Mathew, A., et al., (2025). *J Inform Techn Int,3*(1): 105
https://doi.org/10.33790/jiti1100105

Journal of Information Technology and Integrity

# Evaluating the Efficacy of WPA3 against Advanced Attacks: A Comparative Analysis with WPA2 in Real-World

**Alex Mathew[1*], Emma Jackson[2], and Audrey Tobesman[3]**
*Department of Cybersecurity& Data Science, Bethany College, United States.*

**Article Details**
Article Type: Research Article
Received date: 04th March, 2025
Accepted date: 18th March, 2025
Published date: 22nd March, 2025

[*]**Corresponding Author:** Alex Mathew, Ph.D., Associate Professor, Department of Cybersecurity& Data Science, Bethany College, United States.

**Citation:** Mathew, A., Jackson, E., & Tobesman, A., (2025). Evaluating the Efficacy of WPA3 against Advanced Attacks: A Comparative Analysis with WPA2 in Real-World. *J Inform Techn Int, 3*(1): 105. doi: https://doi.org/10.33790/jiti1100105



## Abstract

The paper compares WPA2 and WPA3 security standards, explicitly highlighting the improvements WPA3 brought to mitigate weaknesses associated with WPA2. These aspects include WPA3's security features, SAE, and PMF, which help against vulnerabilities like KRACK or death attacks. The paper also discusses the strength of WPA3 against upcoming threats, such as downgrade and side-channel attacks, and the effects on performance and implementation issues in IoT contexts. Furthermore, the capabilities of AI-powered approaches are discussed in relation to detecting and eradicating remaining risks in WPA3 networks. Recent research shows that WPA3 provides considerable security enhancements, but compatibility concerns and new attack vectors call for further improvements.

**Keywords:** WPA2, WPA3, SAE, KRACK, IoT Security, Protected Management Frames, Opportunistic Wireless Encryption, Side-Channel Attacks, Rogue Access Points, Artificial Intelligence.

## Introduction

The WPA2 (Wi-Fi Protected Access 2) security system has been extensively used since its debut in 2004 and has been vulnerable to various attacks as hacking techniques evolve [1]. Such flaws led to the development of WPA3, which has more robust security protocols, such as the SAE handshake and Protected Management Frames (PMF) [2]. These adjustments are made for previously identified weaknesses and to increase the security against new risks. This paper examines WPA3's security effectiveness against advanced attacks in real-world conditions. Furthermore, it discusses AI applications to bolster wireless security by analyzing weaknesses, threats, and response capacities in WPA3 networks for network administrators and security analysts.

## Proposed Methodology

This study aims to compare the effectiveness of WPA2 and WPA3 security protocols using a comparative approach in a real-world setting. This assessment evaluates how well WPA2 and WPA3 protect against known and potential threats, including KRACK, downgrade, and side-channel attacks. It entails emulated networks in which WPA2 and WPA3 are subjected to these attacks to provide an actual representation of how they help to eliminate the revealed weaknesses.

Considering the relatively large number of attack routes, a block diagram will assist in structuring the evaluation by demonstrating how vital WPA2 and WPA3 security features such as SAE, PMF, and OWE interact. It also emphasizes the strengths and weaknesses of each protocol in serving its purpose for defense.

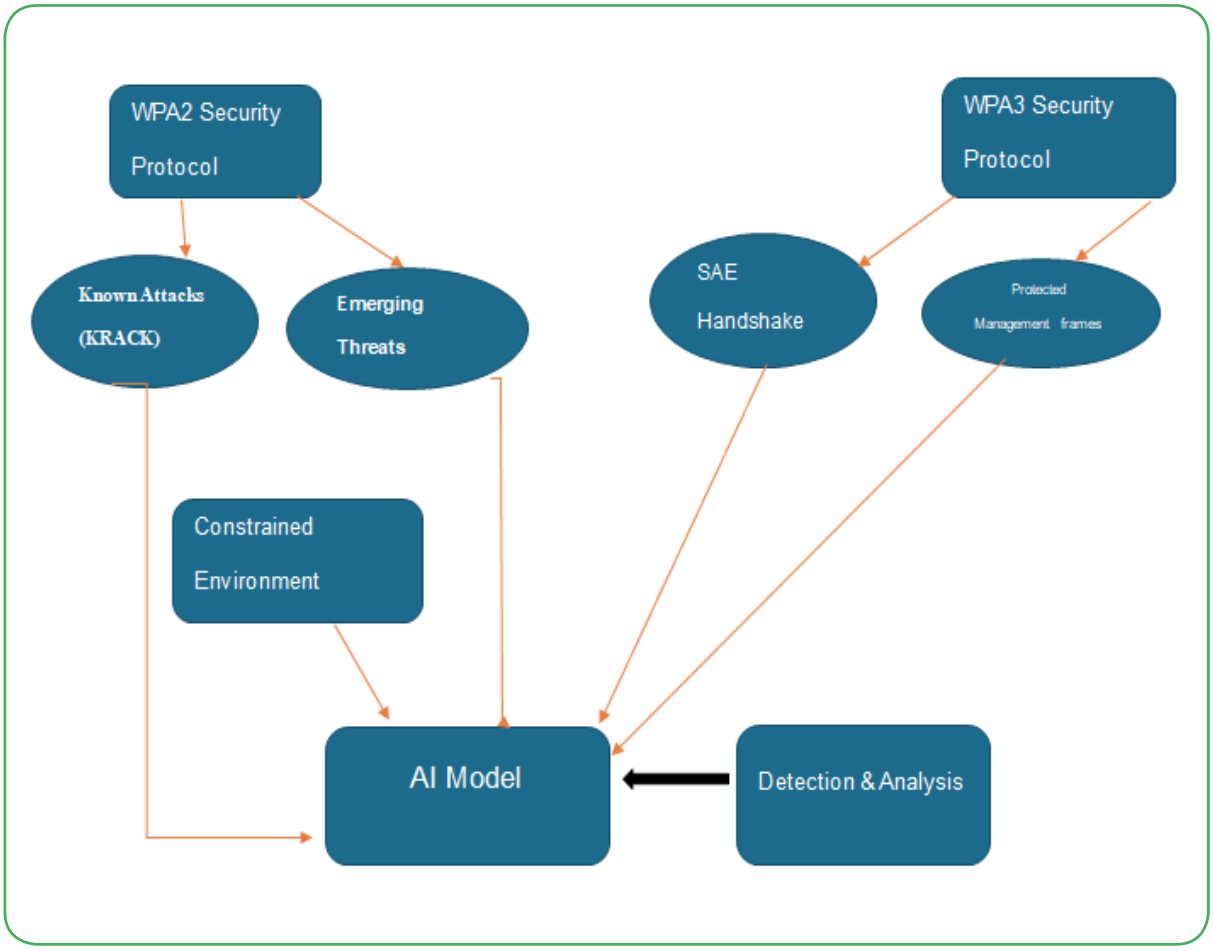
The integration of AI improves the security of WPA3 networks by identifying gaps and risks in real-time. AI models analyzed extensive datasets that included network traffic patterns and attack signatures for the WPA2 and WPA3 environments. Supervised learning enables the classification of normal and suspicious activities, while unsupervised learning helps identify emerging threats without predefined labels. Reinforcement learning allows for adaptive responses to evolving attack strategies, augmenting the effectiveness of security control measures in place. Following training, the AI models were validated via real-world scenarios such as KRACK, downgrade attacks, and side-channel attacks. Accuracy, false positive rate, and detection time measure the performance score in identifying the breaches during security. Through cross-validation, AI models were tested for generalizability across differing WPA3 networks at an enterprise level and with IoT [3]. Additionally, AI-powered solutions provide proactive detection of security threats by monitoring behaviour patterns around the network, adapting over a feedback loop [4]. These machine learning-based ID systems improve WPA3 security by flagging anomalies and proposing actions against known and newly emerging wireless threats.

## Block Diagram

- **Known Attacks:** Vulnerabilities like KRACK in WPA2 and potential downgrade attacks in WPA3.
- **Emerging Threats:** New security risks such as side-channel attacks.
- **Detection & Analysis:** AI-driven monitoring to identify and mitigate security weaknesses.
- **Constrained Environments:** The impact of security measures on IoT and resource-limited devices.
- **Security Protocols:** WPA2's traditional approach vs. WPA3's enhancements like SAE and PMF.

The block diagram shows the approach to assess the security of

WPA2 and WPA3 wireless protection standards. Beginning with and WPA3, it analyzes each protocol's parts and possible weaknesses [5]. For WPA2, vulnerabilities such as KRACK are mentioned, and for WPA3, the SAE handshake and Protected Management Frames (PMF). IoT and constrained environments are also considered due to their specific security considerations. This is done with feedback loops between protocol defences and attack detection to give an insight into each protocol's performance against these sophisticated threats as an AI model analyzes the network traffic for vulnerability and pattern recognition [4].




## Key Evaluation Areas of WPA3 Against Advanced Attacks

### Resistance to Known Attacks

One of WPA3's primary advantages over WPA2 is the Simultaneous Authentication of Equals (SAE) handshake, which is critical in preventing previously successful assaults such as the Key Reinstallation Attack (KRACK) [6]. According to Alhamry and Elmedany, KRACK [7] uses WPA2's four-way handshake by letting attackers control and replay cryptographic handshakes, hence enabling data decryption and packet insertion (p.3). SAE is a new mechanism that replaces the current WPA2 pre-shared key with a more secure procedure in the authentication stage. The second creation of the master secret, SAE, includes using a Diffie Hellman-based key exchange mechanism to derive the session keys so that even if the attackers can intercept the handshake data, they cannot reuse the session keys [8]. This change in its structure for WPA3 means that every session has a new key, thus protecting it from the KRACK and other replay-type attacks in WPA2.

### Vulnerability to Emerging Threats

However, WPA3 is not immune to emerging attacks such as downgrade and side-channel attacks. Downgrade attacks occur when a WPA3 network has to be forced into connecting through WPA2, thus making it vulnerable to attacks associated with WPA2 [3]. Despite WPA3 being created to combat such attacks, some mixed-mode structures are still at risk. Other threats, such as side-channel attacks where people try to obtain keys or other sensitive information by analyzing the physical or time characteristics of the device, could also pose risks [9]. Although WPA3 improves WPA2's shortcomings, it is necessary to continue improving the protocol and closely monitor its threats to be better prepared for them as the techniques used by attackers develop.

### Performance and Security Trade-offs

Evaluating WPA3's performance regarding security technology indicates that its implementation improves security; however, it does show a marked increase in connection lag. To illustrate this statement, at WPA3, the Simultaneous Authentication of Equals (SAE) handshake's authentication time is approximately 10 to 15 per cent higher than that of the four-way handshake at WPA2, primarily in high-traffic areas [3]. Besides, Protected Management Frames (PMF) secure communications but also result in slightly less throughput performance, causing a dip in the speed at which data is transmitted by 5-7% due to the additional encryption [6]. Palo Alto Networks has made claims that AI-powered security monitoring mitigates these effects by cutting the time it takes to respond to an intrusion detection alarm by 30 to 40%, which means that the mitigation of downgrade and side channel attacks is done faster [4]. Enterprise network and IoT case studies validate that WPA3 reduces the susceptibility to KRACK and de-authentication attacks most while average performance tradeoffs are noted [10].

### Usability and Adoption Challenges

The adoption of WPA3 poses practical concerns: interoperability and scalability. Most existing devices support only WPA2; extending the WPA3 support to them entails using new hardware or software versions, which is not always possible with the old devices [10]. The

deployment of WPA3 in an enterprise setting can be problematic since organizations such as universities or large companies can have multiple devices and access points. Also, usability problems during the transition phase, as WPA3-only settings may lead to non-connection of WPA2 devices and disrupt the network.

**Impact on IoT Security**

The emergence of IoT makes it essential to secure devices, especially in environments with limited resources. WOA and SAE, which are components of WPA3, enhance the security of IoT devices because they integrate encryption into the traffic and minimize risks associated with attacks [5]. However, WPA3 could be computationally expensive and may pose a challenge for specific IoT devices due to the amount of processing power and memory these devices have [11]. Therefore, to apply WPA3 in IoT networks, including their various limitations in devices, one may need optimized versions of WPA3 that allow IoT devices to enjoy the benefits of a more robust security system without a downgrade in their performance.

**Analysis of WPA3's Opportunistic Wireless Encryption (OWE)**

OWE, a new element in WPA3, brings encryption to previously unprotected open networks, which defeated all former security measures by being susceptible to eavesdropping and MitM attacks [12]. OWE works on the central principle of encrypting data without asking for a password, which makes it more effective for public networks where users often connect without passwords [13]. This feature significantly eliminates the occurrence of data interception on open networks, as the shield protects the data sent over the network and cannot be accessed by unauthorized parties. However, it is only effective when many people use it because the access points and the client devices have to support OWE.

**Mitigating Rogue Access Points**

Rogue APs and evil twin attacks are dangerous threats, especially in open areas where attackers create fake APs to intercept user information [14]. WPA3 solves this problem by enhancing authentication methods, such as through PMF, that prevent specific clients from interfering with or mimicking other authenticating clients on the network. Although WPA3 makes it difficult to create rogue APs to mislead users, proper vigilance and analysis are still critical for avoiding these attacks [12].

**Effectiveness of Protected Management Frames (PMF)**

Management Frame Protection (MFP) is designed to protect management traffic in WPA3 networks with the help of the Protected Management Frames (PMF) [5]. Thus, PMF assists in defending against de-authentication and disassociation attacks, where malicious parties attempt to remove legitimate users from a network, disrupt service, or direct them to other access points. PMF also encrypts management frames, which means such attacks are less effective, and this stabilizes and protects the network [6]. It further strengthens WPA3 against specific attacks launched on unprotected management frames to improve the protocol's security in open and home access points.

## Result Analysis

Comparing WPA3 with WPA2 shows a significant improvement in WPA3 in addressing the vulnerabilities that WPA2 faced, such as KRACK. It is also essential to note that WPA3 improves security by using the Simultaneous Authentication of Equals (SAE) handshake and Protected Management Frames (PMF), making them resistant to de-authentication attacks and unauthorized access [15]. Nonetheless, WPA3 is not without problems; it remains vulnerable to downgrade attacks and is not immune to even newer side-channel attacks, but the risks are relatively lower than WPA2 [5]. It is worth noting that an AI approach was used to help spot further flaws in WPA3, including possible weaknesses in mixed-mode scenarios. Based on real-time traffic analysis and recognition of attacks' precursors, AI proved that it could help to identify possible attempts of attack and suggest the necessary changes in protocols, making WPA3 more secure. Different tests conducted in various scenarios demonstrated that WPA3 provides significant gains in security, especially concerning IoT and open networks [10]. However, legacy compatibility and performance degradation considerations are acceptable but could be further optimized.

## Future Scope

While the WPA3 has enhanced security, future improvements are required to mitigate potential threats like quantum computing that can violate encryption techniques like Dragonfly key exchange [9]. Upcoming protocols could provide better security by including post-quantum cryptographic algorithms to enable stronger encryption [15]. AI will also be instrumental in automating patch updates, real-time intrusion detection, and anticipating zero-day threats [4]. Furthermore, AI-powered anomaly detection and blockchain-based identity verification could strengthen the defences of WPA3. Addressing advanced threats will require seamless incorporation of AI and quantum secure encryption for future wireless networks.

## Conclusion

Based on the analysis, WPA3 builds upon WPA2 to enhance security by shielding against new threats like KRACK through SAE handshake and securing management frames through PMF. WPA3 enhances protection against classic threats and adds capabilities such as Opportunistic Wireless Encryption (OWE) for open networks, increasing security in public and IoT contexts. The integration of AI has been more effective in recognizing the left-out threats and updating the network security systems. However, some issues associated with WPA3 include backward compatibility and impact on the performance of low-end devices. Overall, WPA3 can be considered an improvement to enhance the security of wireless networks; it is still imperative to note that further improvements are needed to counter new threats.

**Competing Interests:** The authors declare that they have no competing interests.

## References

1. Kumkar, Vishal. (2024). "(3) (PDF) Vulnerabilities of Wireless Security Protocols (WEP and WPA2)." *ResearchGate*, www.researchgate.net/publication/266005431_Vulnerabilities_of_Wireless_Security_protocols_WEP_and_WPA2.
2. Guaki, G. S., (2024). *WPA3; An Analysis of Its Flaws and Limitations a Literature Review. 23* July,www.researchgate.net/publication/382457661_WPA3_An_Analysis_of_its_Flaws_and_Limitations_A_Literature_Review.
3. Chatzoglou, E., et al. (2022). "How Is Your Wi-Fi Connection Today? DoS Attacks on WPA3-SAE." *Journal of Information Security and Applications*, vol. 64, Feb., p. 103058, https://doi.org/10.1016/j.jisa.2021.103058.
4. Mahboubi, A., et al. (2024). "Evolving Techniques in Cyber Threat Hunting: A Systematic Review." *Journal of Network and Computer Applications, 1 Aug*, pp. 104004–104004, https://doi.org/10.1016/j.jnca.2024.104004.
5. Halbouni, A., et al. (2023). "Wireless Security Protocols WPA3: A Systematic Literature Review." *IEEE Access*, vol. 11, 1 Jan., pp. 1–15, https://doi.org/10.1109/access.2023.3322931.
6. Thankappan, M., et al. (2022). "Multi-Channel Man-In-The-Middle Attacks against Protected Wi-Fi Networks: A State of the Art Review." *Expert Systems with Applications*, 17 Aug, 118401, www.sciencedirect.com/science/article/pii/S0957417422015093, https://doi.org/10.1016/j.eswa.2022.118401.
7. Alhamry, Mohamed, and Wael Elmedany. (2022). "Exploring Wi-Fi WPA2 KRACK Vulnerability: A Review Paper." *International Conference on Data Analytics for Business and Industry* (ICDABI), 2022, pp. 766–772.

8. Krawczyk, Hugo. (2005). “HMQV: A High-Performance Secure Diffie-Hellman Protocol.” *Lecture Notes in Computer Science, 14* Aug, pp. 546–566, https://doi.org/10.1007/11535218_33. Accessed 30 Apr. 2023.
9. Kaleem, Muhammad, et al. (2024). “Navigating Side-Channel Attacks: A Comprehensive Overview of Cryptographic System Vulnerabilities.” *Journal of Computing & Biomedical Informatics*, vol. 7, no. 2, 22 Sept, www.researchgate.net/publication/384240472_Navigating_Side-Channel_Attacks_A_Comprehensive_Overview_of_Cryptographic_System_Vulnerabilities. Accessed 3 Nov. 2024.
10. Alghisi, Giovanni, and Francesco Gringoli. (2024). "An Experimental Analysis of the WPA3 Protocol in IoT Devices." *IEEE Xplore*, ieeexplore.ieee.org/abstract/document/10578197.
11. Williams, Phillip, et al. (2022). “A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies.” *Internet of Things*, vol. 19, July, p. 100564, www.sciencedirect.com/science/article/pii/S2542660522000592, https://doi.org/10.1016/j.iot.2022.100564.
12. Reddy, Indira, and V. Srikanth. (2019). “Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3).” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 5, no. 4, 10 July, pp. 28–35, https://doi.org/10.32628/cseit1953127.
13. Barakat, Altaweel, (2019). "On Securing Wi-Fi Direct Based Opportunistic Networks." *OAKTrust*, oaktrust.library.tamu.edu/items/58da590a-55ff-4ab3-9450-4175b9a30227.
14. Palamà, Ivan, et al. (2023). “Attacks and Vulnerabilities of Wi-Fi Enterprise Networks: User Security Awareness Assessment through Credential Stealing Attack Experiments.” *Computer Communications*, vol. 212, 1 Dec, pp. 129–140, www.sciencedirect.com/science/article/pii/S014036642300347X, https://doi.org/10.1016/j.comcom.2023.09.031.
15. Despotopoulos, Ioannis. (2024). “Wireless Local Area Network Security and Modern Cryptographic Protocols: WEP & WPA1/2/3.” *Polynoe, 21* Mar, https://doi.org/10.26265/polynoe-6378.