
97. Kok, S. H., Azween, A., & Jhanjhi, N. Z. (2020). Evaluation metric for crypto-ransomware detection using machine learning. Journal of Information Security and Applications, 55, 102646.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.