Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 08 Issue 02
2025

Research Article
https://doi.org/10.56979/802/2025

A Survey: Enhancing Wireless Security in the Digital Age

Zain Iqbal[1*], Irshad Ahmed Sumra[2], Hadi Abdullah[2], and Ijaz Khan[3]

[1]Department of Information Technology, Lahore Garrison University, Lahore, 54000, Pakistan.
[2]Department of Computer Science, Lahore Garrison University, Lahore, 54000, Pakistan.
[3]Department of Avionics Engineering, National University of Sciences and Technology (NUST), Pakistan.
*Corresponding Author: Zain Iqbal. Email: zk787731@gmail.com

Accepted: December 11, 2024 **Published:** March 01, 2024

Abstract: In today's globalized society, protecting wireless networks from unauthorized users is fundamental. Wireless networks and mobile devices are under constant attack, far more than their wired equivalents, which has made achieving complete protection an unfulfilled goal, despite decades of research. This study considers critical matters such as authentication, confidentiality, integrity, and availability, which are important in the security of wireless networks. We study existing protocols and recommend changes to improve their security. An innovation consists of a new strategic approach to security risk management integrating a data authentication and integration model with machine learning methods. This also provides an examination of the current responses to wireless network security problems, highlighting their advantages and drawbacks in light of constant changes to cyber threats, especially phishing attacks. The objective is to accentuate the need to strengthen wireless networks security to safeguard confidential information from unauthorized access. Additionally, the article provides an in-depth review of methods to address security vulnerabilities associated with wireless networks.

Keywords: Encryption; Wi-Fi Protected Access 2 (WPA2); Wireless Local Area Network (WLAN); Security; Integrity; 802.11i; Firewall.

1. Introduction

The Wireless technology implements radio frequency to connect processors and additional net devices, also known as Wireless Fidelity (Wi-Fi) or Wireless Local Area Network (WLAN). It is progressively gaining popularity due to its comfort of installation. And lack of electric wiring. Because of lower pricing, the marketplace for wireless networks has grown in recent years, letting people work with flexibility. Wi-Fi LANs (Local Area Network) always employ Electromagnetic waves to send data signals from one end of the network towards the other, and they are performed at the physical layer [1]. Access points for Wi-Fi networks are expensive to install, but the time and money saved by installing additional nodes is little. Since there are no connections, wireless communication has become less expensive to maintain than traditional wired networks in terms of hardware as even the industry for wireless connections continues to expand, new security issues and concerns have risen [2]. The security concerns include how to secure information and ensure that communications are legitimate. When we connect to public Wi-Fi at shops or Restaurants to update our social media or respond to emails, wireless security may go under our radar.

Connecting across unsecured lines or networks, on the other hand, is a security risk that might result in data loss, Leaked account passwords, and a slew of other issues. Therefore, it's so important to use the correct Wi-Fi security measures. Security issues are well-known, and several researches have been conducted in this field. The research has centered on the technological elements of security. Radio waves are used to interact with Wi-Fi. The wireless network technology allows devices to connect to the internet. However, since flaws in the protocols on which it is built have been uncovered, this system is particularly vulnerable to hacking [3]. This study investigates wireless internet security methods and approaches and how we can improve the security of WIFI using these different algorithms and discuss the authentication, secrecy, integrity, and availability of wireless services are described in the security requirements of wireless network [4].

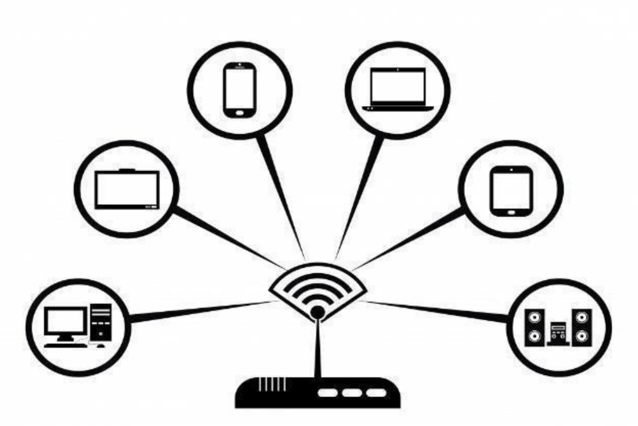

Figure 1. Wireless communication [1].

This paper is organized into seven sections, and Section 2 is based on the literature review of the past research work done on the wireless security architecture. Section 3 explores methodology and attacks protocols and standards and Section 4 categorizes attack flow with attack flow diagrams. Sections 5 provides explanation of solutions, signal-hiding techniques, firewall policies, encryption and decryption, packet sniffing, and VPNs on wireless networks respectively. Section 6 presents a review table summarizing key challenges, threats, and security solutions in wireless networks providing recommendations for future advancements, such as AI-driven security. Finally, in Section 7, we conclude the research work.

2. Literature Review

Nazir, Rashid et al [2] mentioned the WLAN protection and security is a dynamic system which is always evolving and when deployed in the field is susceptible within varying degrees to a class of hacker threats which posed different wireless network security problems. These measures of security in a company are implemented containing solutions that are more than adequate and quite simple. Soft computing is a new area and a lot of effort is being put into development of systems for detection and prevention of intrusion into networks or other types of attacks.

A. Kavianpour et al [3] Showed that the WIFI security refers to how computers linked to wireless networks are protected from unauthorized entrance or damage. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are the most secure communications techniques. Because it provides hackers or attackers with a simple transport medium, it demands a different approach than wired network security, increasing the risk that any security must address.

Emilselvan et al [4].In this paper WEP includes several security flaws. WEP, for example, uses the same key for encryption and validation. If the hacker can access the shared key, he can access the communications. The security and integrity flaws stem from well-known flaws in the WEP that are used for the encryption of data at the data link layer. WPA integrated the IEEE 802.11i standard in its entirety.

Ee Sun et al [5] discussed that Users need to be proactive, have backup plans, and be alert in order to protect themselves from these assaults. This strategy greatly lowers the likelihood of being a victim of such threats. An intrusion prevention system (IPS) can successfully reduce active threats in addition to encryption and pre-encryption methods like Secure Sockets Layer (SSL). It's crucial to realize however, that Distributed Denial-of-Service (DDoS) attacks cannot be stopped by firewalls alone. Because DDoS assaults can imitate legitimate user traffic to exploit security holes and get beyond firewalls, research shows that using firewalls as a protection against these attacks is useless.

In this paper, Eian et al [6] the different attacks on the network i.e., active and passive attacks and meet-in-the-middle attacks have been discussed and some techniques are also discussed to prevent our network from these attacks done by the noxious users. Cryptanalysis uses sub-keys in one round to decrypt the cipher text and cryptography that uses encryption and decryption at the senders and receivers' sides respectively. The Kohlios et al [7] mentioned the WEP protocol may be applied with 40 bits key and a 24-bit, or it can be expanded to utilize a more significant key. As a result, a brute-force Attack can readily compromise the shorter key. Although the giant key can be hacked, the 104-bit key makes the attack more complex. The Kirti Kaushik et al [8] discussed that wireless network authentication has become increasingly crucial with the fast expansion of wireless devices and the rise in intrusion risks. One of the most effective methods for improving wireless network security is physical-layer security based on radio frequency fingerprinting. Initially, they go through the framework of wireless device identification in this document. Furthermore, they examine signal detection strategies for the structure. The Wang Peihong et al [10] explained the numerous configurations that are specified for the security of information and network with the help of different zones, each zone has different firewalls for validating the penetration in the network. Configuration of information will have the knowledge of all the aspects and the factors that may compromise the security. Each zone or firewall has specific actions to perform, some have to detect the malicious code other have to validate the authentic users. When there is a web-based configuration auto detection like an anti-virus system runs in the background will indicate the cracked versions of tools and infected data and information. The Karygiannis et al [11] explained the evolution of wireless networks from time to time. As these have a major role in connecting users worldwide, so it has been divided into different types for ease and saving networks from complexity and intruder attacks. As much greater the network, the greater the chances of compromising its security. This network is classified into LAN, WAN, and MAN for small and large organizations respectively. Thus, their security and control become easy and efficient. The Lakhtaria Kamaljit et al [12] explained encryption is a technique for securing data. Although an intruder could collect encoded data, they would not be able to decrypt it in a realistic period. With wireless authentication, these encryption techniques are used. The Burg et al [14] explained information is public among approved users in Wi-Fi communication. This procedure, however, is vulnerable to a multitude of malicious assaults due to the transmission spirit of the wireless medium. Security/privacy guidelines are established to guard WIFI communication against, Denial of service, Eavesdropping, node access, data falsification, and other wireless dangers.

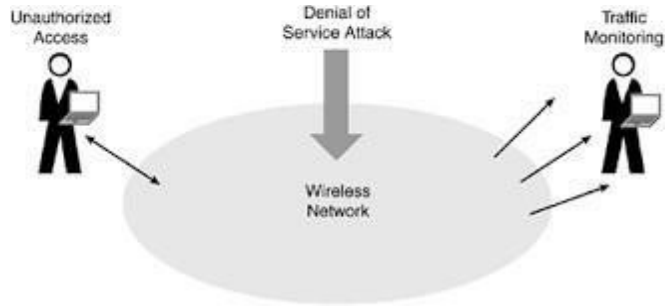

Figure 2. Threats to Wireless Network Security and Denial of Service (DoS) [14]

B, Prabadevi et al [15] proposed WLANs may be built using four distinct Wi-Fi configurations: infrastructure, ad hoc, bridge, and repeater. The first two modes specify how Wi-Fi devices can connect directly or indirectly with one another, while the latter two modes define how to expand a Wi-Fi network's range. **Forbacha** et al [16] discussed this project aims to overcome the drawbacks of traditional fixed telephone lines, which are expensive and dangerous, especially in Cameroon, by developing and deploying a secure Virtual Private Network (VPN) online. In order to replace conventional data cables, the study uses the internet as a data pipeline. The implementation is tested using a CISCO Packet Tracer simulation. The J. Smith et al [17] discussed the findings show that VPNs provide businesses with a dependable, affordable, and secure communication solution. VPNs are crucial for remote business operations because they protect sensitive data from unwanted access and eliminate the need for business travel, both of which are good for the environment. The Kibona et al [18] discussed the this paper outlines wireless broadband networks, a new technology. It emphasizes Wi-Fi networks' background, tools, standards, and applications. However, this research article's primary goal is to determine the numerous issues that arise due to the disposition of these WLANs and make references and recommendations to address these issues and reduce potential risk factors. The Zou, Yulong, et al [19] discussed this paper shows The Wi-Fi standards series, which commonly activate in the 2.4-GHz and 5.8- GHz ISM bands, supports many physical layers. The 5.8-GHz band is more frequently accessible, although it has a shorter radio range. Further modifications (a/b/g/n) indicate different stages in the evolution of the standard, which is primarily aimed toward provoking performance driven by a home and business networking conditions.

3. Methodology

It's vital to clarify some of the security concerns that WLANs face before looking at the security solutions available today. All LANs, whether wired or wireless, are vulnerable to two types of attacks.

- **Active:** Hackers get access to the local area network (LAN) to damage data. This includes DOS, Ad hoc networks, meddle, men, etc. To launch a DoS attack,

Ad hoc networks can be dangerous to your security. These are peer-to-peer networks that connect wireless computers without the use of an access point. A cyber-attack that necessitates the use of software packages and has the potential to inflict major disruption or data loss. To collect packets in transit, the hacker places oneself between an access point and a wireless device [5].

- **Passive:** Hackers obtain access to the LAN but can only listen in on transmitted data because hackers do not need a physical connection to the location. Wireless LANs are more vulnerable to both types of attacks. Passive aggression does not require the use of complex methods or tools. Inactive raid in its most common form. 802.11 networks' RF signal can travel outside of a building's limits [5].

Security protocols were created to provide Wi-Fi networks with authentication and encryption rather than just a wireless Internet connection. WPA2 was the most widely used security protocol in the past due to its high status of security and longevity on the market [6].

WPA 3 offers the best security to date while being a relatively new version that has yet to gain enough adoption. You can still find each protocol in specific modern devices even though WEP is no longer followed as a dependable security protocol and is not used in new devices [5,6].

4. Attack Flow

This section covers the central aggression a challenger can establish against a target customer on a Wi-Fi network with Wi-Fi Protected Access 2—Pre-Shared Key **(**WPA2-PSK) security. States, attacks, and outcomes are the three categories that make up the diagram. A state is a situation that an attacker is in when they can launch an assault or get the result they want. Attacks are typically used to transition between states, although it is also possible to do it directly. A state is a situation that an attacker is in when they can launch an assault or get the result they want. Attacks are typically used to transition between states, although it is also possible to do it directly. An attack is a behavior carried out by the adversary against the victim or AP to change states or realize a desired result [7]. A result is the attacker's evil intention, or, more specifically, what he or she intends to achieve.

4.1. State Join Network

In this case, the attacker can join the network as an authenticated client by entering the passphrase only after the critical acquisition state is reached in the state. From this point, an attacker can execute spoofing on the AP and network clients [8].

4.2. State Non-keyed AP session Hijacking

This state can only be attained through a rogue access point assault. A client's connection with a legitimate AP is seized so that the client thinks they are still talking to the AP when, in fact, they are connected to the attacker. Changing the channel is accomplished. In this instance, the attacker merely diverted the connection and is not aware of the key.

5. Proposed Solutions

Detection, Modification, and Destruction are three main dangers that arise from the nature of wireless communication. Followership is some security solution for dealing with the security attacks and risks mentioned above [9].

5.1. Signal Hiding Techniques

Various steps should be taken by organizations to make it more challenging for an attacker to find their wireless access points. Placement of wireless access points inside a structure, away from windows and exterior walls, disablement of SSID (service set identifier) transmission by wireless access points, provision of SSIDs with cryptic names, and lowering of signal strength to the lowest level still providing sufficient coverage are a few of these measures. Security can be increased by employing directional antennas and signal-shielding techniques [8,9].

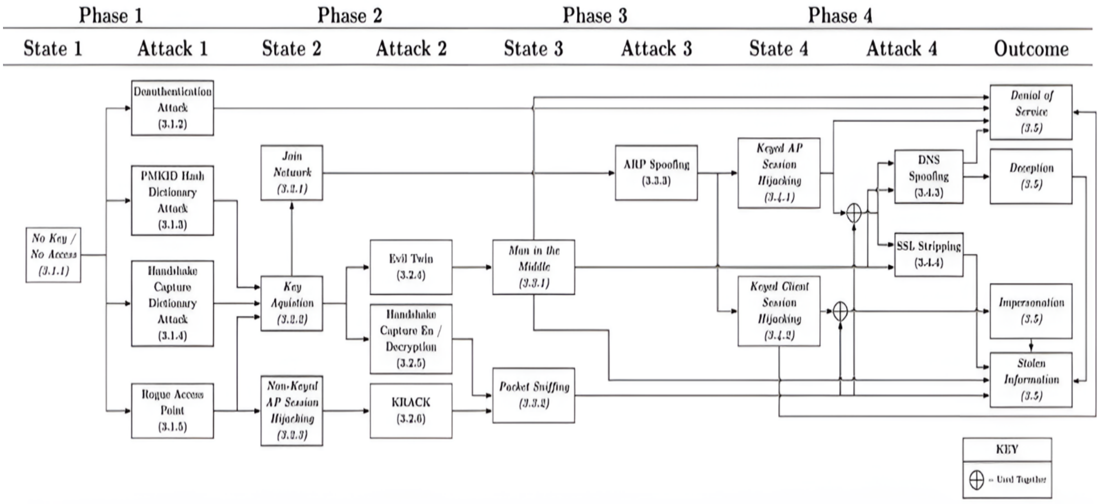

Figure 3. Attack flow diagram with corresponding section numbers [7].

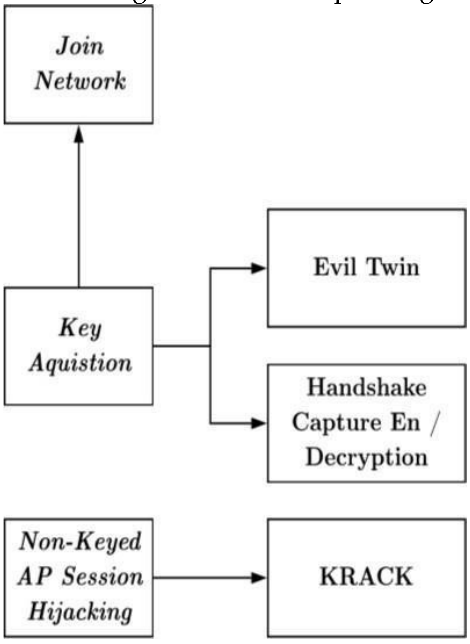
Join Network
Key Aquistion
Evil Twin
Handshake Capture En / Decryption
Non-Keyed AP Session Hijacking
KRACK

Figure 4. Session Hijacking [7].

5.2. Firewall

If your firewall was sent in the off mode, turn it on. Computers on wireless networks require some protection, just like any other device connected to the internet. Wireless networks simplify and ease the usage of everyday life, business, and communication. These networks do, however, carry the risk of losing private data and resulting in significant expenses. Malicious actors have recently developed their skills and exploited wireless network weaknesses to launch attacks, intercept important data, and enter systems without authorization [10]. Due to these behaviors, obtaining adequate security for wireless networks is far more challenging than it needs to be.

One of the numerous tactics created to attempt to ensure the security of data is the firewall, which has shown itself to be highly effective in safeguarding wireless networks. In order to reduce the risks associated with cyberthreats like eavesdropping, man-in-the-middle assaults, and denial-of-service (DoS) attacks, firewalls regulate data flow and stop illegal attempts to access private data. By outlining their primary roles, technical underpinnings, architectural models, and use in cloud-based wireless networks, this study aims to clarify the significance of firewalls for wireless network security [11]. Furthermore, we take into account network guardians against emerging threats and some of these measures in the framework of all-encompassing wireless security policies.

5.3. Encryption and Decryption

Encryption/decryption technology is one of the most efficient ways to safeguard wireless networks; most wireless devices have an encryption and decryption mechanism built-in. This technique encrypts plain text using encryption technology and then decrypts it at the destination, allowing your message to travel safely from sender to receiver [12].

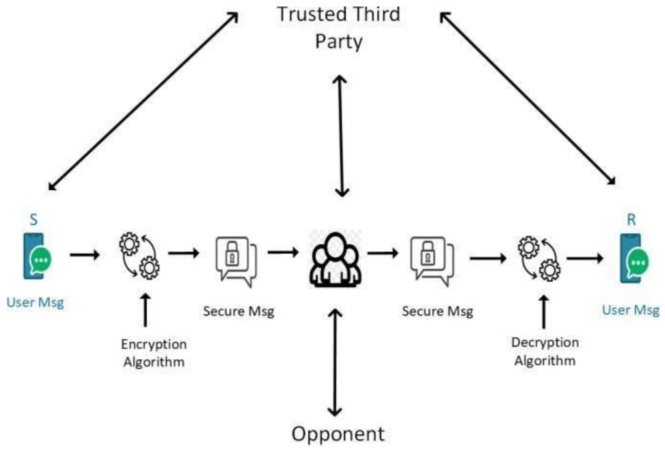

Figure 5. Network security model [12].

Many restaurants, hotels, airports, and other public places provide wireless connections to their clients, but there are exceptions. Some networks to breaking into your system and gain access to the data the information you're sending.

5.3.1. Temporal Key Integrity Protocol:

WPA employs the Temporal Key Integrity Protocol as an encryption mechanism. It fixes weaknesses in the 802.11 WEP encryption technologies and adds support for older network devices. It uses WEP proto col but encrypts Layer 2 data with TKIP and executes a message integrity check (MIC) on the encrypted packet to be sure it hasn't been tampered with [13].

5.3.2. Galois Counter Mode Protocol:

This is an encryption algorithm package that beats CCMP in terms of efficiency and security. GCMP is used by WPA3 [13].

5.3.3. Advanced Encryption Standard:

WPA2 uses the AES encryption algorithm. It's also the favored solution because it's a highly strong encryption system. The target hosts can check if the coded and no encrypted data have been tampered with using Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) [14].

5.4. Packet Sniffing

Hackers sometimes use two methods to track a company's network secretly. They can utilize a "sniffer" to manage all the information via a procedure without being detected [15]. This method is more brutal to notice when a company's network has many connections between devices.

5.5. Virtual Private Network (VPN)

Using a Virtual Private Network (VPN) is an effective way to shield your connection from packet sniffers and other online threats. Because a VPN encrypts traffic as it moves between your device and its destination, sensitive data is shielded from prying eyes. This encryption process applies to any data sent over the internet, including service requests, application messages, and website activities. Since the data is protected by a secure tunnel, a packet sniffer attempting to capture your traffic would only see encrypted data being delivered to your VPN provider. Without the necessary decryption keys, the contents of your communication would stay unintelligible, safeguarding your privacy and security [16]. The Security protocols such as OpenVPN, IPSec, and Wire guard are used by VPNs to guarantee confidentiality and integrity of the data. They prevent unwanted disclosure with tools such as AES-256 encryption, which is so strong that hackers or surveillance agencies cannot decipher transmitted data.

VPN security mechanisms can be fortified with multi-phase encryption schemes. In this case, attacking such data requires breaking multiple layers of security, which is impossible. Moreover, VPNs provide protection against man-in-the-middle (MITM) attackers who try to listen in on communications by capturing network traffic. VPNs, if configured correctly, provide overwhelming protection against these sorts of attacks by implementing authentication and secured key exchange. Furthermore, the document addresses how websites and online services cannot track users because VPNs replace a user's real IP address with one from the VPN server, providing anonymity [17].

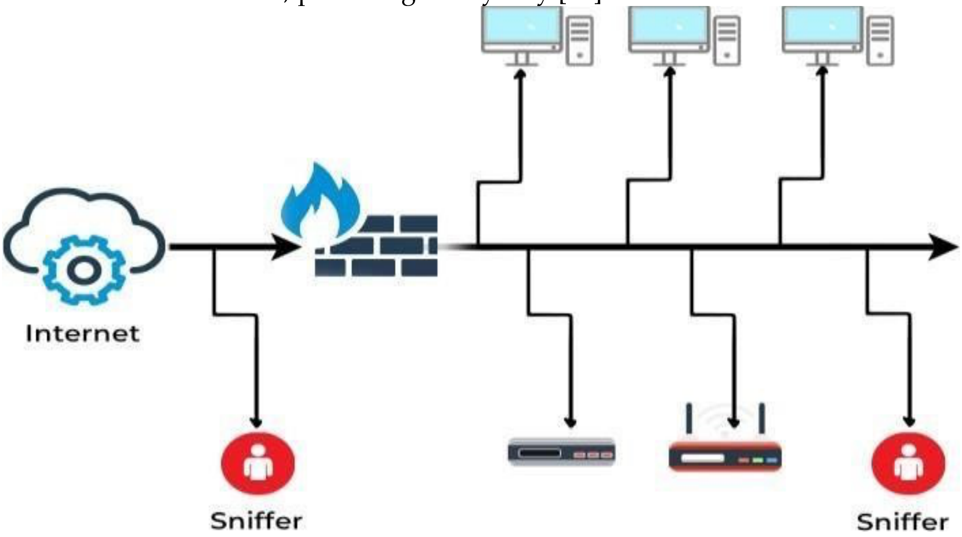

Figure 6. Packet Sniffing [15]

6. Comprehensive Review Table

Table 1. Comparative Review of Wireless Security Measures and Emerging Threats

Category	Key Points	Analysis	Impact	Recommendations
Main Focus	Networks remain protected from data breaches and unwanted access via wireless security.	covering significant dangers and solutions, but excluding future security trends.	Essential for protecting data integrity and network availability.	Expand on next-gen security like AI and quantum encryption.
Challenges	Unauthorized access, weak encryption, insider threats, packet sniffing.	Highlights common issues but needs more real-world cases.	Raises awareness of security risks in wireless environments.	Include technical mitigation strategies with examples.
Threats	Eavesdropping, MITM attacks, malware, rogue APs, DoS attacks.	Identifies major risks but lacks evolving threat analysis.	Crucial for cybersecurity planning in wireless networks.	Discuss AI-driven threat detection and IoT security risks.
Security Solutions	WPA2/WPA3 encryption, MFA, firewalls, IDPS, blockchain security.	Covers best practices but could explore emerging solutions.	enhances wireless security and defends against online attacks.	Compare security protocols and discuss future-proof solutions.
Strengths	Well-structured, covers threats and solutions effectively.	Provides a good foundation but needs deeper analysis.	Useful for IT professionals, businesses, and network admins.	Add case studies and advanced security techniques.

Weaknesses	Lacks real-world examples and advanced security trends.	Could improve clarity and depth in technical areas.	Limits deeper understanding for security professionals.	Include comparisons, future security innovations, and technical details.
Conclusion	Authentication, encryption, and proactive protections are the foundation of wireless security.	Strong summary but should address future challenges.	Reinforces the need for continuous security updates.	Discuss emerging threats like AI-based cyberattacks.

7. Conclusion

Wi-Fi connections are contained in wireless security, which protects from unauthorized users or loss of tools or data. Another word is defending the wireless connection from attackers seeking to compromise its confidentiality, integrity, or availability—Wi-Fi security guards' wireless connectivity. Wireless dangers can occur for many reasons, from someone connecting to your Despite user consent, an access point decodes packets from the air using a packet sniffer. Many wireless customers know the risks of joining a WAP to their wired connection. Protocols WEP, WPA, WPA2, and now WPA3 safeguard your conversations, hide your data, and deter hackers from accessing your network. WPA2 is generally the best option, even though it uses more processing power to secure your network. Others are technical solutions for wireless security risks like authentication and data encryption. These solutions are best practices for any networking environment, such as intrusion detection, firewalls, and content filtering. Adequate network security operating firewalls must be shown in the future. Although monitoring the entire network will be tough, I declare that data protection be implemented at the media gateway. This helps decrease the costs that many businesses are currently facing. With technological advancement, attackers may find another way to breach security, so we will further study more methods to secure communications

References

1. MaxxSouth Broadband. (n.d.). How to secure and configure WIFI ? MaxxSouth Broadband Blog. from https://www.maxxsouth.com/maxxcommunity/how-to-connect-your-device-to-wifi
2. Nazir, Rashid & Laghari, Asif & Kumar, Kamlesh & David, Shibin & Ali, Munwar. Survey on Wireless Network Security. Archives of Computational Methods in Engineering. 29. 10.1007/s11831-021-09631-5. (2021).
3. A. Kavianpour and M. C. Anderson, "An Overview of Wireless Network Security," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA,, pp. 306-309, doi: 10.1109/CSCloud.2017.45. (2017)
4. Emilselvan, G.s.r & Gayathri, Nuka & Kumar, S & Rai, Ankush & Kannan, Raju. ADVANCED ENCRYPTION AND EXTENDED AUTHENTICATION FOR WIRELESS LAN. Asian Journal of Pharmaceutical and Clinical Research. 10. 441. 10.22159/ajpcr.2017.v10s1.19987. (2017).
5. Ee, Sun & Ming, Jeshua & Yap, Jia & Lee, Scott & Tuz Zahra, Fatima. Active and Passive Security Attacks in Wireless Networks and Prevention Techniques. 10.36227/techrxiv.12972857. (2020).
6. Eian, Isaac & Lim, Ka & Yeap, Majesty & Yeo, Hui & Z, Fatima. Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges. 10.20944/preprints202010.0018.v1. (2020).
7. Kohlios, Christopher & Hayajneh, Thaier. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics. 7. 284. 10.3390/electronics7110284. (2018).
8. Kirti Kaushik and Nidhi Sewall. "a research paper on security of wireless network." International Journal of Advance Research (2019).
9. Chap18.Wireless Network Security. JeongKyu Lee. Email: jungkyu21@seoultech.ac.kr. SeoulTech UCS Lab. 2015-1st. Page 2. Table of Contents. 18.1 Wireless Security
10. Wang, Peihong. “Research on firewall technology and its application in computer network security strategy.” Frontiers in Computing and Intelligent Systems. 2. 42-46. 10.54097/fcis.v2i2.3931. (2022).
11. Karygiannis, Tom, and Les Owens. Wireless Network Security: US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2021.
12. Lakhtaria, Kamaljit. “Protecting Computer Network with Encryption Technique: A Study.” 381-390. 10.1007/978-3-642-20998-7_47. (2011).
13. Doomun, Razvi & Soyjaudah, K.M.s. “Modified Temporal Key Integrity Protocol For Efficient Wireless Network Security”. (2012).
14. Burg, Andreas, Anupam Chattopadhyay, and Kwok-Yan Lam. "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things." Proceedings of the IEEE 106.1 (2017): 38-60.
15. B, Prabadevi & Nagamalai, Jeyanthi. “A Review on Various Sniffing Attacks and its Mitigation Techniques.” Indonesian Journal of Electrical Engineering and Computer Science. 12. 1117-1125. 10.11591/ijeecs.v12.i3.pp1117-1125. (2018).
16. Forbacha, Suh & Agwu, Mbuya.Design. “Implementation of a Secure Virtual Private Network Over an Open Network (Internet)”. American Journal of Technology. 2. 1-36. 10.58425/ajt.v2i1.134. (2023).
17. J. Smith and A. Doe, "Securing IEEE 802.11g WLAN using OpenVPN and its impact analysis," International Journal of Network Security, vol. 15, no. 3, pp. 45-60. (2020)
18. Kibona, Lusekelo, and Hassana Agname. "Wireless Network Security: Challenges, Threats and Solutions. A Critical Review." International Journal of Academic Multidisciplinary Research (IJAMR) 4.2 (2018).
19. Zou, Yulong, et al. "A survey on wireless security: Technical challenges, recent advances, and future trends." Proceedings of the IEEE 104.9 (2019): 1727-1765.