**International Journal of Cybersecurity Engineering and Innovation**

ARTICLE INFO

**Article History:** Received: 24-03-2024, Revised: 20-05-2024, Accepted: 22-05-2024, Published: 25-05-2024
**Corresponding author Email:** m.almaiah@ju.edu.jo
**DOI:**




**Vol. 2024 No.1**

# Cyber Security Threats in Wireless LAN: A Literature Review

Mashael Saad Alghareeb[1], Mohammed Almaiah[1], Youakim Badr[2]

[1] *College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

[2] *Computer Science and Engineering Department, The Pennsylvania State University, Malvern, PA, United States, USA*

## Abstract

Wireless LANs have been widely deployed in places such as business organizations, government agencies, hospitals, schools, and even the home environment. Mobility, flexibility, scalability, cost-effectiveness, and rapid deployment are some of the factors driving the spread of this technology. However, due to their nature wireless LANs are vulnerable to several types of attacks. Therefore, this research aims to discuss common threats related to the wireless LAN system, and a comprehensive review of existing studies regarding cybersecurity threats in Wireless LAN. A systematic literature review (SLR) was conducted to identify potential threats and identify appropriate countermeasures for each wireless WLA.

**Keywords:** Wireless LANs, IEE 802.11, Attacks, Security, Access Point (AP), threat, Availability, Authentication, Integrity, Access control, Wireless Countermeasure.

## 1. Introduction

Today, a wireless local area network (WLAN) is an option to reckon with in various sectors, including business, education, government, the public, and individuals. Wireless networks offer many advantages that improve productivity due to increased access to information resources. In fact, network configuration and reconfiguration are easier, faster, and less expensive. However, wireless technology also creates new threats if the message is not encrypted, and an attacker can read it thus compromising confidentiality. Although wireless networks are changing the risks associated with various security threats, the general security objectives remain the same with wired networks: maintaining confidentiality, ensuring integrity, and maintaining the availability of information and information systems (Sathyavani & Selvi, 2014). In order for an organization to best protect its information, there is a need for a security risk assessment. This paper discusses the vulnerabilities and describes the major known attacks/threats to the home and enterprise wireless LAN system. Then a brief overview of WLANs and a comprehensive review of current studies related to wireless LAN cybersecurity threats and vulnerabilities. General guidelines and recommendations for users to protect wireless LANs will also be provided.

### *1.1 Background*

Indeed, wireless networks are at the forefront of modern technologies and are rapidly spreading everywhere. As a result, a growing interest in potential security issues has emerged. In addition, wireless LAN (WLAN) is currently known for its low cost and ease of deployment. In 1997, the Institute of Electrical and Electronics Engineers (IEEE) created the first

WLAN standard. This standard is called IEEE 802.11 (Beard and W. Stallings, 2016). The IEEE 802.11 standard dominates wireless networking technology. This can be attributed to the low cost of hardware and high data rates that support current applications (1 to 54 Mbps) as well as promising future extensions (possibly exceeding 100 Mbps with 802.11n). There has been a lot of work related to WLAN security since then, discovered that the 802.11 security architecture is weak (Sunday, 2008). However, most of these works were helping to improve the security mechanism. Therefore, this project aims to identify the most common types of cyber security attacks and vulnerabilities in the WLAN. In addition, to identify the most critical appropriate cyber security techniques used in the WLAN mitigation process. Consequently, will be determined suitable countermeasures for each attack in the WLAN. Also, to identify the most critical recent technologies that were used in future works in the LAN environment. Users will also be provided with general guidelines and recommendations for protecting wireless LANs.

### *1.2 Motivation*

Wireless LANs have gained much more popularity than wired networks due to their flexibility, cost-effectiveness, and ease of installation. However, the increasing deployment of WLANs presents the hacker with more opportunities. Thus, anyone with the right tools can pick up and transmit wireless signals if they are within range (Suroto, 2018a). Therefore, the vulnerabilities and security threats posed by the open nature of wireless communications must be known.

### *1.3 Problem Statement*

Information is a valuable asset of the organization and therefore needs to be protected from threats, to give confidence that the business can continue to operate continuously. Despite major advancements in wireless technology in recent decades, most wireless networks remain vulnerable to radio jamming assaults due to the open nature of wireless channels, and progress in the design of jamming-resistant wireless networking systems remains restricted (Pirayesh & Zeng, 2021). These attacks aim to break the confidentiality, integrity of information and network availability (Suroto, 2018a). It is therefore important to identify the threats, vulnerabilities, and security risks associated with deploying a WLAN in an enterprise environment. The scope of this project mainly focuses on the threats and vulnerabilities related to WLAN. This paper will discuss the latest threats, vulnerabilities and security risks associated with deploying WLAN in an enterprise environment. The paper will guide wireless LAN users on how to use it safely and protect their organizations from attacks to avoid financial losses. This research aims to achieve the following objectives:

- Identify the most common types of cyber security attacks.
- Identify the most important cybersecurity techniques used in the WLAN mitigation processor or countermeasures.
- Learn about the recent technologies that have been used in future work in the LAN environment

## 2. Research Methodology

The approach taken in this paper is deductive (a systematic literature review methodology), because it looks at the bigger picture (WLAN) and narrows it down to security (threats and countermeasures). In the first stage, the following search string was used to find the paper related to the topic of this paper: Types of Threats and Mitigation Techniques). The search was conducted in Google Scholar and the Saudi Digital Library using the following criteria: an academic journal or a conference paper representing threats WLAN. Publications between 2016 and 2022. Figure 4 shows the distribution of the selected studies by year between the years (2016-2021).

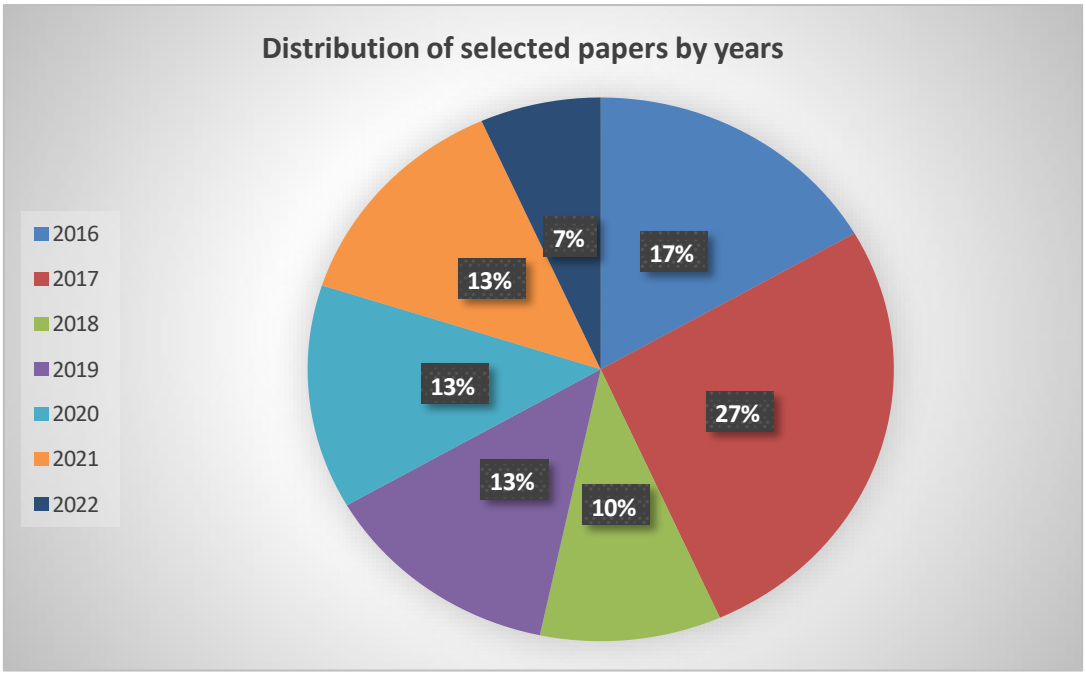


**Figure 1.** Distribution of selected papers by years

## 3. Literature Reviews

### *3.1 Overview of WLAN*

Traditional WLAN components include Access Points (APs), Network interface cards (NICs), client switches, bridges, repeaters, and antennas. In addition, the Authentication, Authorization, and Accounting (AAA) server (specifically the Remote Address Dial-Up User Service [RADIUS] server), Network Management Server (NMS), and "aware wireless" switches and routers are also part of the enterprise WLAN (G. Singh, 2017).

Figure1 shows the components of 802.11 Wireless LAN: Stations, Wireless APS, Ports.

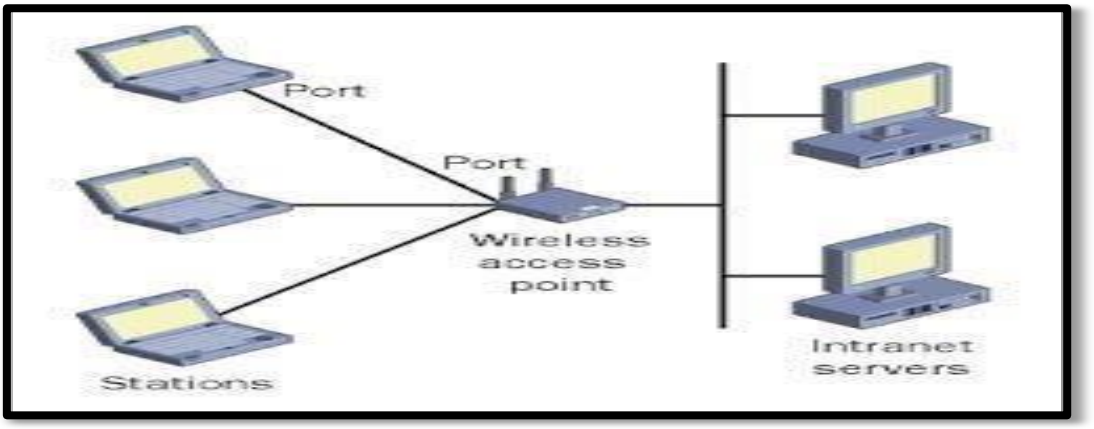


**Figure 2.** Wireless components

*3.1.1 Access Points (APs):*

An access point has a radio card that communicates with individual wireless LAN user devices, as well as a connected network interface card (NIC) that connects to a distribution system such as Ethernet (G. Singh, 2017). Figure 2 below shows the access points (APs).

**Figure 3.** Access Points (AP)

*3.1.2 Network interface cards (NICs):*

A wireless LAN relies on a network interface card (NIC), which runs on the computer device and provides wireless connectivity. A wireless LAN NIC, often known as a radio card, is frequently used to implement the 802.11 standards (G. Singh, 2017). Figure 3 below shows the network interface card (NIC).

**Figure 4.** Network Interface Card (NIC)

*3.2 Related Work*

There has been a lot of researches done in exploring threats, attacks and various steps to overcome them.

For example, (Suroto, 2018), aimed to study the various weaknesses and attacks on the WLAN network and their solutions, in addition to studying some of the current security methods used to secure the WLAN network and exploring the possibility of making improvements to it. The results show that WLAN security is not easy, and it is constantly changing. Based on the results, all companies need to define their own security requirements based on the application that uses the WLAN, for the WLAN to be as protected as a wired LAN.

Baray & Ojha (2021), they describe how new wireless LAN encryption standards such as WEP, WPA/WPA2 and WPA3 are vulnerable to attack. They introduced many security models vulnerabilities such as Wi-Fi security hacking by Aircrack-ng, previous security model vulnerabilities and also performing Aircrack-ng attack on Wi-Fi modems or routers. Moreover, it provides a way for hackers to get Wi-Fi passwords even of the new specific model like WPA3 using old technologies.

However, the new model introduced for the Wi- Fi WPA3 security protocol is also no longer a secure model that can be hacked. In order to crack WPA/WPA2, kali Linux operating system will be required along with Aircrackng packages installed on any compatible PC. Based on this, researchers have discovered some new security vulnerabilities that enable hackers to take out Wi-Fi passwords.

Vanhoef et al., (2017), they developed a new model-based testing technology to analyze Wi-Fi handshake applications. Application-specific vulnerabilities were discovered as well as more general types of vulnerabilities found on different devices. This causes many applications to accept MIC failure reports, even though the network does not use WPA- TKIP. Based on this, this can be exploited as a DoS attack to take down a network that only allows the use of AES-CCMP. The results showed that serious implementation vulnerabilities were discovered. For example, running WPA-TKIP countermeasures against OpenBSD or Windows 10 causes the network to become unavailable forever. Subsequently, to recover from a targeted DoS attack against Windows 7, you must restart the access point. Kavianpour & Anderson, (2017) they discuss to need to identify key elements related to network security and provide an overview of potential vulnerabilities to threats and countermeasures associated with technology designed for IEEE 802.11 Wireless LAN Standard. In addition, basic security requirements are discussed, and access control principles are included to address future trends in wireless security to reduce vulnerabilities and prevent the most common threats. Information security, according to the CIA triad, should adhere to three fundamental principles: confidentiality, integrity, and availability. To achieve complete security, all three notions are required to some extent. The network will be vulnerable to attack if this does not happen. Access control and authentication are two more principals that are involved (Sejdić et al., 2011).

### *3.2.1 Confidentiality Attacks*

Confidentiality is the prevention of data disclosure, both intentionally and unintentionally. For example, (Bhushan et al., 2017), this study provided a comprehensive review of MITM to classify and analyze the scope of MITM attacks. The OSI reference model and two basic network technologies such as GSM and UMTS were used. MITM attacks are categorized based on various criteria such as the location of the attacker, impersonation techniques, and the nature of the channel. Accordingly, the existing countermeasures were cleared. As a result, the paper classified MITM attacks into four categories which are MITM-based spoofing, TLS/SSL MITM, BGP MIT M, and faulty base station-based MITM attack. Finally, it provided the prevention mechanisms for all these attacks and also identified some future research directions.

For instance, (Rahim, 2017) the study aimed to discuss one of the wireless network breaches, a man-in-the-middle attack. In addition to presenting some of the weaknesses that led to it and how to discover it. Also, to how to protect ourselves from this attack and avoid it. Also, (Amin & Mahamud, 2019) the aim of the study was that the authors proposed a method for preventing MITM attacks using a Linux bash script at the client end. Due to different types of tools and techniques to penetrate the physical and wireless network. A new mechanism is proposed that does not depend on encryption and it is called MR-ARP, the main working process is to use the concept of voting system. As a result, for MR-ARP which uses the concept of a voting system to give an accurate result, it may take longer to determine the safe path.

For example, (Tian et al., 2021) The study aimed to suggested an Evil Twin Attack detection method that first captures the Wi-Fi signal, and then extracts the short training sequence and the long training sequence as a feature for each Wi-Fi hotspot. Based on this, a convolutional neural network (CNN) was trained to verify the identity of each hotspot. The experimental results showed that the proposed method can identify the hot spot with prior knowledge and effectively detect the Evil Twin attack. Based on the results, the limitation of the method is that it takes advantage of hardware features and channels feature for device recognition, which theoretically makes it only applicable in identifying statically deployed hotspots. Also, the effect of noise on performance is not evaluated due to the lack of a controlled test environment. In addition, (Nakhila, 2018) the study aimed to explore the current security threats to WLAN networks and the corresponding defense solutions. WLAN vulnerabilities have been divided into two sides, client and administrator. Client-side vulnerability investigation relies on Evil Twin Attack (ETA) scanning while Administrator-side research targets Wi- Fi Protected Access II (WPA2). Accordingly, three new technologies for detecting ETA were introduced. Detection methods are based on (1) establishing a secure connection to a remote server to detect the change of the gateway's public IP address by switching from one access point (AP) to another. (2) Monitoring multiple Wi-Fi channels in random order for specific data packets sent by the remote server. (3) Combine the previous solutions into a single universal method for ETA detection using Virtual Wireless Network Clients (VWCs). On the other hand, a new vulnerability has been introduced that allows the attacker to force the victim's smartphone to consume data over the cellular network by initiating data download on the victim's cell phone without the victim's permission. As a result, a new scheme has been developed to speed up the severity

of an active dictionary attack on WPA2 based on two new ideas. First, the system connects several VWCs to the AP at the same time - each VWC has its own spoofed MAC address. Second, each of the VWCs can try multiple passphrases with a single wireless session. Moreover, a new technology has been introduced to avoid bandwidth limitations imposed by Wi-Fi hotspots. It showed that the proposed method creates multiple VWCs to access the WLAN.

However, combining the individual bandwidth of each VWC increases the total bandwidth that the attacker gains. The results showed that all proposal techniques were implemented and evaluated in realistic scenarios. Also, (Abare & Garba, 2019) in this work we proposed an improved model for preventing a KRACK attack, the proposed model includes encrypting the entire handshake messages and the generated Nonce values. Next, an alpha check (a type of logical switch) was proposed which switches from 1 to 0 when the PTK is first installed. The results showed proof of the efficiency of the proposed model, as the results obtained from the comparison between the two models were measured in terms of the average execution time in seconds, and they show how the performance of the proposed model was better. Based on the results, this proposed model will help enhance security in the four-way handshake authentication process against pairwise transient key reinstallations. For instances, (Ahadi et al., 2022) the study aimed to suggest different techniques for detecting the evil twin attack. However, Evil Twin is a kind of adversary that impersonates a legitimate access point (LAP) because it can happen by spoofing the name (SSID) and MAC address (BSSID) of a legitimate access point (LAP). This attack can cause various threats such as MITM, outage, and access point ban. A new technology has been proposed based on two fingerprints from Access Point, Received Signal Strength Index (RSSI) and number of hops, which are difficult to copy by the opponent. The technology is implemented in a system called "ETDetector", which can detect and prevent the attack.

*3.2.2 Integrity Attacks*

Integrity is the ability to govern the purposeful and unintended alteration of data. For examples, (Kim et al., 2019) The study aimed to propose a covert jamming attack scheme using fake ACK frame injection that interferes with and deceives transmitters in IEEE 802.11 WLAN. The scheme immobilizes the proposed obfuscation attack retransmission mechanism for the victims' MAC and transport layers. Accordingly, to prevent fake injection of an ACK frame in IEEE 802.11 WLANs, ACK frames must also be encrypted to ensure acknowledgment integrity.

3.2.3 Availability Attacks

Availability is the ability to control the availability of system resources to authorized users/systems/processes on demand. For instance, (Lounis & Zulkernine, 2020) study aimed to present three attacks on Wi-Fi availability. These attacks can violate the authentication, confidentiality, and integrity of Wi-Fi networks. In terms of the impact of the attack, attacks on availability have a greater impact. However, these attacks cause a denial of service on Wi-Fi users by preventing them from connecting to a legitimate network. The evil twin scheme and race state-based vulnerability exploitation were used to generate the attacks. The results showed that countermeasures were proposed to fix the exploited vulnerability and mitigate the attacks. For instance, (Pirayesh & Zeng, 2021) the study presented current jamming attacks and anti-jamming strategies in wireless local area networks (WLANs), cellular networks, radio- cognitive networks (CRNs), ZigBee networks, Bluetooth networks, vehicle networks, LoRa networks, RFID networks, and GPS. Thus, to achieve the goal of a comprehensive knowledge landscape of current jamming/anti-jamming strategies and stimulate more research efforts to secure wireless networks against jamming attacks. Accordingly, an insight into the design of jamming resilient wireless networking systems and an overview of anti-jamming techniques is presented.

Also, (Santoro et al., 2017) the study aimed to address the problem of identifying virtual jamming attacks on IEEE 802.11 networks. A number of Network Intrusion Detection Systems (NIDSs) have been presented in the literature to detect this type of attack. In addition, new hybrid NIDS is proposed based on DS theory that is able to efficiently detect NAV attacks. Accordingly, the solution has been experimentally evaluated using multiple scenarios in an IEEE 802.11 network. In. addition, (Brar, n.d.) The study aimed to provide a solution to the jamming attack over the wireless network. An internal threat model is considered, where the jammer is part of the network and is familiar with the network's secrets and protocol specifications. Jammer can perform the classification in real time by decoding the first few bytes of the transmitted packet. In addition, to prevent packet classification in real time, various schemes have been developed. However, these schemes combine coding basics such as the strong hiding commitment scheme and physical layer properties so as to turn the jammer into a random system. Also, a measurement was made of how each jammer performed by its effect on packet transmission rate and packet delivery rate. With the aim of analyzing the security of the method and determining the amount of computational and communication expenses. The results show that intrusion detection and intrusion prevention systems still need to be improved to ensure consistent network security. Also, they are not reliable enough (especially regarding

false positives and false negatives) and are difficult to manage. However, it is clear that these systems are now necessary for companies to ensure their security. For example, (Dalal et al., 2022), the study aimed to first describe the attacks on WPA3 networks that were reported in previous work. In addition, they show that the DE authentication attack and beacon flood attack, which are known to be possible on a WPA2 network, are still possible with WPA3. All eight attacks were launched and tested using a test containing an Enterprise Access Point (AP) and Intrusion Detection System (IDS). Experimental results show that AP is vulnerable to eight out of nine attacks and that IDS is unable to detect any of them. Based on the results, a signature-based identifier design was proposed, which incorporates techniques to detect all attacks. Also, these techniques were applied in the testing and it was verified that the proprietary IDS system is able to successfully detect all attacks. In addition, schemes have been introduced to mitigate the impact of attacks as soon as they are discovered. The code to carry out the attacks as well as the private IDS system was made publicly available, so that it could be used for future work by the research community as a whole. Also, (Seth et al., 2019) the main objective of the study was to focus on DoS DE authentication attack in Wi-Fi networks. Therefore, the victim's station is disconnected from the network due to a DoS DE authentication attack, since the minimum number of resources required to initiate a DE authentication attack. As a result, the schemes for de- authenticating DoS attack detection have major flaws, they require protocol modification, require firmware upgrade, no proof of validity etc. Based on this, it has been suggested that a de-authentication attack be detected. Also, (Siahaan, 2016) in this study, penetration testing was conducted, which is one of the common methods of password cracking, and it is the best way to measure the level of security. This tool is not intended to hide confidential information. Accordingly, it helps people to increase the security of the existing gap by using penetration testing. However, they do not realize that the name they are joining is a fake SSID. As a result, attackers use this moment to get the password. Then, shortly after they attempted to connect multiple times, the attacker had already registered the SSID password.

*3.2.4 Access control Attacks*

Access control is the control of a legitimate user's access to resources. For example, (Dahiya & Gill, 2017) The study aimed to propose the automatic detection of rogue access point, which depends on the Hopfield Neural Network algorithm. The reason for this, the main attack on any organization is the attack of Man in the Middle which is difficult to manage. This attack leads to a number of unauthorized access points and rogue access points that are not easily detected. Native hardware passwords are stored in matrix weight and pattern matching format at login time. The results of the simulation experiment showed that this method is more secure than the traditional method in WLAN. Also, Umesh, A. S. B. D. A. S. (2017) The aim of the study is to suggest the importance of access points, but a Rogue access point can damage the entire network which is harmful. Also, simple prevention techniques that can be used or drawn to make a WLAN more secure are discussed. Based on this, some RAP discovery methods are discussed that will help make WLAN more secure and robust. Also, (Alotaibi & Elleithy, 2016) The study aimed to detect MAC address spoofing in wireless networks by using a measurement that is difficult to spoof related to the location of the wireless device, that is, the received signal strength (RSS). A technique is proposed based on the random forest method, which characterizes the shape of the data set to detect MAC address spoofing, rather than assuming that the data is Gaussian distributed. All previous methods based on clustering algorithms assume that there are two groups, which is not a valid assumption, because one device, such as AP, can form two groups. The results, from experience and extensive evaluations, show that the proposed method performs very well in terms of accuracy and prediction time.

*3.2.5 Authentication Attacks*

Authentication is the procedure through which a system verifies a user's identity before allowing them access. For example, (Khalid et al., 2020) the purpose of the research is to add the idea of Kerberos to the Extensible Authentication Protocol EAP so that it can better implement wireless LAN security authentication and enhance authentication security. To solve the problem of weak password guessing attacks caused by dictionary attacks, replay attacks in the authentication process, and man-in-the-middle attacks in the existing wireless local area network in terms of security authentication. Some flaws found based on the EAP authentication protocol have been analyzed. Based on this, it has been suggested that the existing Kerberos authentication protocol be improved so that it can be better integrated with the Extensible Authentication Protocol (EAP). The results show that, by empirical comparison, the average traffic volume for KEAP is significantly higher than that of EAP- TLS, and the average bit error rate is lower. It can be inferred that KEAP has a certain degree of security improvement over the current EAP-TLS public authentication protocol. Based on the results, the security of the wireless network has been shown to be significantly improved in terms of access to authentication. This is of great practical importance for wireless LAN security authentication.

Also, Ma & Ning, (2018) the study aimed to improve the Radius server in EAP authentication mode. The KEAPII protocol for EAP-based authentication method is proposed, in order to solve the dictionary attack problem, the Man-in-the-Middle Attack problem, the accuracy of transmission data received by Radius server, and the judging of restart attacks by Radius protocol. First, private and public key pair attributes and hash key attributes are added in the Radius protocol. Then, after referring to the concept of Kerberos protocol authentication, the concept of card authorization was introduced into the Radius server. Finally, a spreadsheet is created that combines the key sequence number in the base Hash string and the random number in both the client and the Radius server. The results show that, after security analysis, the KEAPII protocol ensures message security during transmission, and the Radius server has improved the accuracy of received messages. Based on the results, the client and Radius servers were guaranteed to avoid replay attacks.

*3.2.6 General Attacks*

For examples, (Ozkan-Okay et al., 2021) The study aimed to reduce the shortcomings of existing IDSs for WLANs and build a more effective system that can detect dynamically complex and unknown attack variants. In this context, a methodology has been proposed and has mainly two contributions. The first contribution is a feature selection approach (FSAP) to increase the speed of attack detection by reducing the number of features used. The second contribution is a hybrid attack detection technology, SABADT (Signature and Anomaly Based Attack Detection Technology), which detects attacks quickly and with high accuracy. The proposed methodology was performed on the KDD'99 and UNSW- NB15 datasets. Accordingly, the obtained results were compared with existing machine learning techniques. Then, a detection model was generated using the KDD'99 and UNSW-NB15 training data sets and tested on the KDD'99 and UNSW-NB15 test data sets. The results showed, the obtained accuracy rates of 99.65% and 99.17% are very high when compared with the leading methods in the literature. In addition, common tools were used to obtain a mixture of normal activities and existing attack behaviors in order to test new attacks in the scope of the study. Also, the different types of attacks were captured using the Wireshark tool. However, only some of the captured attacks were used in the testing phase. In this test case, the attacks were detected with an accuracy of 99.69%.

Also, (R. R. Singh et al., 2020) the study aimed to model a variety of detected attacks such as KRACK, low encryption and key recovery attacks. They were analyzed using the example of TAMARIN against the safety characteristics of the four-way handshake standard. This finds out which security features have been violated. The results show that TAMARIN models exposed to KRACK attacks do not violate any of the standard security features, indicating that the properties, as defined by the standard, are insufficient. Based on the results, an additional security feature is proposed and we show that it is violated by systems vulnerable to KRACK attacks, and that imposing this feature succeeds in stopping it. However, it demonstrates how TAMARIN can be used to automatically test the suitability of a set of security features against attacks, and that proposed mitigations make 802.11 secure against such attacks.

In addition, (Premkumar & Sundararajan, 2020) the study aimed to propose a new lightweight Deep Learning (DLDM)-based defense mechanism to detect and isolate DFP attacks. However, the network should be protected against DoS attacks with the help of the proposed DLDM framework structure. In addition, it describes the new algorithm for the successful detection of DoS attacks, such as fatigue, jamming, fast routing, and flooding. Extensive simulations have been conducted that can accurately isolate adversaries and are more resilient in the face of DoS attacks. The results show that our proposed simulation can achieve high detection rate, transmission rate, packet delivery rate, and accuracy. Also, this also reduces power consumption and false alarm rate.

For instances, (Aung & Thant, 2017) The study aims at the proposed work in implementing a network security system for wireless link layer attacks and understanding the patterns of these attacks. However, wireless link layer attacks target the lower layers of the Open System Interconnection (OSI) protocol stack to render the network unusable. In addition, link layer attacks in a wireless network are known to be one of the weakest points of wireless networks due to unprotected management frames. An approach has been proposed that can detect and mitigate wireless link layers. Moreover, the Wireless Link Layer Attack Detection Algorithm (WLLADA) has also been proposed using active and passive finger print methods to detect masquerade denial-of-service (DoS) attacks. Based on this, the proposed algorithm was implemented with a real-time setup using the Kali Linux environment with Python network programming

Also, (Thing, 2017)The study analyzed threats and attacks targeting the IEEE 802.11 network and also identified the challenges of achieving accurate threat and attack classification, especially in situations where they are new and the detection and classification system has not previously encountered. A solution based on the detection and classification of anomalies using a deep learning approach is then proposed. In addition, the deep learning approach self-learns the necessary

features to detect anomalies in the network and is able to perform classification attack accurately. The results showed, in the experiment they considered classification as a multi-class problem (that is, legitimate traffic, flood-type attacks, injection-type attacks and spoofing-type attacks identity), and an overall accuracy of 98.6688% in classifying attacks was achieved by the proposed solution.

Also, (Qin et al., 2018) The study aimed to propose a new method for detecting attacks in wireless enterprise networks using an approach based on SVM with real data set (AWID). This study presents a 2D data cleaning method that uses SVM to improve detection accuracy with respect to all identified potential attack types, not just overall accuracy. The results showed the detection accuracy of flood attacks, injection attacks and normal data 89.18%, 87.34% and 99.88%, respectively. Based on the results, the method works with simpler data attributes and faster and more efficient training thanks to the 2D data cleaning application. In future work, we recommend developing methods for sorting attacks using other ML algorithms and improving the classification accuracy for impersonation attacks. For example, (Aminanto & Kim, 2016) the study aimed to focus on improving impersonation attack detection. The feature selection method was used in order to identify the most important features for impersonation attack detection. However Artificial Neural Network (ANN) has been taken advantage of for feature selection and we implement Stacked Auto Encoder (SAE), a deep learning algorithm as classifier for the AWID dataset. Experiments show that the reduced input features are significantly improved for impersonation attack detection. In the near future, all attack classes will be tested for the AWID dataset. In addition, the combination of several learning methods as group learning is a difficult problem in order to achieve optimal IDS in Wi-Fi.

Also, (Kaur, 2016) the paper mainly aimed at two types of DOS attack, DE authentication and dissociation framework attack which are used for termination purpose in infrastructure network. Various detection and prevention mechanisms have also been put in place for these types of attacks. The results show the investigation of how to implement, detect, and prevent a dismantling/deauthentication attack. However, in future work a workable solution was required to detect and prevent these types of attacks in a real-time environment which can be easily adapted in the network environment and provide backward compatibility for all the system, making our wireless LAN more secure and reliable. Also, (Letsoalo & Ojo, 2016) the study discussed various MAC address spoofing detection and prevention techniques and their associated strengths and weaknesses. It has been noted that the problem with these MAC spoofing detection techniques is that they generate a lot of false positives and false negatives.

Also, some of these technologies require that the wireless network contain additional hardware in order to perform the required computation and encryption. However, this can also degrade network performance. Depending on the security level requirements, one can choose any of these methods. MAC address spoofing introduces other potential attacks in WLANs such as session hijacking and denial of service attacks. The results showed, noting that spoofing can be prevented by authentication at scale, which is not possible in the case of WLANs. In 802.11 wireless networks, authentication and encryption are not provided for the management and control frameworks. However, these frames are sent in clear text and make the network vulnerable to various attacks, and management frames authentication provides a good alternative to prevent spoofing. Accordingly, it is necessary to develop an effective approach that detects both management and deceptive data framework with minimal hardware changes which should also give less false positive results.

Several effective and reliable passive techniques can be combined to test if MAC address spoofing cannot be detected and prevented with low false positives and false negatives without affecting network performance. Thus, the combined route results can be linked to create a robust and reliable IDS system. However, different route test scenarios including variable traffic load from low to high and change of distance between attacker node and origin station from far to near must be considered. Also, (Lu & Yu, 2021) The study aims by analyzing Wi-Fi network vulnerabilities and common encryption methods vulnerabilities to propose a method for Wi-Fi penetration testing based on Kali Linux which is divided into four stages: setup, information gathering, simulation attack and reporting. Using monitoring, scanning, capturing, data analysis, password cracking, fake wireless access point spoofing, and other methods, Wi-Fi penetration testing with Kali Linux is processed in a simulated environment. Experimental results show that the method of Wi-Fi penetration testing with Kali Linux has a good effect on improving Wi-Fi security assessment.

## 4. Analysis and Results

*Q1: To review what are the common types of cybersecurity threats and attacks in a WLAN environment?*

In this section, we have analyzed the most common types of cybersecurity threats and attacks based on WLAN classifying. According to the CIA's triad, information security must meet three main principles, namely confidentiality, integrity and availability. All three concepts are required to some degree to achieve true security. Otherwise, the network will be vulnerable to attack. Moreover, two other basics were involved access control and authentication.

**Confidentiality** is the prevention of intentional/unintentional disclosure of data.
**Integrity** is control over intentional/unintentional modification of data.
**Availability** is the control over the availability of system resources on demand to authorized users/systems/processes.
Access control is the control of access to a resource by a legitimate user.
**Authentication** is the process by which the system verifies the identity of the user it wants to access (Sejdić et al., 2011).

*4.1 Confidentiality Attacks*

In this type of attack, Intruders try to intercept highly confidential or sensitive data transferred via a wireless network, either encrypted or in clear text, using the 802.11 or higher layer protocols. Eavesdropping, Man-in-the-Middle attacks, traffic analysis, and other passive attacks are examples (Sejdić et al., 2011). Table 1 below shows different types of attacks/threats in WLAN with mitigation techniques and future work on confidentiality.

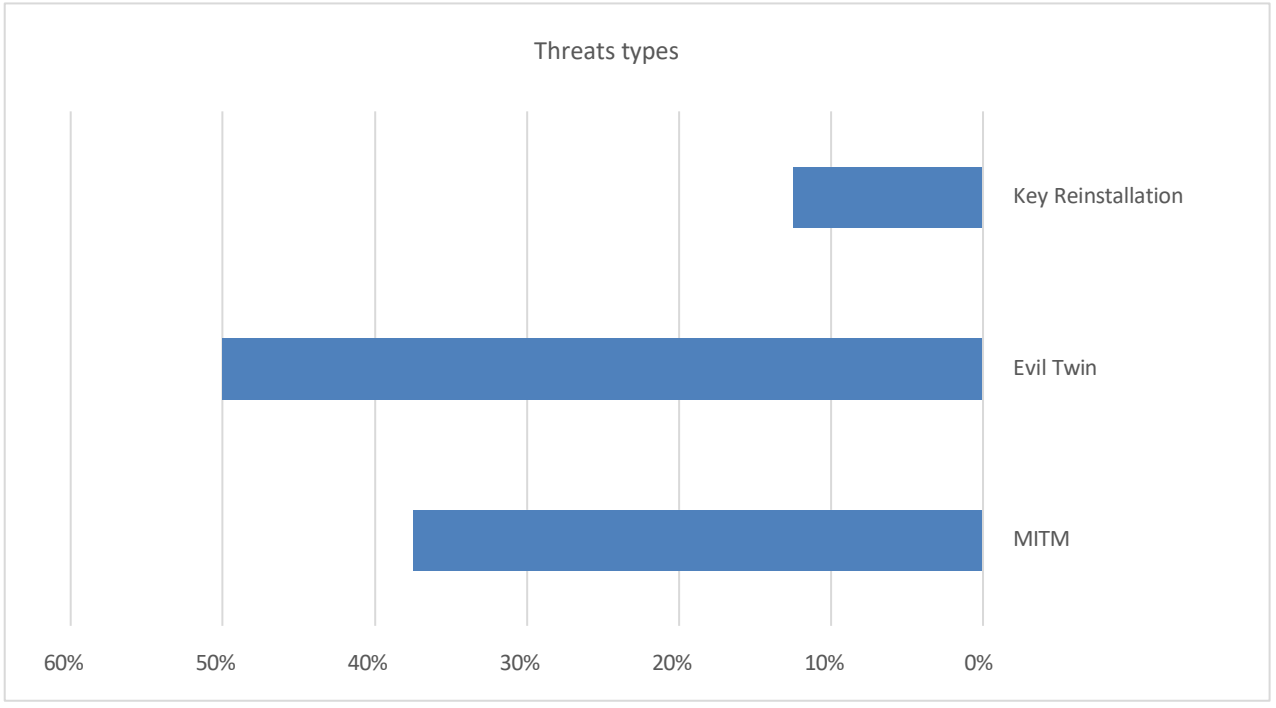


**Figure 5.** Findings of the most common types of Cyber threats and attacks on Confidentiality

*4.2 Integrity Attacks*

These attacks send forged/modified control, management, or data frames over wireless to deceive the recipient or aid another type of attack. Table 2 below shows different types of attacks/threats in WLAN with mitigation techniques and future work on integrity.

**Table 1.** The different type of threats in WLAN with mitigation techniques and future work on confidentiality

| **Author, publication year** | **Threat** | **Methods or Tools- type** | **Suggested mitigations** | **Future work** |
|---|---|---|---|---|
| Bhushan et al., 2017 | MITM attacks | By spoofing, attackers intercept communication between two end points (victims) and obtain data between them without the victim's knowledge. such as important type of this attack: Domain Name Server (DNS) spoofing is a type of attack in which tampered DNS records are used to reroute online traffic to a spoof website that seems identical to the original destination. Because DNS is an unencrypted protocol, spoofing makes it easier to intercept traffic.javascript:voi d()<br>Attackers intrude into the communication channel between the two points of contact.<br>Secure Socket Layer (SSL) and Transport Security Layer (TST) are protocols that ensure secure data transmission<br>over the internet, | Security measures such as VPN or IPsec can be used, which only protect against direct data confidentiality attacks.<br>A method has been proposed to detect and locate a MITM attacker in wireless networks by calculating the time of flight (RTT) and calculating the received signal strength (RSS) from the access point, if there is an attacker, these values are higher than there is no attacker.<br>Therefore, it is possible to detect an attacker by following signals that are unusual in network calculations, by empirical data such as signal strength and delay time, so it is possible to detect an attacker by sampling and RTT calculations during the process of<br>transmitting data | - |

| | | | | |
|---|---|---|---|---|
| | | and they require the use of other protocols to start the session, which include:<br>1- Record protocols to guarantee confidentiality.<br>2- Handshaking protocols: negotiation session establish.<br>3- Cipher spec protocol: for newly negotiation connection.<br>4- Alert protocol for detect errors. | between sender and receiver.<br>In addition, the clock synchronization protocol, this protocol is used to synchronize clocks by passing a time- stamped message, so each connection must present a fixed delay time, when any attackers with a non-constant delay can detect it by legitimate receiving nodes. | |
| (Rahim, (2017) | Man-in-the-middle attack | The public keys of the recipient and sender are stolen and replaced by eavesdropping. | Although the receiver and sender's public keys are stolen and replaced by eavesdroppers, eavesdroppers cannot execute a man-in-the-middle attack to view and edit messages using the interlock protocol method. This is because the encrypted communication is split into two halves and delivered in stages, making it impossible for eavesdroppers to figure out what the original message was. | - |

| | | | | |
|---|---|---|---|---|
| Amin & Mahamud, 2019 | Intercepting TCP sessions or SSL/SSH tunnels using typical man-in-the-middle attack tools on an evil twin AP. | Sniff, Ettercap tools | | A new mechanism that does not depend on encryption has been proposed called MR-ARP. The main working process is the use of the concept of the voting system. When an ARP request or message arrives indicating a new MAC address of an existing IP address from the ARP cache, MR- ARP queries that node corresponding to the current MAC address to check if that IP address is still used by that node. But the proposed mitigation is also not crypto-based. Unlike S-ARP, it does not require any key or certificate process. It does not require any central server either. As a result, there is no chance for our system to stop working at any given time unless the device the system is running on is out of processing. For MR-ARP which uses the concept of a voting system to |
| | | | | Give an accurate result, however, determining the safe path may take longer. Accordingly, the process of saving long-term memory to a file that is different and unique from other processes is used. (Using a Linux bash script at the client end). |

| | | | | |
|---|---|---|---|---|
| (Tian et al., 2021) | Evil Twin Attack To entice users, masquerading as an approved AP by broadcasting the WLAN's service set identifier (SSID). | cqureAP, HermesAP, HostAP, OpenAP, Quetec, WifiBSD tools. | a convolutional neural network (CNN) was trained to verify the identity of each hotspot. The experimental results showed that the proposed method can identify the hot spot with prior knowledge and effectively detect the Evil Twin attack | |
| Nakhila, 2018 | Evil Twin Attack | Targets Wi-Fi Protected Access II (WPA2). | Accordingly, three new technologies for detecting ETA were introduced. Detection methods are based on (1) establishing a secure connection to a remote server to detect the change of the gateway's public IP address by switching from one | As a future work, the proposed system can be ported to Mobile O.S, for example, Android, or to Windows using different |
| | | | Access point (AP) to another. (2) Monitoring multiple Wi-Fi channels in random order for specific data packets sent by the remote server. (3) Combine the previous solutions into a single universal method for ETA detection using Virtual Wireless Network Clients (VWCs). | Drivers and chipsets for wireless interface cards. Also, for example, Windows O.S users can use the Winpcap driver with supported interface cards. In addition, Android O.S users can use the PCAP library on the wireless interface card based on the RTL8187 chipset. |

| | | | | |
|---|---|---|---|---|
| Abare & Garba, 2019) | The key Reinstallation Attack:<br>In the WPA2 protocol, the key Reinstallation Attack attacks the four-way handshake needed to establish a nonce (a form of "shared secret"). | The adversary manipulates and replays handshake messages to trick the victim into reinstalling an already-in-use key, and when the key is reinstalled, associated parameters such as the incremental transmit packet number (Nonce) and receive packet | The proposed model includes encrypting the entire handshake messages and the generated Nonce values.<br>Next, an alpha check (a type of logical switch) was proposed which switches from 1 to 0 when the PTK is first installed. | - |
| | | Number (replay counter) are reset to their initial values. | this proposed model will help enhance security in the four-way handshake authentication process against pairwise transient key reinstallations. | |
| (Ahadi et al., 2022) | Evil twin attack | Evil Twin is a kind of adversary that impersonates a legitimate access point (LAP) because it can happen by spoofing the name (SSID) and MAC address (BSSID) of a legitimate access point (LAP). This attack can cause various threats such as MITM, outage, and access point ban | A new technology has been proposed based on two fingerprints from Access Point, Received Signal Strength Index (RSSI) and number of hops, which are difficult to copy by the opponent. The technology is implemented in a system called "ETDetector", which can detect and prevent the attack. | - |

**Table 2.** The different type of threats in WLAN with mitigation techniques and future work on integrity

| Author, publication year | Threat Attack | Methods or Tools- type | Suggested mitigations | Future work |
|---|---|---|---|---|
| Kim et al., 2019 | jamming attack scheme using fake ACK frame injection that interferes with and deceives transmitters in IEEE 802.11 WLAN. | The scheme immobilizes the proposed obfuscation attack retransmission mechanism for the victims' MAC and transport layers. | To prevent fake injection of an ACK frame in IEEE 802.11 WLANs, ACK frames must also be encrypted to ensure acknowledgment integrity | - |

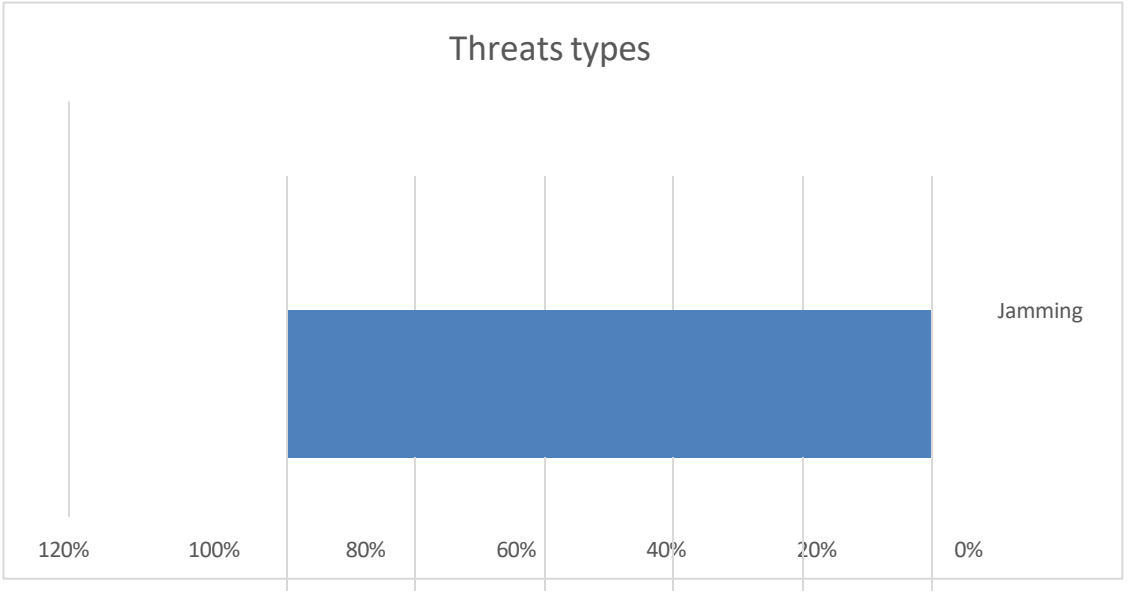


**Figure 6.** Findings of the most common types of Cyber threats and attacks on Integrity

*4.3 Availability Attacks*

These attacks aim to prevent legal users from using wireless LAN services.
Table 3 below shows different types of attacks/threats in WLAN with mitigation techniques and future work on availability.

| Author, publication year | Threat Attack | Methods or Tools-type | Suggested mitigations | Future work |
|---|---|---|---|---|
| , (Lounis & Zulkernine, 2020) | Denial-of-Service Attack: in this sort of attack, an attacker tries to block or inhibit regular network communication by flooding | An attacker impersonates the access point by spoofing management | These attacks can be mitigated by enforcing MFP | - |

| | | | | |
|---|---|---|---|---|
| | a legitimate client with bogus packets, incorrect messages, and duplicate IP or MA addresses.<br>DoS attacks on WPA2-PSK: Different types of DoS attacks have been proved to be vulnerable to WPA2-PSK, which can be classified into three categories:<br>(1) Thru Management Frames | frames, resulting in assaults such as deauthentication, deassociation, and sleep deprivation. | (Managemen t Frame Protection), i.e., 802.11w. | |
| | (2) Thru Protocol Misuse | An attacker could gain access to the radio by abusing MAC-layer protocols, such as greedy behavior on CSMA/CA or RTS/CTS. | There exist some detection approaches but not in the standard of IEEE 802.11. | - |
| | (3) Thru Jamming | The attacker generates out random signals on the network's operational radio channel to cause interference. | To reduce the impact of jamming attacks, techniques like FHSS can be used. | - |
| Pirayesh & Zeng, 2021 | Constant jamming attack Jamming Attacks<br>that delicately target the PHY transmission and MAC protocols of Wi-Fi communications. jamming attacks and anti-<br>jamming techniques for Wi- Fi, cellular, cognitive radio, ZigBee, Bluetooth, vehicular, RFID, and GPS wireless networks. | destroy legitimate users' packet reception by introducing high-energy interference into their data transmissions, and prevent them from accessing the channel by Constantly occupying it. One of its advantages is that it is highly effective, and the weak point is that it is ineffective energy. | Informative tables have been created to summarize the current jamming attacks and anti- jamming techniques for each network, which will help the public understand the basics of jamming and anti- jamming strategies. | Absorb comprehen sive knowledge of current jamming/a nti- jamming research findings and facilitate future design of jamming resilient wireless communica tion systems. |

| | | | | |
|---|---|---|---|---|
| (Santoro et al., 2017) | virtual jamming attacks on IEEE 802.11. | By Intrusion Detection Systems (NIDSs) | Proposing a new hybrid NIDS based on DS theory capable of efficiently detecting NAV attacks. In order to evaluate the proposed solution, the hybrid NIDS was tested on a real wireless scenario. A list of 14 different scenarios is proposed to Simulate realistic scenarios in Wi-Fi networks | For future work, the focus is on developing real-time hybrid NIDS capable of detecting a wide range of cyber threats and attacks against wireless networks. Similarly, the proposed hybrid NIDS application will be extended to other wireless communication technologies, such as LTE and WiMAX. In addition, added the possibility of automatic selection of relevant metrics designed for specific types of attacks. |

| | | | |
|---|---|---|---|
| Brar, T. S. (2017) | jamming attack | Jammer can perform the classification in real time by decoding the first few bytes of the transmitted packet. | Offer a solution to detect selective jamming attacks. To prevent these attacks different encryption schemes are implemented . An experimental framework has been developed to prove and quantify attacks against TCP and Voice over Internet Protocol (WVoIP) communications. |

| | | | | |
|---|---|---|---|---|
| (Dalal et al., 2022). | DE authentication attack and beacon flood attack | An intruder overwhelms a network by flooding it with thousands of bogus beacons, causing the wireless AP to become overburdened and unable to serve valid packets. As a result, legitimate clients will have a tough time locating the real AP. | A signature-based identifier design was proposed, which incorporates techniques to detect all attacks. Also, these techniques were applied in the testing and it was verified that the proprietary IDS system is able to successfully detect all attacks. In addition, schemes have been introduced to mitigate the impact of attacks as soon as they are discovered. | The code to carry out the attacks as well as the private IDS system was made publicly available, so that it could be used for future work by the research community as a whole. In particular, the research will help build a new and updated dataset based on WPA3, which in turn will aid in the developme nt of improved IDSs. |
| (Seth et al., 2019) | 802.11 De-authentication & Disassociation: | attacker pretends to be a client or AP and sends unauthorized management frames by flooding the legitimate target with thousands of authentication or disassociation messages. This compels them | The DES-based IDS detector is proposed to detect a deauthorizati on attack in a Wi-Fi network. Accordingly, the proposed scheme is easy to implement, | - |

| | | | | |
|---|---|---|---|---|
| | | to exit either the authentication or association states (Tao & Ruighaver, 2005). | and no modification of the protocol is required. Set up deauthentication frames terminal with aircrack-ng on a machine running KALI Linux. Wi-Fi is sniffed using the netsniff-ng utility. | |
| Siahaan, 2016) | Fake SSID | The attacker floods the air with thousands of beacon frames with fake SSIDs and all access points get busy processing the fake SSIDs. | penetration testing was conducted, which is one of the common methods of password cracking, and it is the best way to measure the level of security. This tool directs the user to try to connect with a similar SSID. However, they do not realize that the name they are joining is a fake SSID. Attackers use this moment to get the password. Shortly after they attempted to connect multiple times, the attacker had already registered the SSID password. | - |

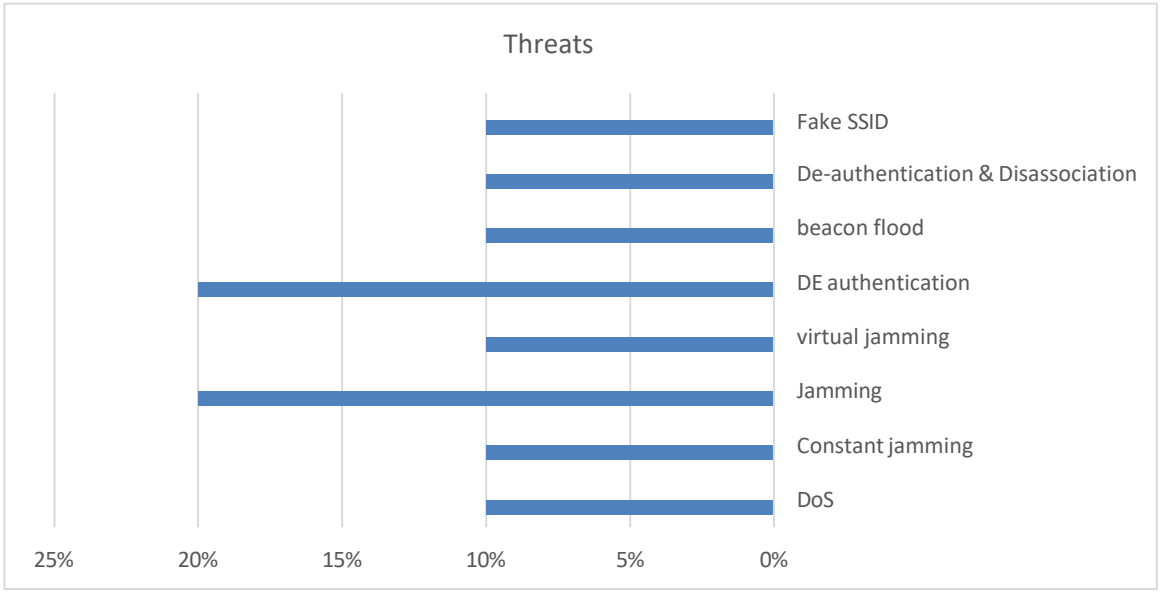


**Figure 7.** Findings of the most common types of Cyber threats and attacks on Availability

### 4.4 Access Control Attacks

Access Control Attacks: Bypassing filters and firewalls, these attacks attempt to obtain unauthorized access to a network. Table 4 below shows different types of attacks/threats in WLAN with mitigation techniques and future work on access control.

**Table 4** the different type of threats in WLAN with mitigation techniques and futuer work on access control

| **Author, publication year** | **Threat Attack** | **Methods or Tools- type** | **Suggested mitigations** | **Future work** |
|---|---|---|---|---|
| Umesh, A. S. B. D. A. S. (2017). | Rogue Access Points | Any hardware or Software. Installing an unprotected AP inside a firewall, allowing access to a trusted network through an open backdoor. | Proposing a Hopfield Neural Network approach to automatically detect such rogue access points in wireless networks. Native hardware passwords are stored in matrix weight and pattern matching format at login time. The simulations concluded that this neural network algorithm takes less time to execute and stores a number of patterns very precisely. Also, the connections of the | |

| | | | | |
|---|---|---|---|---|
| | | | various devices are stored in the form of network parameters that are difficult to break and the variance in the input and output data shows the presence of unauthorized points such as rogue access points. In addition, the researchers created a secret key to encrypt and decrypt messages using HPNN. The proposed neural network approach is a safe and easy-to-operate method compared to the traditional encryption method. The proposed model is designed to use the existing WLAN infrastructure and no additional equipment is required to perform this detection. | |
| Dahiya & Gill, 2017 | Rogue Access Points on any organization is the attack of Man in the Middle. | This attack leads to a number of unauthorized access points and rogue access points that are not easily detected. Native hardware passwords are stored in matrix weight and pattern matching format at login time. | Propose the automatic detection of rogue access point, which depends on the Hopfield Neural Network algorithm. | - |
| Alotaibi & Elleithy, 2016 | MAC addresses spoofing | In this type of attack ،by impersonating a valid network user, the attacker has access to privileged data and other resources such as printers, servers, and | A technique for detecting MAC address spoofing based on random forest has been proposed. Moreover, it has a good prediction .time | In future work, a new or external detection method for detecting MAC |

| | | |
|---|---|---|
| | so on. To do so, the attacker changes their MAC address and impersonates a legitimate access point or station. Because 802.11 networks do not authenticate source MAC address frames, this may be done quickly. As a result, the attacker. can impersonate MAC addresses and take control of a session. Furthermore, 802.11 does not require an access point to demonstrate that it is a legitimate access point. | address spoofing will be considere d. New/exit detection methods only require training with a legitimate device without covering the entire network range. A single class SVM-based approach will be planned to create a legitimate hardware profile. |

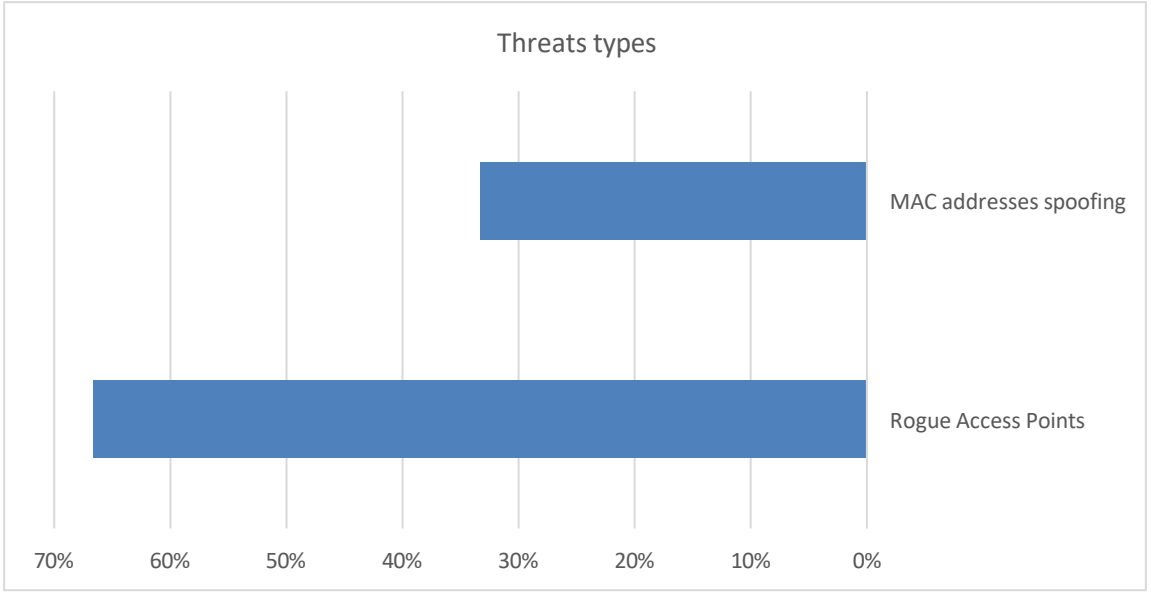


**Figure 8.** Findings of the most common types of Cyber threats and attacks on Access control

*4.5 Authentication Attacks*

Authentication Attacks: is the procedure through which a system verifies a user's identity before. Table 5 below shows different types of attacks/threats in WLAN with mitigation techniques and future work on access control.

**Table 5.** The different type of threats in WLAN with mitigation techniques and future work on authentication

| **Author, publication year** | **Threat Attack** | **Methods or Tools- type** | **Suggested mitigations** | **Future work** |
|---|---|---|---|---|
| (Khalid et al., 2020) | Dictionary attacks, re-attacks in the authentication process, and man-in- the-middle. | The problem of weak password guessing attacks caused by dictionary attacks, re-attacks in the authentication process, and man-in- the-middle attacks in the current wireless LAN in terms of security authentication. | it has been suggested that the existing Kerberos authentication protocol be improved so that it can be better integrated with the Extensible Authentication Protocol (EAP). The results show that, by empirical comparison, the average traffic volume for KEAP is significantly higher than that of EAP-TLS, and the average bit error rate is lower. It can be inferred that KEAP has a certain degree of security improvement over the current EAP-TLS public authentication protocol | |
| Ma & Ning, 2018) | dictionary attack and brute force attack. | Intruders use these attacks to steal valid user identities and credentials in order to gain access to networks and services that are otherwise private | The KEAPII protocol for EAP- based authentication method is proposed, in order to solve the dictionary attack problem, the Man-in-the-Middle Attack problem, the accuracy of transmission data received by Radius server, and the judging of restart attacks by Radius protocol. The results show that, after security analysis, the KEAPII protocol ensures message security during transmission, and the Radius server has improved the accuracy of received messages. Based on the results, the client and Radius servers were guaranteed to avoid replay attacks. | - |

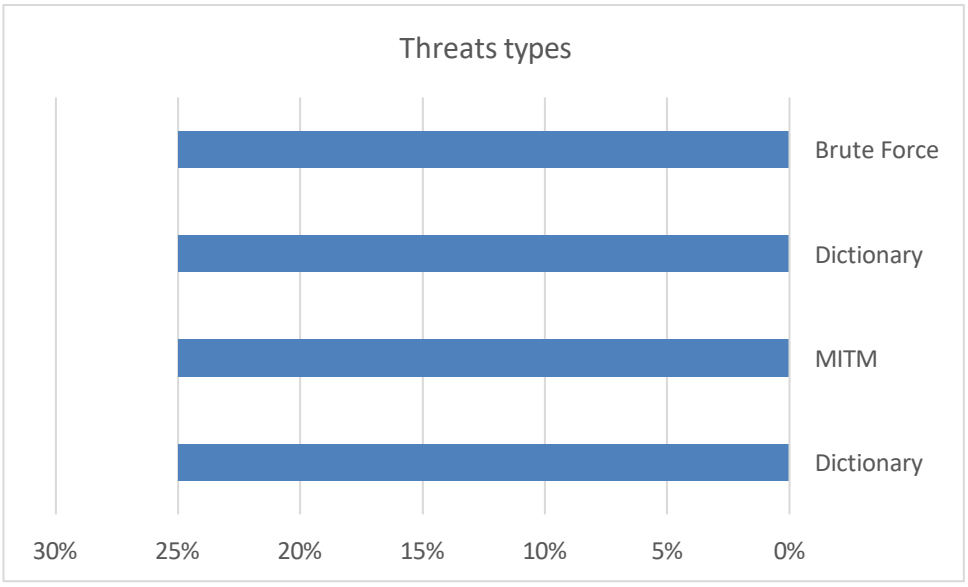


**Figure 9.** Findings of the most common types of Cyber threats and attacks on Authentication

*4.6 General Attacks*

Table 6 below shows different types of attacks/threats in WLAN with mitigation techniques and future work on general.

**Table 6.** The different type of threats in WLAN with mitigation techniques and future work on general

| **Author, publication year** | **Threat** | **Methods or Tools- type** | **Suggested mitigations** | **Future work** |
|---|---|---|---|---|
| Ozkan-Okay et al., 2021 | Dynamically complex and unknown attack variants. (Legitimate traffic, flood-type attacks, injection-type attacks and spoofing-type attacks. ) | Signature and Anomaly Based Attack | Propose a solution based on detection and classification of anomalies using a deep learning approach. | - |
| R. R. Singh et al., 2020 | KRACK, low encryption and key recovery attacks. | Using TAMARIN versus the security features of the four-way handshake standard. | An additional security feature is proposed and we show that it is violated by systems vulnerable to KRACK attacks., and that imposing this feature succeeds in stopping it. However, it | |

| | | | | |
|---|---|---|---|---|
| | | | demonstrates how TAMARIN can be used to automatically test the suitability of a set of security features against attacks | |
| Premkumar & Sundararajan, 2020 | Denial-of-service | such as fatigue, jamming, fast routing, and flooding. | Propose a new lightweight defense mechanism based on deep learning (DLDM) to detect and isolate DFP attacks. The results show that the proposed simulation can achieve high detection rate, transmission rate, packet delivery rate, and accuracy. Also, this also reduces power consumption and false alarm rate. However, extensive simulations have been conducted that can precisely isolate enemies and be more resilient in the face of DoS attacks. | In the future, optimization in a deep learning model by applying various optimization techniques and if there is any public dataset that includes these attacks will be discussed. Based on the results, further exploration of spatial information is suggested to find ways to eliminate these different unknown enemies from the wireless network. In addition, it can be seen that wireless sensor networks are more robust and less vulnerable to DoS attacks. |

| | | | | |
|---|---|---|---|---|
| Premkumar & Sundararajan, 2020 | Denial-of-service | such as fatigue, jamming, fast routing, and flooding. | Propose a new lightweight defense mechanism based on deep learning (DLDM) to detect and isolate DFP attacks. The results show that the proposed simulation can achieve high detection rate, transmission rate, packet delivery rate, and accuracy. Also, this also reduces power consumption and false alarm rate. However, extensive simulations have been conducted that can precisely isolate enemies and be more resilient in the face of DoS attacks. | In the future, optimization in a deep learning model by applying various optimization techniques and if there is any public dataset that includes these attacks will be discussed. Based on the results, further exploration of spatial information is suggested to find ways to eliminate these different unknown enemies from the wireless network. In addition, it can be seen that wireless sensor networks are more robust and less vulnerable to DoS attacks. |
| Aung & Thant, 2017 | Link layer attacks ((DoS)) | because of unprotected management frames. | Wireless Link Layer Attacks Detection algorithm (WLLADA) is also proposed by using active and passive finger printing methods to detect masquerading denial of service (DoS) attacks. Proposed algorithm is implemented with a real time set-up using in Kali Linux environment with python network programming. | This proposed work only detects and mitigate wireless link layer attacks. In future work, prevention and auditing modules will be considered for management frames. |

| | | | | |
|---|---|---|---|---|
| (Thing, 2017) | Legitimate traffic,flood-type attacks, injection-type attacks and spoofing-type attacks identity. | detection and classification system attack | Propose a solution based on detection and classification of anomalies using a deep learning approach. In addition, the deep learning approach self-learns the necessary features to detect anomalies in the network and is able to accurately carry out a classification attack. The results showed that, in the experiment, they considered classification as a multi-category problem (that is, legitimate traffic, flood-type attacks, injection-type attacks and spoofing-type attacks), and an overall accuracy of 98.6688% in classifying the attacks. | - |
| Qin et al., 2018 | Flood attacks, injection attacks and normal data | For detecting in wireless enterprise networks | Propose a new method for detecting attacks in wireless enterprise networks using an approach based on SVM with real data set (AWID). | In future work, develop methods for sorting attacks using other ML algorithms and improve the classification accuracy for impersonation attacks. |
| Aminant o & Kim, 2016 | Impersonation attack detection | detection of impersonator attacks | The feature selection method was used in order to identify the most important features for detecting an impersonation attack. However, we have taken advantage of an Artificial Neural Network (ANN) for feature selection and we implement Stacked Auto Encoder (SAE), a deep learning algorithm as a classifier for the AWID dataset. Experiments show that | In the near future, all attack classes will be tested for the AWID dataset. In addition, the combination of several learning methods such as group learning is a difficult problem in order to achieve optimal IDS in Wi-Fi. |

| | | | | |
|---|---|---|---|---|
| | | | the reduced input features are significantly improved for impersonation attack detection. | |
| Kaur, (2016 | DOS attack | DE authentication and dissociation framework attack which are used for termination purpose in infrastructure network | countermeasure: Pseudo random number-based authentication and Signal Print Targeted both AP AND CLIENT -MAC Spoof Detection. | In future work, a workable solution was needed to detect and prevent these types of attacks in a real-time environment which can be easily adapted into the network environment and provide backward compatibility for all the system, making our wireless LAN more secure and reliable. |
| (Letsoalo & Ojo, 2016) | session hijacking and denial of service attacks | MAC address spoofing | The results showed, noting that spoofing can be prevented by authentication at scale, which is not possible in the case of WLANs. In 802.11 wireless networks, authentication and encryption are not provided for the management and control frameworks. However, these frames are sent in clear text and make the network vulnerable to various attacks, and management frames authentication provides a good alternative to prevent spoofing. | |
| Lu & Yu, 2021 | password cracking | Fake wireless access point spoofing | Suggesting a method for Wi-Fi penetration testing based on Kali Linux which is divided into four stages: setup, information gathering, simulation attack and reporting. Using monitoring, scanning, capture, data analysis, | |

| | | |
|---|---|---|
| | | password cracking, fake wireless access point spoofing, and other methods, Wi- Fi penetration testing with Kali Linux is processed in a simulated environment. Experimental results show that the method of Wi-Fi penetration testing with Kali Linux has a good effect on improving Wi-Fi security assessment. |

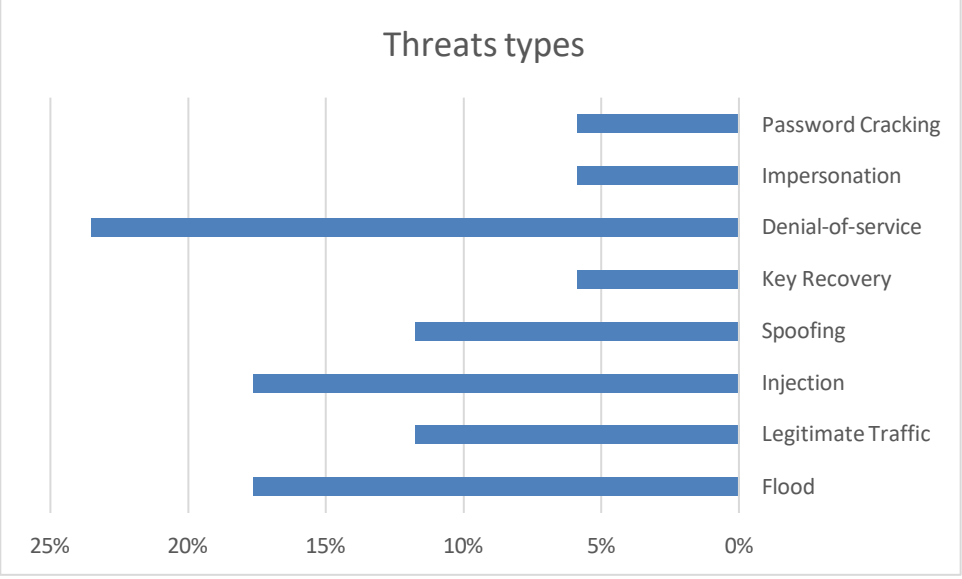


**Figure 10.** Findings of the most common types of Cyber threats and attacks on general

*Q2: To review what are the suitable cybersecurity mitigation techniques for WLAN threats and attacks?*

In this section, we have presented the study results related to the most common mitigation methods that have been used in previous studies to address the multiple types of cybersecurity attacks in WLAN as mentioned in the above section, which are the Hopfield Neural Network approach and the deep learning approach. Figure 11 showed suggested mitigation techniques to address WLAN threats.

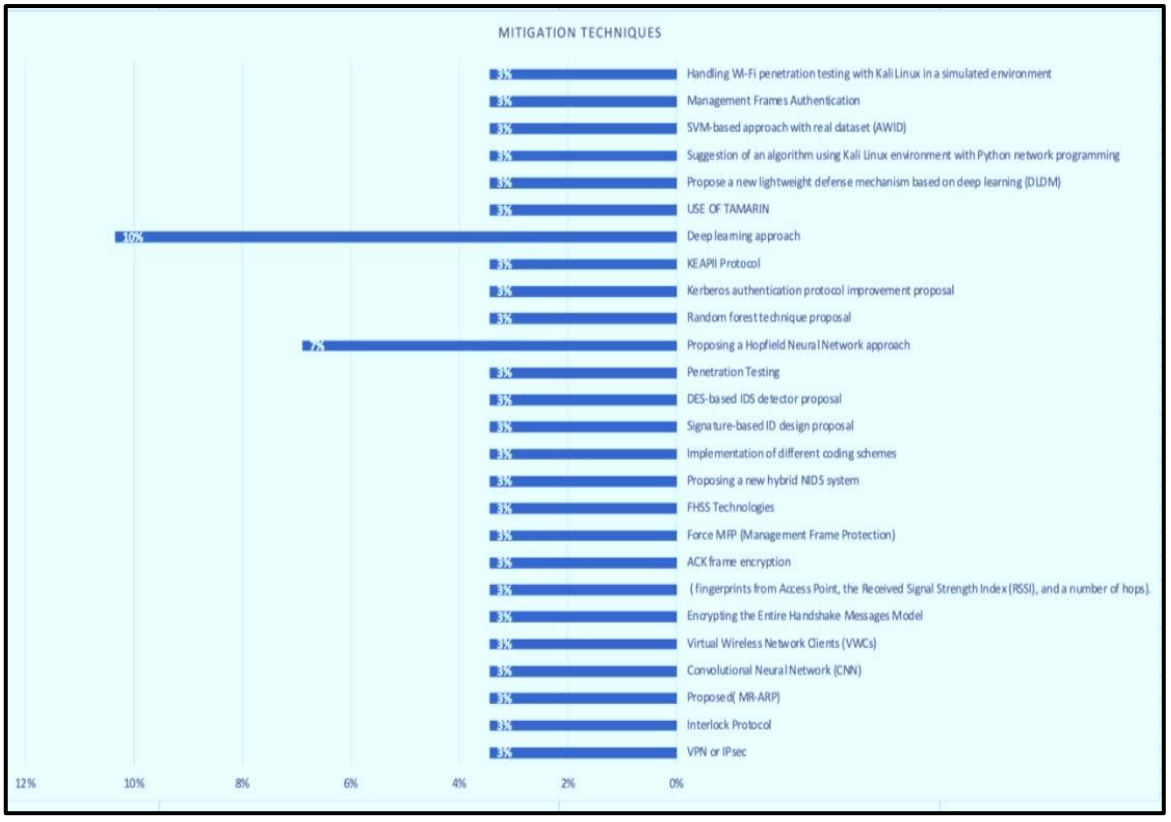


**Figure 11.** Findings of the types of Mitigation Technique for WLAN threats and attack

## 5. Conclusion

Securing a wireless network is an ongoing process. Realistically, there is still no one-size- fits-all security solution. When a new technology is first introduced, hackers research the protocol, look for vulnerabilities, and then put together a program and script to try to exploit those vulnerabilities. As a result, we will never be able to eliminate all threats and weaknesses, and even if we do, we will most likely waste money by repelling a low probability, low impact attack. Consequently, effective WLAN security will always be a balancing act between acceptable risk and countermeasures to prevent such threats or risks. This project aims to discuss common threats related to the wireless LAN system, and a comprehensive review of existing studies related to cybersecurity threats in the wireless LAN. A systematic literature review (SLR) was performed to identify potential threats and identify appropriate countermeasures for each WLAN. Based on our findings, which indicated that the DoS, Jamming, and MITM attacks are the most common threat. In addition, the results reveal the use of the most proposed techniques to mitigate wireless LAN attacks, which are the Hopfield Neural Network approach and the deep learning approach. In addition to getting acquainted with the latest technologies that were used in future work. Therefore, this paper recommends future researchers conduct more research.

## References

[1] G. Abare and E. J. Garba, "A proposed model for enhanced security against key reinstallation attack on wireless networks," *Int. J. Sci. Res. Netw. Secur. Commun.*, vol. 7, no. 3, pp. 21–27, 2019.
[2] S. A. A. Ahadi, E. Baray, N. Rakesh, and S. Varshney, "Public Wi-Fi security threat evil twin attack detection based on signal variant and hop count," *AIP Conf. Proc.*, vol. 2424, no. 1, p. 020002, 2022.
[3] B. Alotaibi and K. Elleithy, "A new MAC address spoofing detection technique based on random forests," *Sensors*, vol. 16, no. 3, p. 281, 2016.
[4] A. A. M. M. Amin and M. S. Mahamud, "An alternative approach of mitigating ARP-based man-in-the-middle attack using client site bash script," in *Proc. 6th Int. Conf. Electr. Electron. Eng. (ICEEE)*, 2019, pp. 112–115.
[5] M. E. Aminanto and K. Kim, "Detecting impersonation attack in WiFi networks using deep learning approach," in *Proc. Int. Workshop Inf. Secur. Appl.*, 2016, pp. 136–147.

[6] M. A. C. Aung and K. P. Thant, "Detection and mitigation of wireless link layer attacks," in *Proc. IEEE 15th Int. Conf. SERA*, 2017, pp. 173–178.
[7] E. Baray and N. K. Ojha, "WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique," in *Proc. 5th Int. Conf. Comput. Methodol. Commun. (ICCMC)*, 2021, pp. 23–30.
[8] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking—A review," in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Autom. (ICACCA)*, 2017, pp. 1–6.
[9] T. S. Brar, "Study and detection of jamming attacks in wireless networks," unpublished.
[10] M. Dahiya and S. Gill, "Detection of rogue access point in WLAN using Hopfield neural network," *Int. J. Electr. Comput. Eng.*, vol. 7, no. 2, p. 1060, 2017.
[11] N. Dalal *et al.*, "A wireless intrusion detection system for 802.11 WPA3 networks," in *Proc. 14th Int. Conf. COMSNETS*, 2022, pp. 384–392.
[12] J. Kaur, "MAC layer management frame denial of service attacks," in *Proc. Int. Conf. Micro-Electron. Telecommun. Eng. (ICMETE)*, 2016, pp. 155–160.
[13] A. Kavianpour and M. C. Anderson, "An overview of wireless network security," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput.*, 2017, pp. 306–309.
[14] H. Khalid *et al.*, "Cybersecurity in Industry 4.0 context: Background, issues, and future directions," *Nine Pillars Technol. Ind.*, vol. 4, pp. 263–307, 2020.
[15] W. Kim, J. Park, J. Jo, and H. Lim, "Covert jamming using fake ACK frame injection on IEEE 802.11 wireless LANs," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1502–1505, 2019.
[16] E. Letsoalo and S. Ojo, "Survey of media access control address spoofing attacks detection and prevention techniques in wireless networks," in *Proc. IST-Africa Week Conf.*, 2016, pp. 1–10.
[17] K. Lounis and M. Zulkernine, "Exploiting race condition for Wi-Fi denial of service attacks," in *Proc. 13th Int. Conf. Security Inf. Netw.*, 2020, pp. 1–8.
[18] H.-J. Lu and Y. Yu, "Research on WiFi penetration testing with Kali Linux," *Complexity*, vol. 2021, 2021.
[19] Y. Ma and H. Ning, "Improvement of EAP authentication method based on RADIUS server," in *Proc. IEEE 18th Int. Conf. Commun. Technol. (ICCT)*, 2018, pp. 1324–1328.
[20] O. Nakhila, *Masquerading Techniques in IEEE 802.11 Wireless Local Area Networks*, 2018.
[21] M. Ozkan-Okay *et al.*, "SABADT: Hybrid intrusion detection approach for cyber attacks identification in WLAN," *IEEE Access*, vol. 9, pp. 157639–157653, 2021.
[22] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *arXiv:2101.00292*, 2021.
[23] M. Premkumar and T. V. P. Sundararajan, "DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks," *Microprocess. Microsyst.*, vol. 79, p. 103278, 2020.
[24] Y. Qin *et al.*, "Attack detection for wireless enterprise network: A machine learning approach," in *Proc. IEEE ICSPCC*, 2018, pp. 1–6.
[25] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," *ARPN J. Eng. Appl. Sci.*, vol. 12, no. 22, pp. 6483–6487, 2017.
[26] D. Santoro *et al.*, "A hybrid intrusion detection system for virtual jamming attacks on wireless networks," *Measurement*, vol. 109, pp. 79–87, 2017.
[27] K. S. Sathyavani and P. Selvi, "Wireless network security vulnerabilities, threats and countermeasures," in *Proc. Int. Conf. Inf. Image Process.*, 2014.
[28] E. Sejdić, I. Djurović, and Lj. Stanković, "Fractional Fourier transform as a signal processing tool: An overview," *Signal Process.*, vol. 91, no. 6, pp. 1351–1369, 2011.
[29] A. D. Seth, S. Biswas, and A. K. Dhar, "De-authentication attack detection using discrete event systems in 802.11 Wi-Fi networks," in *Proc. IEEE ANTS*, 2019, pp. 1–6.
[30] A. P. U. Siahaan, *WLAN Penetration Examination of the University of Pembangunan Panca Budi*, 2016.
[31] G. Singh, "Wireless network components and security protocol," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, 2017.
[32] R. R. Singh *et al.*, "Modelling of 802.11 4-way handshake attacks and analysis of security properties," in *Proc. Int. Workshop Secur. Trust Manag.*, 2020, pp. 3–21.
[33] N. A. Sunday, *Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures*, Blekinge Inst. Technol., 2008.
[34] S. Suroto, "WLAN security: Threats and countermeasures," *JOIV: Int. J. Informatics Visualization*, vol. 2, no. 4, pp. 232–238, 2018.
[35] Z. Tao and A. B. Ruighaver, "Wireless intrusion detection: Not as easy as traditional network intrusion detection," in *Proc. IEEE TENCON*, 2005, pp. 1–5.
[36] V. L. L. Thing, "IEEE 802.11 network anomaly detection and attack classification: A deep learning approach," in *Proc. IEEE WCNC*, 2017, pp. 1–6.
[37] Y. Tian, S. Wang, and L. Zhang, "CNN-based evil twin attack detection in WiFi networks," *MATEC Web Conf.*, vol. 336, p. 08006, 2021.
[38] A. S. B. D. A. S. Umesh, "Rogue access point: A threat to wireless society," unpublished.
[39] M. Vanhoef, D. Schepers, and F. Piessens, "Discovering logical vulnerabilities in the Wi-Fi handshake using model-based testing," in *Proc. ACM AsiaCCS*, 2017, pp. 360–371.