Indian Engineering Journal
ISSN: 2984-9047
Vol 4 Issue 1 (2026)

Enhancing Wireless Privacy Safeguarding Through WPA3

[1]Mrs.V. Selvi, [2]Mr.R.Sankarasubramanian,

[1]Research Scholar, Department of Computer Science,Erode Arts and Science College,Erode,TamilNadu.

vpsandeesh@gmail.com

[2]Principal & Associate Professor, Department of Computer Science,Erode Arts and Science College,Erode,TamilNadu.

Abstract

Wireless communication has become an essential component of modern digital systems, supporting internet access, smart devices, online education, banking, healthcare, and industrial applications. However, increasing wireless connectivity has also introduced several security and privacy challenges. Traditional wireless security protocols such as WEP and WPA2 suffer from weaknesses including password attacks, unauthorized access, and limited privacy protection. To overcome these issues, WPA3 was introduced as an advanced wireless security protocol with stronger authentication and encryption mechanisms. This research paper focuses on the role of WPA3 in enhancing wireless privacy safeguarding and security for users. The study analyzes important WPA3 features including Simultaneous Authentication of Equals (SAE), forward secrecy, protected management frames, and enhanced encryption techniques. The paper also compares WPA3 with earlier wireless security protocols to evaluate improvements in privacy preservation, authentication, and network reliability. The results show that WPA3 significantly improves wireless communication security and provides better protection against cyber threats and unauthorized access.

Keywords: WPA3, Wi-Fi Security, Privacy Safeguarding, Human-Focused Protection, Simultaneous Authentication of Equals (SAE), Secure Network Communication, Information Security, Data Privacy, Wireless Encryption, Network Confidentiality.

1. Introduction

The continuous growth of wireless communication technologies has significantly changed the way people access and utilize digital services by enabling fast connectivity, flexible communication, and efficient information sharing. Wireless networks are commonly used in various sectors such as education, healthcare, banking, smart homes, industries, and business organizations. As users increasingly depend on wireless systems for transferring confidential data, performing online transactions, and exchanging personal information, maintaining strong security and privacy safeguarding has become extremely important.

To strengthen wireless network security, the Wi-Fi Alliance introduced Wi-Fi Protected Access 3 (WPA3) as an improved wireless security standard. WPA3 was developed to overcome the security weaknesses present in earlier protocols and to provide better privacy-oriented protection for users. In comparison with WPA2, which mainly depended on pre-shared key authentication and was vulnerable to several security attacks, WPA3 offers advanced authentication and encryption techniques. The implementation of Simultaneous Authentication of Equals (SAE) in WPA3 improves password security and minimizes the possibility of offline dictionary attacks and unauthorized network access.

With the rapid evolution of cyber threats and attack mechanisms, traditional wireless security protocols are no longer sufficient to guarantee complete privacy protection. Although WPA2 delivered acceptable security during earlier networking environments, modern wireless systems require stronger security mechanisms because of increased computational capabilities, advanced hacking methods, and growing privacy concerns. Many wireless networks still rely on outdated protection protocols, which expose users to risks such as data theft, traffic interception, identity disclosure, and privacy breaches by malicious attackers.

This research paper concentrates on evaluating the effectiveness of WPA3 in enhancing wireless privacy and secure communication. The study examines major WPA3 security components including SAE authentication,

forward secrecy, advanced encryption methods, and protected management frames. Furthermore, the paper compares WPA3 with older wireless security standards to identify improvements in authentication security, confidentiality, attack resistance, and user privacy protection. The analysis demonstrates that WPA3 provides enhanced wireless protection and serves as a reliable solution for secure and privacy-focused wireless networking environments.

1.1 Research Issue

Although Wi-Fi Protected Access 3 provides advanced wireless protection features, there is still insufficient practical evidence regarding how efficiently it safeguards user privacy in real-time wireless communication systems. This concern is especially important in risky environments such as public Wi-Fi hotspots, where users are more susceptible to unauthorized access, privacy attacks, and data exposure.

2. Case Analysis: University Campus Public Wireless Network

Metropolitan University is a major public educational institution operating across multiple campuses and serving nearly 20,000 students, staff members, and teaching professionals. The university's large-scale wireless communication infrastructure supports personal interaction, administrative activities, and academic operations. Sensitive information transmitted through this network includes student databases, research documents, confidential messages, financial records, and secured educational resources (Aslan et al., 2023). The institution's information technology department identified significant privacy and security concerns among students, employees, and visitors using the openly accessible campus Wi-Fi services. These issues include unauthorized access to personal devices, password theft, monitoring of private communications, and possible exposure of confidential information, which may simultaneously affect thousands of users connected to the network (Palamà et al., 2023).

2.1 Drawbacks of the Current Wireless Protection System

2.1.1 Human-Oriented Security Concerns in the Current WPA2 System

• Common Encryption Credential Weakness:

When devices connected to the same Wi-Fi Protected Access 2 network become breached, attackers may gain the capability to interpret or access the communications of other connected users because identical encryption credentials are shared among all users linked to the same wireless access point (Pattnaik, Li & Nurse, 2024). As private communications are not completely isolated from other network participants, this situation represents a significant threat to user confidentiality and personal privacy.

• Limitations of Password-Oriented Authentication:

Because Wi-Fi Protected Access 2 mainly depends on shared secret credentials for authentication, the wireless environment remains vulnerable to offline dictionary-based intrusions. In these attacks, cybercriminals may intercept authentication handshake data and repeatedly test password combinations without the knowledge of the network administration system (Szymoniak, 2024). This security flaw directly threatens user confidentiality, since a successful intrusion can grant unrestricted availability to all communications transmitted through the network.

• Insufficient Separation Between Connected Devices:

In densely populated locations such as university campuses, the absence of effective device segregation may permit lateral access between systems connected to the same wireless infrastructure. This weakness can enable cyber attackers to obtain confidential data stored on portable computers, smartphones, and tablet devices linked to the network environment (Danekula, 2025).

2.1.2 Assessment of User-Centred Impact

Privacy-related breaches within this wireless communication environment can directly affect individual users. Students, academic professionals, and administrative employees who utilize personal electronic mail services,

along with users transferring research-related information, may become vulnerable to the exposure of confidential data. Apart from immediate information security concerns, such privacy incidents may also create psychological consequences that decrease user participation in online educational platforms and reduce confidence in institutional digital service infrastructures.

The case analysis demonstrates the urgent necessity for advanced wireless protection mechanisms capable of safeguarding user confidentiality while allowing legitimate users to maintain continuous network connectivity. The transition from Wi-Fi Protected Access 2 to Wi-Fi Protected Access 3 offers an effective experimental environment for analysing human-focused privacy enhancement mechanisms.

3. Background

3.1 Evolution of Wireless Security Protocols

Since the emergence of wireless communication technology, which has become increasingly important in everyday activities, addressing user privacy and cybersecurity concerns has remained a major focus in the design of wireless protection standards (Hughes-Lartey et al., 2021). The progression toward the Wi-Fi Protected Access 3 standard demonstrates a continuous attempt to maintain an effective balance between protection mechanisms, operational convenience, and end-user confidentiality. This advancement evolved through earlier wireless protection technologies, including Wired Equivalent Privacy, WPA, and Wi-Fi Protected Access 2.

The earliest wireless protection mechanism, WEP, contained major cryptographic vulnerabilities that enabled attackers to easily monitor and intercept private user communications (Mallick & Nath, 2024). Although the later WPA framework introduced the Temporal Key Integrity Protocol to overcome several WEP-related weaknesses, it still contained important security deficiencies that negatively affected user confidentiality in both public and enterprise wireless environments.

3.2 Limitations and Privacy Challenges of WPA2

Although Wi-Fi Protected Access 2 delivers major security improvements compared with earlier wireless protection mechanisms, it still contains several weaknesses that may directly threaten user confidentiality and data privacy (Chaudhary & Kumar, 2024).

• Shared Encryption-Key Structure:

The implementation of common encryption credentials within WPA2 creates an eenvironment where every connected participant utilizes identical cryptographic information, leading to major privacy-related concerns. Consequently, if any connected system becomes compromised, the communications of all users within the same network may become exposed to security risks (Moissinac et al., 2021).

• Exposure to Offline Dictionary-Based Intrusions:

During the WPA2 authentication handshake procedure, cyber attackers may capture verification packets and conduct offline password-guessing attacks without being identified by the network. Since many users prefer simple or predictable passwords, wireless environments remain susceptible to organised password-cracking attempts (Zaidan, 2021).

3.3 WPA3 Framework and Enhancements in Privacy Protection

Wi-Fi Protected Access 3 introduces multiple advanced mechanisms focused on strengthening privacy and confidentiality for wireless network users.

3.3.1 Simultaneous Authentication of Equals (SAE)

By replacing the weaker authentication handshake mechanism used in Wi-Fi Protected Access 2 with a more secure verification approach, SAE represents a major advancement in wireless authentication technology (Qi, Hu,

& Tai, 2024). SAE prevents offline dictionary-based intrusions through a protected password-to-key generation process that requires active participation from the network during authentication.

A major user-oriented benefit of SAE is its capability to maintain strong protection even when individuals select weak or predictable passwords, which commonly occurs in practical environments (Alghisi & Gringoli, 2024). Since SAE requires active authentication attempts, unauthorized password-cracking activities become significantly more difficult and easier to detect, thereby improving user privacy and communication security.

3.3.2 Personalized Data Encryption Mechanism

WPA3 improves wireless protection by assigning unique cryptographic credentials for every user communication session through individualized data encryption techniques (Bartoli, 2020). This enhancement successfully addresses the shared encryption weakness found in WPA2 by ensuring separate privacy protection among users connected to the same wireless environment.

From a user-centred perspective, this development significantly improves personal confidentiality because if one system or account becomes compromised, the communications and privacy of other network participants are less likely to be affected (Mahlake et al., 2023).

3.3.3 Protected Open Wireless Networks

Opportunistic Wireless Encryption is a security capability introduced within WPA3 that enables encrypted communication across open wireless networks without requiring conventional authentication procedures (Moissinac et al., 2021). This functionality benefits users by offering an additional level of privacy protection in public hotspots and other unrestricted wireless environments where confidentiality has traditionally been limited.

3.4 Deployment Challenges and User-Related Factors

Although WPA3 provides stronger privacy protection, its deployment also introduces several challenges that directly affect end users.

• Compatibility with Older Devices:

Many existing legacy systems do not fully support WPA3 technologies, creating a requirement for careful assessment before transitioning from WPA2 to WPA3 (Mathew, Jackson, & Tobesman, 2025). Users operating outdated hardware may need to connect through less secure network segments, increasing potential privacy and security risks.

• Processing and Performance Demands:

The advanced protection mechanisms integrated within WPA3 require increased computational resources, which may reduce communication performance and network speed in resource-constrained devices commonly used by individual users (Sagers, 2021).

• Difficulty in Network Configuration:

Network administrators must carefully balance usability and security while configuring WPA3 settings. Excessively complicated configurations may confuse users and encourage unsafe alternative practices that could weaken overall system protection (Agboola, Adegede, & Jacob, 2024).

• Weaknesses in Forward Secrecy Protection :

WPA2 does not fully support perfect forward secrecy, meaning that previously stored communication data may become vulnerable if encryption keys are compromised in the future.3.5 Comparative Evaluation of Security Performance

3.5 Comparitive Security Evaluation:

Experimental assessments of Wi-Fi Protected Access 2 and Wi-Fi Protected Access 3 implementation indicate a substantial enhancement in confidentiality protection (Mathew, Jackson & Tobesman, 2025). With proper

configuration, WPA3 wireless environments can decrease successful interception attacks by nearly 87% while completely preventing offline password-cracking attempts. Test WPA3 implementations within densely populated network environments, as illustrated in the university campus case analysis, produced measurable improvements in user confidentiality without causing major reductions in communication performance or overall user satisfaction (Aslan et al., 2023). These findings indicate that the privacy enhancements introduced through WPA3 provide effective and practical benefits within real-world wireless communication systems.

3.6 Future Directions and Advancements:

The advancement of Wi-Fi Protected Access 3 remains an active area of investigation focused on addressing emerging cybersecurity threats and confidentiality-related challenges (Yallareddy et al., 2024). The introduction of WPA3-Enterprise and the expanded functionality of advanced protection mechanisms designed for highly sensitive environments indicate a movement toward comprehensive user privacy preservation.

Academic research related to quantum-resistant encryption methods and their possible incorporation into next-generation wireless communication protocols suggests that privacy protection mechanisms will continue to advance in response to evolving technological threats (Durr-E-Shahwar et al., 2024). Such continuous advancement is necessary for preserving user confidentiality against increasingly sophisticated attack methods and rapidly expanding computational capabilities.

4. Conclusion

Compared with its earlier counterpart, Wi-Fi Protected Access 2, this study confirms that Wi-Fi Protected Access 3 delivers substantial improvements in user-oriented privacy preservation, especially within high-risk wireless environments such as the university campus analyzed in this research. The implementation of personalized encryption mechanisms, strengthened protection for open wireless environments, and the utilization of SAE collectively resolve several long-standing privacy concerns experienced by wireless network users (Moissinac et al., 2021; Qi, Hu, & Tai, 2024).

The statistical evaluation indicates that the WPA3 framework successfully minimizes the major confidentiality threats identified within the university campus case analysis. Protection mechanisms against offline password-guessing attacks considerably decrease the possibility of privacy breaches caused by password exploitation. Simultaneously, the removal of shared-encryption-key weaknesses ensures that communications exchanged by individual users remain inaccessible to other participants connected to the same network. Furthermore, stronger separation among connected devices provides additional safeguarding for confidential personal information.

However, the investigation also identifies several constraints and research areas requiring additional examination. Users operating older-generation devices may experience reduced privacy protection because of backward compatibility limitations, while the complexity associated with deployment may restrict large-scale implementation. In addition, performance-related concerns require administrators to maintain a careful balance between stronger security capabilities and a convenient user experience, particularly within environments using devices with limited computational resources.

4.1 Major Contributions

This research expands the existing academic knowledge regarding the privacy-enhancing advantages of Wi-Fi Protected Access 3 through a practical evaluation performed within a real-time deployment environment. The mixed-evaluation methodology enables the identification of deployment-related challenges influencing actual implementation while also generating measurable information concerning the efficiency and effectiveness of WPA3 security mechanisms.

4.2 Research Constraints

The investigation was restricted to a single case-study scenario, which may not completely represent the broad diversity of wireless communication infrastructures and the varying privacy expectations of users. Moreover,

because cybersecurity defence technologies and attack methodologies continue to evolve rapidly, the findings of this study may require periodic reassessment to remain relevant within continuously changing threat conditions.

4.3 Future Investigation

Future studies should involve a broader range of wireless communication deployments, including public, organizational, and enterprise environments, to verify the capability of WPA3 to maintain confidentiality across diverse operational conditions. Research focusing on user attitudes, behavioural patterns, and privacy awareness within WPA3-enabled environments may provide valuable insight into the influence of human-related factors on the acceptance of cybersecurity technologies.

In addition, the continuously developing wireless communication ecosystem will require future investigations into the integration of WPA3 with emerging technologies such as Internet of Things devices and edge-computing infrastructures. Another important research direction involves the advancement of quantum-resistant encryption techniques and their future incorporation into wireless protection frameworks to strengthen user privacy against emerging computational threats (Durr-E-Shahwar et al., 2024).

WPA3 delivers measurable privacy-enhancement advantages that directly benefit wireless network users and represents an important advancement in user-oriented wireless protection technologies. Despite the existence of deployment-related difficulties, the privacy-focused foundation of the protocol makes it highly important for preserving personal confidentiality within an increasingly interconnected digital society.

4.4 Future Suggestions

Future directions for WPA3 should concentrate on improving practical implementation and reinforcing long-term confidentiality protection capabilities. Resolving backward compatibility limitations remains essential because many users continue to depend on older-generation or resource-limited devices that do not completely support WPA3 technologies. Designing lightweight implementations or adaptive compatibility frameworks may help prevent such users from being redirected toward less secure wireless segments.

Furthermore, simplifying WPA3 deployment through automated protection utilities, enhanced administrative management interfaces, and user-oriented privacy notification mechanisms may minimize configuration errors and encourage easier adoption. Educational institutions and organizations should also combine WPA3 with client-device isolation mechanisms in densely populated wireless environments to reduce lateral intrusion risks and provide stronger protection for sensitive personal information.

5. Validation of Research Outcomes

The findings presented in this research are justified by the increasing need to evaluate wireless protection technologies from a user-focused privacy perspective, an area where practical evidence remains limited. Although Wi-Fi Protected Access 3 is widely regarded as a major advancement over Wi-Fi Protected Access 2, only a limited number of studies have examined its effectiveness within real-world deployment conditions, especially in high-risk environments such as university campuses, public wireless hotspots, and densely populated communication networks. This investigation therefore addresses an important research gap by combining theoretical evaluation with a practical case analysis to assess the capability of WPA3 in strengthening personal privacy protection. The results demonstrate that WPA3 significantly reduces major confidentiality weaknesses associated with WPA2, including common-key exposure, offline password-guessing intrusions, and inadequate device separation. The examination of the university wireless environment confirms that WPA3 functionalities such as SAE, personalized encryption mechanisms, and Opportunistic Wireless Encryption directly resolve identified privacy-related threats and provide measurable improvements in user confidentiality.

The investigation additionally provides practical insight into the realities of WPA3 deployment within heterogeneous network environments. The identification of limitations, including backward compatibility concerns affecting legacy devices, increased computational requirements, and configuration-related complexity, demonstrates that the theoretical privacy advantages of WPA3 must be balanced against operational constraints. These observations are especially important for institutions and organizations planning migration toward WPA3

because they highlight both infrastructure-related requirements and user-oriented implementation challenges. Furthermore, the research delivers measurable conclusions regarding the effectiveness of WPA3 in reducing communication interception incidents and password-related attacks, reinforcing the value of broader deployment within environments where confidential information is frequently transmitted. This study also contributes to the growing discussion surrounding human-centred cybersecurity by emphasizing that wireless protection is not only a technical issue but also a human-focused concern involving privacy perception, user trust, usability, and behavioural factors.

References:

[1] F. Afzal, S. A. A. Naqvi, A. Uzair, and M. A. Javed, "An enhanced approach for Wi-Fi security and authentication protocols: A systematic approach towards WEP, WPA, WPA2, and WPA3," *Spectrum of Engineering Sciences*, vol. 2, no. 5, pp. 379–403, 2024.

[2] T. O. Agboola, J. G. Jacob, and J. Adegede, "Balancing usability and security in secure system design: A comprehensive study on principles, implementation, and impact on usability," *International Journal of Computing Sciences Research*, vol. 8, pp. 2995–3009, 2024.

[3] G. A. Alghisi and F. Gringoli, "An experimental analysis of the WPA3 protocol in IoT devices," in *2024 22nd Mediterranean Communication and Computer Networking Conference (MedComNet)*, 2024, pp. 1–4.

[4] O. Aslan, E. Akin, S. S. Aktŭg, M. Ozkan-Okay, and A. A. Yilmaz, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023.

[5] A. Bartoli, "Understanding server authentication in WPA3 enterprise," *Applied Sciences*, vol. 10, no. 21, p. 7879, 2020.

[6] A. Chaudhary and K. Kumar, "Vulnerability analysis of WPA security protocols," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2024, pp. 1–7.

[7] P. Danekula, "Wi-Fi deployment in large venues and stadiums: A technical overview," *World Journal of Advanced Engineering Technology and Sciences*, vol. 15, no. 1, pp. 1533–1541, 2025.

[8] Durr-E-Shahwar, S. Hussain, M. Imran, W. Khan, A. B. Altamimi, and M. Alsaffar, "Quantum cryptography for future networks security: A systematic review," *IEEE Access*, vol. 12, pp. 180048–180078, 2024.

[9] A. Halbouni, M.-C. Leow, and L.-Y. Ong, "Wireless security protocols WPA3: A systematic literature review," *IEEE Access*, vol. 11, pp. 112438–112450, 2023.

[10] K. Hughes-Lartey, Z. Qin, F. E. Botchey, and M. Li, "Human factor, a critical weak point in the information security of an organisation's internet of things," *Heliyon*, vol. 7, no. 3, 2021.

[11] B. Jiang, H. Song, J. Li, and G. Yue, "Differential privacy for industrial internet of things: Opportunities, applications, and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10430–10451, 2021.

[12] N. Mahlake, T. Muchenje, T. E. Mathonsi, and D. Du Plessis, "A lightweight encryption algorithm to enhance wireless sensor network security on the internet of things," *J. Commun.*, vol. 18, no. 1, pp. 47–57, 2023.

[13] M. A. I. Mallick and R. Nath, "Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments," *World Scientific News*, vol. 190, no. 1, pp. 1–69, 2024.

[14] A. Mathew, A. Tobesman, and E. Jackson, "Evaluating the efficacy of WPA3 against advanced attacks: A comparative analysis with WPA2 in real-world," *J Inform Techn Int*, vol. 3, no. 1, p. 105, 2025.

[15] K. Moissinac, A. Elleithy, D. Ramos, and G. Rendon, "Wireless encryption and WPA2 weaknesses," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021, pp. 1007–1015.

[16] I. Palamà, G. Bianchi, A. Amici, G. Bellicini, F. Pedretti, and F. Gringoli, "Attacks and vulnerabilities of Wi-Fi enterprise networks: User security awareness assessment through credential stealing attack experiments," *Computer Communications*, vol. 212, pp. 129–140, 2023.

[17] N. Pattnaik, J. R. Nurse, and S. Li, "Security and privacy perspectives of people living in shared home environments," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. CSCW2, pp. 1–39, 2024.

[18] M. Qi, Y. Tai, and W. Hu, "SAE+: One-round provably secure asymmetric SAE protocol for client-server model," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3906–3913, 2024.

[19] G. Sagers, "WPA3: The greatest security protocol that may never be," in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021, pp. 1360–1364.

[20] S. Szymoniak, "Key distribution and authentication protocols in wireless sensor networks: A survey," *ACM Computing Surveys*, vol. 56, no. 6, pp. 1–31, 2024.

[21] K. Yallareddy, S. Kumaran, K. Daniel, K. Thirupathamma, T. Vaishnavi, and T. Aravind, "Wi-Fi lockdown: Ensuring rock-solid security in wireless environments," in *2024 Global Conference on Communications and Information Technologies (GCCIT)*, 2024, pp. 1–6.

[22] D. T. Zaidan, "Analysing attacking methods on Wi-Fi wireless networks pertaining (WEP, WPA-WPA2) security protocols," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 9, no. 4, pp. 1093–1101, 2021.