Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

An Enhanced Approach for Wi-Fi Security and Authentication Protocols: A Systematic Approach towards WEP, WPA, WPA2, and WPA3

Faiza Afzal[1]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
faizaafzal.official@gmail.com

Ahmad Uzair[2]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
ahmaduzair2585@gmail.com

M. Aetsam Javed[3]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
SU92-PHCSW-F24-023@superior.edu.pk

Syed Asad Ali Naqvi[4]
Department of Computer Science, Faculty of Computer Science & IT Superior. University Lahore, 54000, Pakistan
syedasad.alinaqvi@superior.edu.pk

Hamayun Khan[5]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Abstract

The size of wireless networks and the number of wireless devices are growing daily. A crucial part of wireless security involves preventing unauthorized access by using wireless security protocols to protect the data in wireless networks. The article

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

examines security threats facing wireless networks and the effectiveness of security protocols deployed to combat these threats. The thesis will base its study on Wireless Local Area Networks (WLAN) as defined by IEEE standards 802.11a/b/g/n. Features of each WLAN Security protocol, from WEP, WPA and IEEE 802.11i will be analyzed and the effectiveness of each protocol in ensuring data integrity, data confidentiality, and network availability will be presented. The evolution of Wi-Fi security protocols has paralleled the growing demand for secure wireless communication in an interconnected world. Starting with the flawed Wired Equivalent Privacy (WEP), the journey toward robust security has seen the development of WPA, WPA2, and WPA3. Each protocol aimed to address the vulnerabilities of its predecessor, adopting more sophisticated encryption techniques and authentication mechanisms. This paper provides a comprehensive analysis of these protocols, highlighting their technical advancements, weaknesses, and real-world applications. Through systematic review methodologies and real-time examples, the study underscores the critical need for continuous innovation to combat emerging cyber threats in an era of rapid technological advancement. In a network where frequent handovers of a client device are required from one Access point to another; the large latencies may lead to poor Quality of Service (QoS) or even interruption of real-time and interactive network services such as Voice over Internet Protocol (VOIP).

Keywords: Wi-Fi security, wireless protocols, WEP, WPA, WPA2, WPA3, cybersecurity, encryption, authentication, real-world examples.

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Introduction

Wireless networks have experienced an explosive growth in recent years. This rapid growth is due to the proliferation of laptop computers, Personal Digital Assistants (PDAs) and other handheld devices and also due to many advantages offered by wireless networks to both the user and the network operator [1]. Wireless communication is the backbone of modern connectivity, enabling everything from home automation systems to critical infrastructure. Wi-Fi networks, once a technological luxury, have become indispensable in daily life. However, their reliance on open transmission mediums exposes them to significant security vulnerabilities, including unauthorized access, data interception, and denial-of-service attacks [2]. To counter these challenges, Wi-Fi security protocols have evolved over the past two decades. The journey began with WEP in 1997, a protocol that was soon criticized for its vulnerabilities [3]. WPA and WPA2 emerged as solutions to address WEP's flaws, and WPA3, introduced in 2018, represents the most advanced standard to date. Each protocol has brought incremental improvements, balancing compatibility with legacy systems and the need for enhanced security [4]. This paper conducts an in-depth analysis of WEP, WPA, WPA2, and WPA3, focusing on their encryption methodologies, authentication mechanisms, and vulnerabilities. Real-world examples illustrate their practical implications, while a comparative framework highlights the progress made and areas for improvement [5].

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

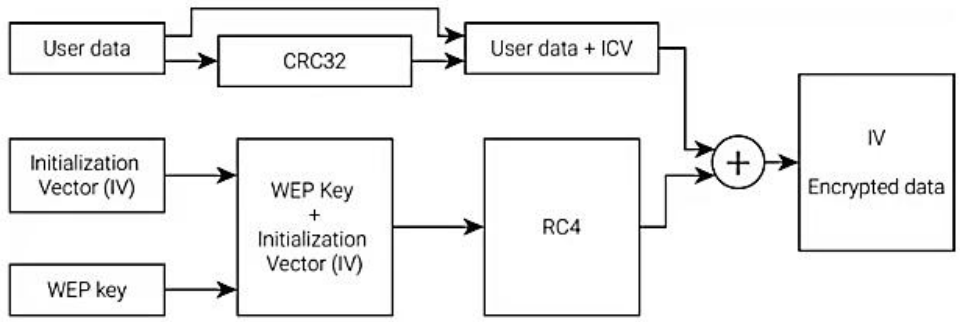

Figure 1: WEP Security Encryption [6]

Background

When we created the first iBook with WiFi capabilities back in 1999, it was magical. Being able to connect to the internet without wires felt like science fiction becoming reality. But we knew that for WiFi to truly revolutionize how people use computers, it had to be secure [7]. That's why I've always been fascinated by the evolution of WiFi security protocols. From the early days of WEP to the latest WPA3 standard, it's been a constant race between hackers and security researchers. With each new protocol, we've taken another step towards making WiFi not just convenient, but truly safe and trustworthy [8, 9].

In this paper, I want to take you on a journey through the history of WiFi security. We'll look at how each protocol works, where it succeeds, and where it falls short. Most importantly, we'll explore what we can learn from the past to build even better security for the future of wireless networking [10, 11].

The WEP Era: A False Start

Wired Equivalent Privacy (WEP) was the original WiFi security protocol, introduced way back in 1997. The idea was simple - use a shared key to encrypt data so that only devices with that key could access the network. Here's how it worked:

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

- The access point and client share a secret 40-bit or 104-bit key
- This key is combined with a 24-bit initialization vector (IV) to create a seed
- The seed is input into a pseudo-random number generator to create a keystream
- The keystream is XORed with the plaintext to produce the ciphertext
- It sounds good on paper. But in practice, WEP had some serious flaws. By 2001, researchers had found major vulnerabilities in WEP [12, 13].
- The 24-bit IV was too short, leading to frequent key reuse.
- Weak integrity check using CRC-32 allowed packet forgery.
- The lack of key management made it easy for attackers to recover the key [14, 16]. Within a few years, tools were widely available that could crack WEP keys in minutes. WEP was officially deprecated in 2004, but incredibly, some routers still support it today. Security through obscurity doesn't work. We needed a protocol built on strong, publicly vetted cryptography [17].

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Table 1: Comparative Analysis of WIFI Security Protocol [18]

Capabilities		WEP	WPA/WPA2	WPA3
Year in released		1997	2004	2018
En/Decryption	Personal	RC4	TKIP/AES-CCMP	AES-CCMP
	Enterprise		TKIP/AES-CCMP	AES-GCMP
Integrity	Personal	No	CCMP 64-bit MIC	CCMP 64-bit MIC
	Enterprise			GCMP 128-bit MIC
Key length	Personal	40-bit or 104-bit	128-bit	128-bit
	Enterprise		128-bit	256-bit
Pre-shared key		PSK	PSK	SAE
Open network encryption		Open	Not supported	OWE
Easy connect		Not supported	WPS	DPP
PMF		Not supported	Optional	Mandatory
Offline dictionary attack		Vulnerable	Vulnerable	Invulnerable

WPA: A Bridge to Better Security

WiFi Protected Access (WPA) was rushed out in 2003 as a stopgap measure to address WEP's flaws. Its main innovation was the Temporal Key Integrity Protocol (TKIP):

i. Uses a 128-bit key instead of 40/104-bit
ii. Implements a key mixing function for each packet
iii. Extends the IV to 48 bits to prevent reuse
iv. Adds a strong message integrity check (MIC)

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

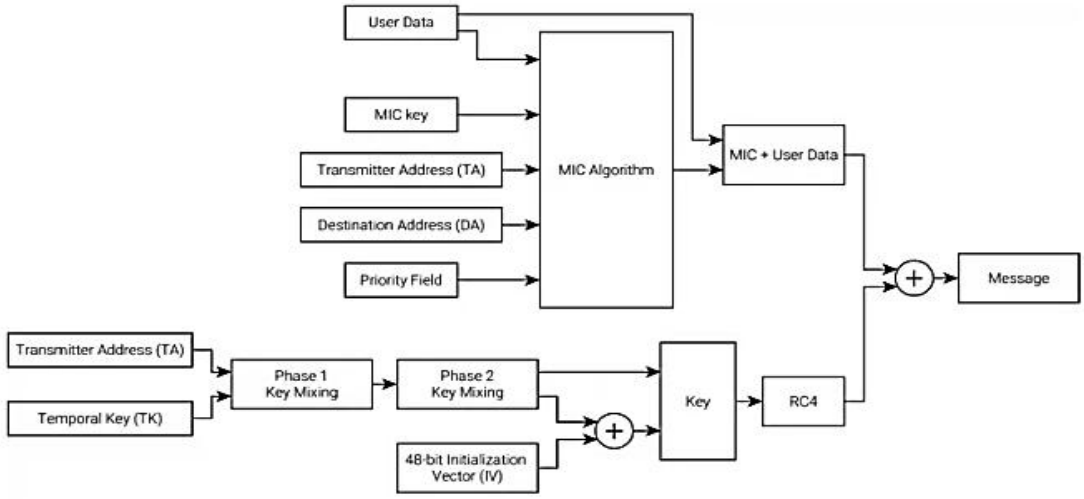

Figure 2: WPA Security Encryption [19]

Weaknesses in WPA

While vastly superior to WEP, WPA still had some issues:

- TKIP was vulnerable to certain packet injection and decryption attacks
- PSK mode was susceptible to offline dictionary attacks
- No protection against evil twin attacks

These weaknesses led to the development of WPA2, which would become the gold standard for WiFi security for over a decade.

- WPA2: Raising the Bar
- CCMP: AES Comes to WiFi

The cornerstone of WPA2 is the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). It's based on the Advanced Encryption Standard (AES), which is still considered cryptographically secure today [20].

CCMP provides:

- Strong 128-bit AES encryption
- Integrity protection and authentication
- Protection against replay attacks

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Unlike TKIP, CCMP was designed from the ground up for WiFi security. It's faster, more secure, and more efficient [21]

Table 2: Comparative Analysis of WEP, WPA & WPA2

Feature	WEP	WPA	WPA2	Ref
Encryption Standard	RCA	TKIP	AES	[22]
Key Length	64 Bit	128 Bit	256 Bit	[22]
Introduce Year	1997	2003	2004	[23]
Key Management	Pre shared key	Pre Shared key	PSK Or Enterprise	[24]
Vulnerability	Weak encryption	Vulnerable to replay attack	Secure but prone to brute force	[25]
Authentication	Open system or Shared key	802.1X or PSK	802.1X Or PSK	[26]
Data Integrity	CRC32 (Weak)	MIC	CCMP	[27]
Compatibility	Legacy Device	Most Device	Most Modern Device	[28]
Usage	Deprecated, insecure	Rarely used	Widely Used	[29]

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Advantage	Simple setup	Better than WEP	Strong encryption	[30]
Disadvantage	Very insecure	Outdated	Brute force with weak password	[31]

Key Management and Handshake

WPA2 uses a 4-way handshake to establish session keys:

- The access point sends a random number (ANonce) to the client.
- The client generates its random number (SNonce) and derives the Pairwise Transient Key (PTK).
- The client sends the SNonce and a Message Integrity Code (MIC) to the AP.
- The AP derives the PTK and sends a confirmation to the client.

This process ensures that both parties have the correct keys without ever transmitting the actual key over the air. WPA2-Enterprise added support for:

- EAP methods for flexible authentication
- Per-user keys for better isolation
- RADIUS server integration for centralized management. These features made WPA2 suitable for large-scale enterprise deployments, not just home networks [32].

Vulnerabilities in WPA2

- Despite its strengths, researchers have found some flaws in WPA2
- KRACK attack: Exploits the 4-way handshake to decrypt traffic

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

- Hashcat: Enables faster brute-force attacks on weak passphrases
- Dragonblood: Targets the Dragonfly handshake in WPA3-transition mode

While these attacks are concerning, they generally require physical proximity and significant effort. For most users, WPA2 remains secure when configured correctly [33]. WPA3: The Next Generation Simultaneous Authentication of Equals (SAE). WPA3's biggest innovation is replacing the PSK with Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange. Past traffic can't be decrypted if the password is compromised while protection against offline dictionary attacks and resistance to quantum computer attacks increases. SAE uses a Diffie-Hellman key exchange, allowing devices to derive a shared key without ever transmitting it [34].

192-bit Security Suite

- For high-security environments, WPA3-Enterprise offers a 192-bit security suite:
- 256-bit AES-GCM encryption
- 384-bit HMAC-SHA384 for key derivation and confirmation
- ECDH and ECDSA using 384-bit curves

This level of security is overkill for most users, but critical for government and military applications [35].

2. The Importance of Open Standards

One clear lesson from the history of WiFi security is the value of open standards. WEP's proprietary design led to critical flaws, while the openly published WPA2 and WPA3 standards have proven much more robust [38, 40]. Each new protocol has had to balance

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

increased security with ease of use. WPA3's Enhanced Open is a great example of improving security without sacrificing convenience.

TKIP was designed to work on existing WEP hardware with just a firmware update. It wasn't perfect, but it brought us time to develop a more comprehensive solution. You enter a passphrase, which is used to derive the encryption keys. It's simple and effective, as long as you use a strong passphrase.

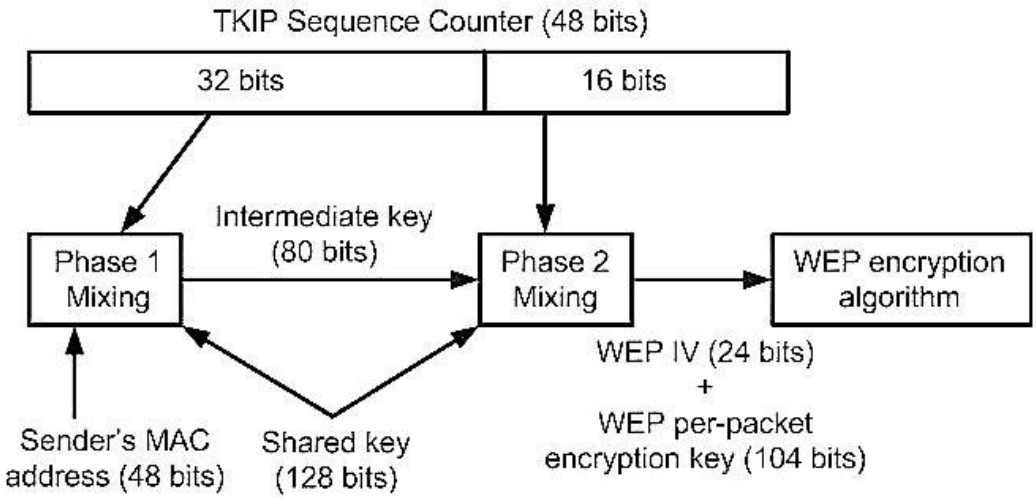

Figure 3: TKIP Security Encryption [36]

The Need for Regular Updates

The discovery of KRACK and other attacks shows that even well-designed protocols can have vulnerabilities. Regular security updates are crucial for maintaining strong WiFi security.

As we look ahead, several trends are likely to shape the future of WiFi security:

- Integration with 5G and other wireless technologies
- Increased use of machine learning for threat detection
- Quantum-resistant cryptography and Enhanced protection against side-channel attacks [37]

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

The evolution of WiFi security protocols from WEP to WPA3 is a testament to human ingenuity and perseverance. With each iteration, we've learned from past mistakes and pushed the boundaries of what's possible in wireless security. As we continue to build a world where everything is connected, strong WiFi security will only become more critical. By understanding the strengths and weaknesses of each protocol, we can make informed decisions about how to protect our networks and data [38, 39]. The journey from WEP to WPA3 shows us that perfect security may be unattainable, but we can always strive to make it better. It's this relentless pursuit of improvement that drives innovation and keeps our digital lives safe. In the end, that's what great technology is all about - not just making things work, but making them work better, safer, and more seamlessly than ever before. That's the kind of magical experience we've always strived for at Apple, and it's what we should demand from all our technology [40, 41].

Table 3: Features of WLAN standards by IEEE for WiFi Security

WLAN Standard	Year Ratified	Operating Frequency	Maximum Data Rate	Physical Layer
Legacy 802.11	1997	2.4 GHz	2 Mbps	FHSS/DSSS
802.11b	1999	2.4 GHz	11 Mbps	DSSS
802.11a	1999	5 GHz	54 Mbps	OFDM
802.11g	2003	2.4 GHz	54 Mbps	OFDM
802.11n (Draft)	Published 2007	2.4/5 GHz	600 Mbps	MIMO

Enhanced Open

WPA3 introduces Enhanced Open, which provides encryption for open networks:

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Uses Opportunistic Wireless Encryption (OWE) and protects against passive eavesdropping. Mostly it doesn't require a pre-shared key. This feature makes public WiFi hotspots much safer to use. Transition Mode and Backwards Compatibility. To ease adoption, WPA3 includes a transition mode that supports both WPA2 and WPA3 clients. This allows gradual upgrades without breaking compatibility [42, 43]. Like any new protocol, WPA3 has faced some early challenges:

- Dragonblood attacks targeting SAE implementation flaws
- Potential for downgrade attacks in transition mode
- Side-channel attacks on certain implementations

The WiFi Alliance has already released patches for many of these issues, highlighting the importance of keeping devices updated [44, 45].

Research Methodology

This study employs a systematic review methodology to evaluate the evolution and efficacy of Wi-Fi security protocols. The methodology includes the following components: The study adopts a qualitative approach, combining comparative analysis, case study evaluation, and literature review. Primary sources include IEEE 802.11 specifications and white papers, while secondary sources include peer-reviewed journals, industry reports, and practical field studies. Protocols were assessed based on:

- Encryption Standards: The robustness of encryption mechanisms.
- Authentication Methods: Effectiveness in ensuring secure access.
- Vulnerabilities: Known weaknesses and susceptibility to attacks.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Real-World Applications: Utility in both personal and enterprise settings.

Case Study Selection

Case studies of real-world attacks and practical deployments were selected to validate the analysis. Examples include KRACK attacks on WPA2 networks and WPA3 adoption in smart cities. Introduced Wired Equivalent Privacy (WEP) was the first protocol designed to secure wireless communication. It aimed to replicate the security of wired networks but was quickly found inadequate due to design flaws.

Key Features and Vulnerabilities

Encryption: RC4 stream cipher with 24-bit initialization vectors (IVs).Authentication: Shared static keys. Data Integrity: CRC-32 checksum for error detection. Predictable IVs: Enabled attackers to decrypt data packets using brute-force methods. Weak Encryption: Susceptible to statistical attacks. A study revealed that several legacy networks still used WEP. Using tools like Air crack-ng, researchers demonstrated how easily these networks could be compromised within minutes.

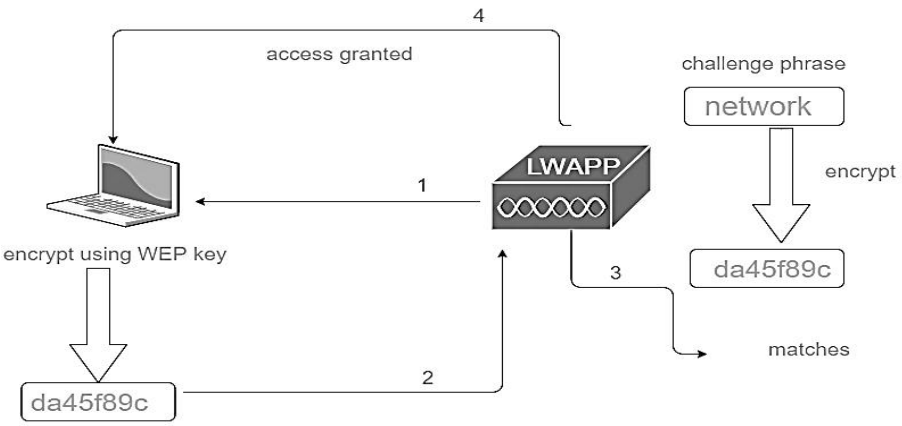

Figure 4: WEP Authentication [46]

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

WPA: A Transitional Solution

Wi-Fi Protected Access (WPA) was introduced as an interim solution to address WEP vulnerabilities. It improved encryption and integrity mechanisms while maintaining compatibility with existing hardware. Temporal Key Integrity Protocol (TKIP) with dynamic key generation. Pre-Shared Key (PSK) and 802.1X for enterprise environments. Data Integrity: Message Integrity Code (MIC).

Legacy Dependency: Continued reliance on RC4 meant inherited weaknesses. Replay Attacks: Exploited flaws in encryption mechanisms. Attackers deployed an "Evil Twin" access point to mimic legitimate WPA-secured networks. This exploit forced users to connect to the rogue network, exposing their credentials [47].

Table 4: WEP and WPA Encryption & Authentication

	WEP	WPA
Encryption	40-bit keys	128-bit keys
	Static key – Same key used by everyone in the network	Dynamic key assignment – Keys change per user, per session, per packet
	Manual distribution of keys	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication utilizing 802.11X and EAP

WPA2: Setting the Benchmark

WPA2, introduced in 2004, replaced WPA as the industry standard, employing AES encryption with CCMP for enhanced security.

Key Features and Vulnerabilities

Encryption: Advanced Encryption Standard (AES) with 128-bit keys. Authentication: PSK and 802.1X. Integrity: CCMP to prevent data tampering. KRACK Attacks: Exploited the four-way handshake, allowing attackers to intercept and manipulate encrypted

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

data.Unprotected Management Frames: Opened networks to spoofing and reauthentication attacks. Researchers demonstrated KRACK attacks on WPA2 networks, emphasizing the need for enhanced protections like those in WPA3. Introduced WPA3 addresses WPA2â€™s shortcomings, incorporating advanced cryptographic techniques and user-friendly features [48].

- Encryption: AES-GCMP with 256-bit keys.
- Authentication: Simultaneous Authentication of Equals (SAE).
- Integrity: Protected Management Frames (PMF).

Challenges and Comparative Reflection: The Evolution of Security Paradigms

Backward Compatibility: Older devices require firmware upgrades. Implementation Flaws: Certain deployments of SAE were vulnerable to dictionary attacks. WPA3-secured networks successfully protected IoT devices from unauthorized access while ensuring high-speed data transmission The progression from WEP to WPA3 is a journey that reflects the ever-evolving nature of cybersecurity. Where WEP failed due to static encryption and key reuse, WPA began to address these issues, albeit with a reliance on outdated algorithms. WPA2 introduced the modern standard with AES encryption, yet even it had to contend with newly discovered vulnerabilities. WPA3, designed for the future, promises to secure the wireless networks of tomorrow by addressing the very real challenges posed by modern cyber threats. Each protocol has made significant strides toward securing wireless networks, but each has also exposed the limits of its era. What was once considered a strong defense against attackers is now regarded as inadequate in the face of rapidly advancing cyber threats. As we look toward the future, WPA3 seems poised to lead the charge,

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

offering a more secure and resilient model for Wi-Fi security in an increasingly interconnected world. In the end, wireless security is not a one-time fix but a continuous journey of adaptation and evolution. WPA3 is a powerful step forward, but as new technologies emerge and attack vectors evolve, the task of securing wireless communication will require constant vigilance and innovation.

Table 5: Comparative Analysis of Encryption & Authentication Standard Protocols of WEP, WPA, WPA2, and WPA3

Standard	WEP	WPA	WPA2	WPA3
Release	1997	2003	2004	2018
Encryption	RC 4	TKIP with RC 4	AES CCMP	AES CCMP and GCMP
Key size(s)	64 and 128 bits	128 bits	128 bits	128 and 256 bits
Cipher type	Stream	Stream	Block	Block
Authentication	Open system and shared key	Pre-shared key and 802.1x with EAP variant	Pre-shared key and 802.1x with EAP variant	Simultaneous Authentication of Equals and 802.1x with EAP variant

Conclusion

This systematic literature review studied the wireless security certificate Wi-Fi Protected Access WPA3. Findings show that the devised systematic literature review is the first of its kind in wireless security protocols. In this article, we presented four course modules on critical cybersecurity topics that can be adopted incollege-level cybersecurity courses in which these topics are covered. The evolution of Wi-Fi security protocols reflects the dynamic nature of cyber security, where innovation must outpace emerging threats. While WPA3 sets a new benchmark, the challenges of implementation and compatibility underscore the need for continuous advancements. As quantum computing and AI-driven attacks loom on the horizon, future protocols must anticipate and address these disruptive technologies. The journey

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

from WEP to WPA3 is not just a technological narrative but a testament to the relentless pursuit of secure digital communication.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(4), 28-35.

[2] Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access.

[3] Ambavkar, P. S., Patil, P. U., Meshram, B. B., & Swamy, P. K. (2012). Wpa exploitation in the world of wireless network. Int J Adv Res Comput Eng Technol, 1(4), 609-618.

[4] Cahyadi, D., Astuti, I. F., & Nazaruddin, N. (2023, February). Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 n. In AIP Conference Proceedings (Vol. 2482, No. 1). AIP Publishing.

[5] Baray, E., & Ojha, N. K. (2021, April). WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In 2021 5th International conference on computing methodologies and communication (ICCMC) (pp. 23-30). IEEE.

[6] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[7] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[8] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[9] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[10] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[11] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[12] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[13] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[14] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[15] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[16] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[17] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[18] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[19] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[20] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[21] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[22] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[23] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[24] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[25] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[26] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[27] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[28] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[29] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[30] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[31] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[32] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[33] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[34] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[35] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[36] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[37] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[38] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[39] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[40] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[41] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[42] Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M. (2016, May). An empirical study of wifi security and performance in morocco-wardriving in rabat. In 2016 International Conference on Electrical and Information Technologies (ICEIT) (pp. 362-367). IEEE.

[43] Sagers, G., Hosack, B., Rowley, R. J., Twitchell, D., & Nagaraj, R. (2015, January). Where's the security in WiFi? An argument for industry awareness. In 2015 48th Hawaii international conference on system sciences (pp. 5453-5461). IEEE.

[44] Zhang, S., Venkatnarayan, R. H., & Shahzad, M. (2020, December). A wifi-based home security system. In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 129-137). IEEE.

[45] Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., ... & Alexis, W. (2016, November). Securing commercial WiFi-based UAVs from common security attacks. In MILCOM 2016-2016 IEEE Military Communications Conference (pp. 1213-1218). IEEE.

[46] Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359.

[47] Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis of deep learning. IEEE Access, 8, 186125-186137.

[48] Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 55(5), 1-37.