IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 September 2023, accepted 2 October 2023, date of publication 9 October 2023, date of current version 17 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3322931

SURVEY

Wireless Security Protocols WPA3: A Systematic Literature Review

ASMAA HALBOUNI, (Graduate Student Member, IEEE), LEE-YENG ONG, (Senior Member, IEEE), AND MENG-CHEW LEOW, (Senior Member, IEEE)
Faculty of Information Science and Technology, Multimedia University, Malacca 75450, Malaysia
Corresponding author: Lee-Yeng Ong (lyong@mmu.edu.my)

This work was supported by the Telekom Malaysia Research and Development under Grant RDTC/221073 (MMUE/230002).

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 in order to protect the data in wireless networks. In 2018, Wi-Fi Protected Access 3 (WPA3) was ratified to protect the data in devices bearing the Wi-Fi trademark. WPA3 has many security improvements over previous wireless security protocols, by providing a better encryption method and key sharing. In this paper, a Systematic Literature Review (SLR) was conducted to analyze three aspects of WPA3 protocol: the reasons behind the release of WPA3, the encryption methods and mode of operation in this protocol, and the attacks that remain penetrating WPA3. In this review, thirty-six articles were identified as the selected research articles, written between 2018 and 2023, focusing mainly on WPA3. After the analysis of the selected articles, the encryption methods and modes of operation were presented in the SLR. In addition, the vulnerabilities that the WPA3 protocol solved and the ones that remain unsolved were discussed. This study concluded that WPA3 excels over its predecessors by providing more security and reliability to wireless networks. The result of this SLR of WPA3 proposes two methods that seek to increase the security level of WPA3 networks, which has been discussed in the discussion section.

INDEX TERMS Wireless security protocol, Wi-Fi Protected Access 3, WPA3.

I. INTRODUCTION

The most common type of network is wireless networks, which connect devices without using cables to exchange data. Wireless networks are expanding continuously, whether for public use at the corporate level or for personal usage at home. Wi-Fi has become an essential and normal part of our daily lives. When explaining wireless terminologies, the terms Wireless Local Area Network (WLAN) and Wi-Fi are usually used interchangeably. WLAN is a type of network where data is exchanged wirelessly using high-frequency radio waves. Wi-Fi refers to the family of wireless network protocols known as IEEE 802.11 that can build WLANs. The data in the wireless network is propagated in a wireless medium, making it insecure against internal and external security threats, where anybody who breaches wireless security can access the network. Wireless networks have security risks, hence various protocols have been developed throughout time to offer security against various risks. In 1997, the 802.11 WLAN standard is introduced by the Institute of Electrical and Electronic Engineers (IEEE). Various wireless security standards were developed to be employed in the wireless networks used in homes, offices, and public areas [1]. Wired Equivalent Privacy (WEP) was the first security protocol to be released, and in 2004, it became deprecated. After WEP, Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) were introduced with the IEEE 802.11i standard. WPA was introduced in 2003. After WPA was proven to have major flaws and vulnerabilities, it was replaced by WPA2 in 2004 and is still being used until now. Finally, Wi-Fi Protected Access 3 (WPA3) was released in 2018 to solve all the shortcomings of its predecessors by providing high protection and usability for its users [2].

The advancement of WPA3's encryption and encoding methods proved its ability to deliver higher security levels to both personal and enterprise users. When investigating

The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Mueen Uddin.

related works on WPA3, the results show that WPA3 is implemented to overcome the previous security protocols in addition to the vulnerabilities solved by WPA3 and the ones that remain unsolved. However, at the time of conducting this work, there was no research focusing on providing a systematic literature review purely on WPA3. Even though WPA3 is still new, some review papers on wireless security have included it to compare it with its predecessors.

Several studies on cybersecurity threats and vulnerabilities of wireless security protocols can be found in [3] and [4]. Both research discussed how wireless networks are attacked using the design flaws in WEP, WPA, and WPA2. The vulnerabilities in WEP, WPA, and WPA2 protocols are mentioned in [3], while [4] presented an evaluation among the wireless security protocols based on encryption, authentication methods, and wireless security requirements, besides including a comparison among WEP, WPA, WPA2, and WPA3.

A review has been conducted to examine the danger of Wi-Fi networks and the insecure reasons among WEP, WPA, WPA2, and WPA3 [5], [6]. However, [5] only focused on mentioning the vulnerabilities in these protocols without giving practical countermeasures to avoid them and in [6] mentioned the vulnerabilities in addition to suggestions added to WPA3 to update the protocol.

To the best of our knowledge, there is no systematic literature review (SLR) focusing solely on the security certificate WPA3. Therefore, this systematic review presents an extensive research study on the reasons behind the release of WPA3, the encryption methods and mode of operation in this protocol, and unsolved vulnerabilities of the wireless security protocol WPA3. This SLR is conducted based on Kitchenham and Charter's method [7]. The primary aim of this work is to provide SLR of WPA3 to help researchers know more about WPA3. The contributions of this systematic review are summarized as follows:

1. Showing the reasons behind the release of the WPA3 protocol.
2. Discuss the main features of each wireless security protocol and their related attacks.
3. Highlights the vulnerabilities of WPA3 that remain unsolved. In addition to provide a discussion of attacks in WPA3 between the years 2018 and 2023.
4. Propose two methods to improve the security of WPA3 protocol.

The remainder of this paper is structured as follows: Section II provides a brief description of the current state of wireless security protocols. The method used in this work is in section III. Section IV explains the results obtained from the selected papers and a discussion. Section V defines the limitations of the study and the conclusion is given in Section VI.

II. WIRELESS SECURITY PROTOCOL

This section describes the wireless security protocols in terms of the authentication process and vulnerabilities, starting with WEP until WPA3.

A. WIRED EQUIVALENT PRIVACY (WEP)

WEP was introduced to provide security for wired LANs by encryption. It is based on Rivest Cipher 4 (RC4) encryption to increase the speed of communication [4]. The encryption key of WEP is 64-bit composed of a secret key of 40-bit long with a 24-bit initialization vector (IV) concatenated to it. WEP uses Cycle Redundancy Check known as CRC-32 to compare the plaintext to Integrity Check Value (ICV) for integrity [1].

WEP has proven to be vulnerable and easy to be broken [4]. In 2003, free software was able to crack the WEP's passwords within minutes. Another vulnerability in WEP is its ability to broadcast fake data packets because of the shared key authentication, which makes it easy for an attacker to forge an authentication message. The reuse of the initialization vector also makes WEP weak, where different cryptanalysis methods can decrypt the data. Other attacks can be found in [1]. In 2004, the Wi-Fi Alliance officially abandoned the WEP protocol [4], [8].

B. Wi-Fi PROTECTED ACCESS (WPA)

WPA was released to tackle the issues in WEP without the need of changing the hardware. It was only firmware upgradation required to uplift the security aspect based on the same hardware. WPA uses Temporal Key Integrity Protocol (TKIP) for encryption where it uses RC4 to generate other keys. In WPA, 128-bit per packet is generated dynamically. The Pre-Shared Key (PSK) is a static key used to initiate communication between two parties. To authenticate the wireless devices, a 256-bit is used, but it is never transmitted over the air. The encryption key and Message Integrity Code are derived from the PSK. The 4-way handshaking mechanism is used to provide for key management [8], [9].

The main vulnerability in WPA is in RC4, where having keys computed under the same initialization vector makes it easy to compute the Temporal Key by an attacker. Another vulnerability is when there is a poor password, then it is vulnerable to brute force attacks where a dictionary attack can be used if the password is less than 20 characters [8]. Other attacks can be found in [1].

C. Wi-Fi PROTECTED ACCESS 2 (WPA2)

WPA2 was able to deliver a significant enhancement over the previous security protocols. The big difference was in its encryption method. WPA2 is using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which uses the Advanced Encryption Standard (AES) block cipher for its data encryption [10]. To generate a key in WPA2, a 4-way handshake is required to have a Pairwise Transient Key (PTK) and Group Temporal Key (GTK), in addition to a group key handshake.

In WPA2, there are two modes of operation, Pre-Shared Key (PSK) mode for personal networks and enterprise mode for larger corporate networks. In WPA2-PSK, an access point authenticates a client based on a password that is shared in

advance, whereas the authentication in enterprise mode is performed via the Extensible Authentication Protocol (EAP) in 802.1x architecture [9].

One weakness in WPA2 is when an attacker can access the network and have particular keys to execute an attack on other devices connected to the network. Although such an action needs roughly 2 to 14 hours to be executed, it is considered a security issue that must be solved [3]. In addition to that, WPA2 allows the reinitialization of keys, which leads to attacks called KRACK. This attack utilizes the 4-way handshake that wireless security protocols used to authenticate their users while connecting to the network. After setting the counters to their original settings, the attacker can replay and decrypt messages [11]. The details of other attacks can be found in [1].

D. Wi-Fi PROTECTED ACCESS 3 (WPA3)

In June 2018, the Wi-Fi Alliance announced Wi-Fi Protected Access 3 (WPA3) and in July 2020, WPA3 became mandatory for Wi-Fi-certified implementations. It was expected that the adoption rate of WPA3 will grow fast, but the statistics showed the opposite of that [12].

Enhancing the security of the WPA2-PSK handshake was the primary motivation for the development of WPA3. Independent researchers were unable to peer-review the newly implemented features since the WPA3 development process was kept secret from the public [13].

WPA3, similar to its predecessor, has two modes of operation: WPA3-Personal and WPA3-Enterprise. WPA3 permits a transition mode where WPA2 and WPA3 are supported simultaneously to provide backward compatibility [13].

WPA3-personal is using Simultaneous Authentication of Equals (SAE), which represents a secure key exchange protocol between peers designed for authentication purposes [4], [9]. And so, the authentication is performed based on a password that is shared among all handshake parties. A high-entropy Pairwise Master Key (PMK) is the output of WPA3-SAE authentication, that will be utilized as input for the 4-way handshake to create a Pairwise Transient Key (PTK) [13], [14]. Management Frame Protection (MFP) is used in WPA3-SAE mainly to prevent deauthentication attacks where the attackers force the users to disconnect from the Access Point (AP) [14].

Not all the current 802.11 hardware is able to support MFP or SAE, and so, WPA3 certificate has a transition mode that supports WPA2 and WPA3 simultaneously. In this mode, WPA2 AP will be connected using the 4-way handshake without MFP, and WPA3 AP will be connected using the SAE handshake with MFP.

WPA3-Enterprise is not fundamentally changed from the WPA2 version, but is focused instead on adding improvements and increasing misuse resistance. At a protocol level, WPA3 offers an optional 192-bit security mode that uses 256-bit Galois/Counter Mode Protocol (GCMP), widely written as GCMP-256, to provide authenticated encryption [9].

1) DRAGONFLY PROTOCOL

Based on the Wi-Fi Alliance, SAE protocol is using a Dragonfly handshake. According to some research, Dragonfly and SAE are synonymous. For other searches, Dragonfly is considered as one component of many in the SAE protocol. IEEE 802.11 standard defines SAE as a variant of the Dragonfly, a password-authenticated key exchange based on a zero-knowledge proof [4], [9].

Dragonfly is a symmetric peer-to-peer protocol. In Dragonfly, both participants of the exchange are considered equals and have a secure symmetric key from a low-entropy shared secret over insecure public channels, and so they can therefore initiate the handshake simultaneously. Dragonfly is based on discrete logarithmic and elliptic curves (ECC) or finite fields (FFC) cryptography. In Dragonfly, there are two message exchanges between participants, the commit exchange and confirm exchange, as shown in Figure 1 [15].

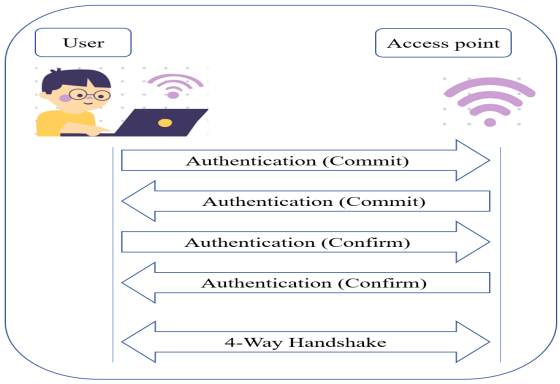

FIGURE 1. WPA3 Authentication: Dragonfly protocol.

The first commit exchange messages can be initiated, then the process continues to confirm exchange messages after both participants confirm their unique, single guess at the password. The commit exchange is to force each participant to reveal what they think the password is and the confirm exchange is to assess the correctness of the passwords provided by each participant. A successful confirmation occurs after a participant accepts the authentication, and when both participants accept the authentication, the handshake process will be terminated [9], [15].

2) MANAGEMENT FRAME PROTECTION (MFP)

Management Frame Protection (MFP) is defined in the IEEE 802.11w amendment and incorporated in IEEE 802.11 base standard in 2012. MFP provides protection mechanisms for management frames includes origin authenticity, confidentiality, integrity, and replay protection. The mechanisms seek to improve the security levels and apply defense mechanisms against attacks targeting management frames. The Wi-Fi Alliance made MFP mandatory in WPA3 protocol to prevent the attacker from forcibly disconnecting a user from the wireless network. WPA3 access points will advertise MFP as an optional due to the transition mode. WPA2 users will be

TABLE 1. Attacks still exist in WPA3.

ATTACK'S NAME	ATTACK'S TIMELINE		DESCRIPTION
	Before WPA3	After WPA3	
DOWNGRADE ATTACK		×	- *Downgrade Attack against WPA3-Transition mode* This attack happens when a network supports WPA2 and WPA3. In this attack, the attacker will create a rogue AP and force the user who supports WPA3 to be connected to its rogue AP that supports only WPA2 and then perform attacks on the WPA2 handshake to recover the password. This attack forces users to downgrade from WPA3 to WPA2, so the network is vulnerable to WPA2's weaknesses. - *Downgrade Attack against WPA3-Dragonfly handshake* In this attack, the downgrade is in the Dragonfly handshake where it uses a weak security group. Upon starting a handshake, a commit frame is sent to the AP along with the security group. The user would be forced to downgrade its security group after attempting to locate a security group that would work by setting up a rogue access point that only accepts a weak security group.
SIDE-CHANNEL ATTACK		×	- *Timing-based Side-Channel* When an AP uses a security group, the response time of the AP depends on the password being used. The duration needed by an AP to respond to a commit message can leak information about the password. An attacker can exploit this to perform a dictionary attack by simulating the time required to process each password and comparing the result with the observed timings. - *Cache-based Side-Channel* When an attacker has gained control over an application on a user's device, then he is able to observe memory access patterns on the user's device when the device sends the commit frames during the Dragonfly handshake. The memory access patterns have data regarding the password, that can be simulated by the attacker to guess the password and then compare the observed one with the guessed one to know the real password.
ROGUE ACCESS POINT	×		A rogue access point is an access point installed on a network without the network owner's permission.
EVIL TWIN ATTACK	×		This attack works by tricking users into connecting to a fake AP that mimics a legitimate network.
DENIAL OF SERVICE (DOS)	×	×	The cookie-exchange method used in WPA3 to prevent fake commit frames using fake MAC addresses caused by an attacker who can generate 16 fake commit frames per second. This action will cause high usage of the AP CPU and prevent or delay other users from connecting to it.
BRUTE-FORCE	×		A brute force attack is when an attacker uses a trial-and-error method to form millions of key combinations to guess the network's password and acquire access.
DEAUTHENTICATION		×	This attack forces the user to be disconnected from the AP by using a deauthentication attack. Due to Management Frame Protection in WPA3, the attacker will be prevented from faking the deauthentication frame when the 4-way handshake is completed. Despite that, the attacker will send multiple deauthentication frames after the association request from the user to an AP, and this will cause confusion for the user to process the packets from the AP, which will lead to AP disconnection.
DICTIONARY ATTACK	×		This attack considers a type of brute-force attack where an attacker tries to get the password using a dictionary list. In this attack, the attacker tries to find the password without capturing the 4-way handshake packets between users and AP.
ARP SPOOFING	×		ARP spoofing is when an attacker takes the advantage of being a Man in The Middle (MiTM) between users and AP in order to intercept communication between network devices.
SSL STRIPPING	×		This attack deals with packets sent over the Internet. This attack leads to downgrading from HTTP secure connection to HTTP less secure connection, resulting in an unencrypted connection. An attacker will be positioned in the middle to manipulate the requests and force the server to respond with HTTP less secure web page.
DNS SPOOFING	×		This attack depends on MiTM to acquire access to place itself between users and AP in order to redirect the altered DNS records to a fraudulent website that resembles its intended destination.

connected using the 4-way handshake with MFP un-enabled and WPA3 users will be connected using SAE with MFP enabled.

3) WPA3 ATTACKS

There are many vulnerabilities that have been found in previous wireless security protocols that cause damage to the

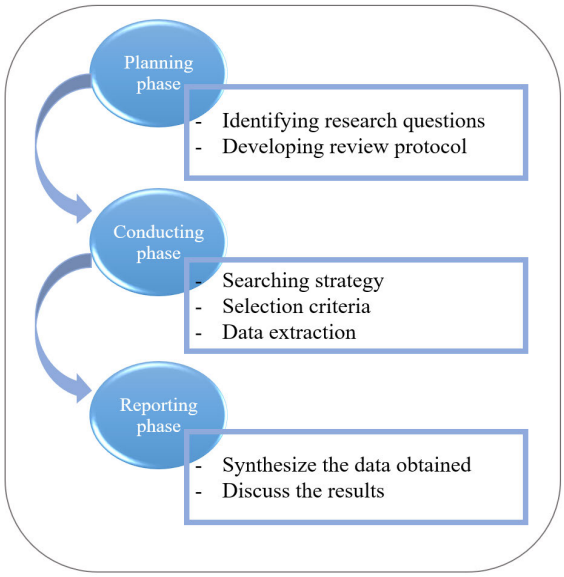

FIGURE 2. Research review methodology.

networks or acquire undesired control. WPA2 was modified and updated to WPA3 in an effort to improve security by addressing these vulnerabilities. Table 1 shows attacks in WPA3 protocol. In Table 1, the attacks were categorized as *Before WPA3* and *After WPA3*. *Before WPA3* means that attacks do exist in the previous protocols and are still not solved by WPA3. *After WPA3* means that attacks occurred only in WPA3 because of either encryption methods or the handshake process. On the other hand, there are attacks that WPA3 was able to solve and prevent such as Handshake Capture Dictionary Attack, PMKID Hash Dictionary Attack, Handshake Capture En/Decryption Attack, and finally the most important one is the KRACK Attack that was the main reason to develop WPA2 to WPA3 [1].

III. RESEARCH METHODOLOGY

This work aims to provide a systematic review of the latest security certificate, WPA3. The guideline for performing this review is by following Kitchenham and Charter's method [7]. Their method composes of three stages: planning, conducting the review, and reporting the findings, as shown in Figure 2. The *planning stage* is the first stage where the questions of the research and the review protocol are defined. The second stage is the *conducting stage* where the review protocol will be implemented. The review protocol outlines the search strategy and criteria for selecting and excluding the research papers and extracting the required data. *Reporting stage*, the final stage involves synthesizing the data obtained.

A. RESEARCH QUESTIONS

The primary objective of this work is to provide a review of the emergence of the wireless security certificate WPA3. The following research questions were developed in line with the primary objective:

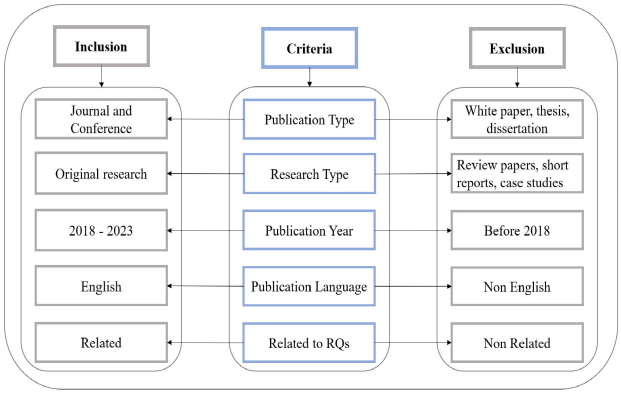

FIGURE 3. Inclusion and exclusion criteria.

1. ***RQ1: What are the reasons for the emergence of the security certificate WPA3?***
2. ***RQ2: What is the encryption method used in WPA3 that differs from its predecessors?***
3. ***RQ3: What are the attacks that WPA3 was able to prevent, and the attacks still could not prevent?***

B. DATA SEARCH STRATEGY

The search strategy is the most important part of a systematic literature review. The steps here are to define the keywords and the source of the study. The search for articles in the English language was conducted from the following digital libraries:

- Google Scholar
- ACM Digital Library
- Springer
- IEEE Xplore
- ArXiv
- Science Direct

For the keywords, they were derived from the research questions and Boolean operator (ORs) was used to limit our research and to define the search string, as follows:

"WPA3" OR "WPA3 Attack" OR "WPA3 Security" OR "WPA3 Certificate"

Based on the keywords searches in the digital libraries, 416 articles were collected.

C. PAPERS SELECTION CRITERIA

Initially, 416 papers were collected based on the search terms mentioned earlier. Then, these papers were filtered based on their relatedness to our topic in this review. The filtration process is as follows: First, remove all the duplicated articles that were collected from the different digital libraries. Before the articles were accepted as primary articles, these articles are analyzed against the inclusion and exclusion criteria, which are shown in Figure 3. Also, from references in the selected articles, additional related articles were investigated and applied with the search strategy.

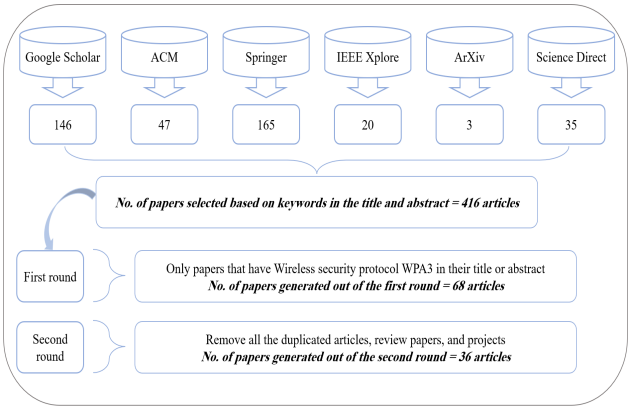

FIGURE 4. Articles selection process.

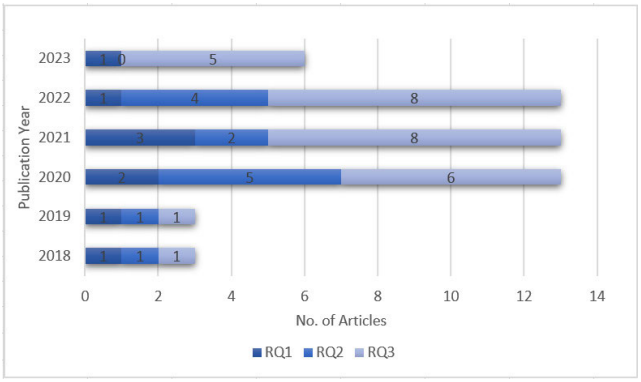

FIGURE 5. Number of articles based on publication year.

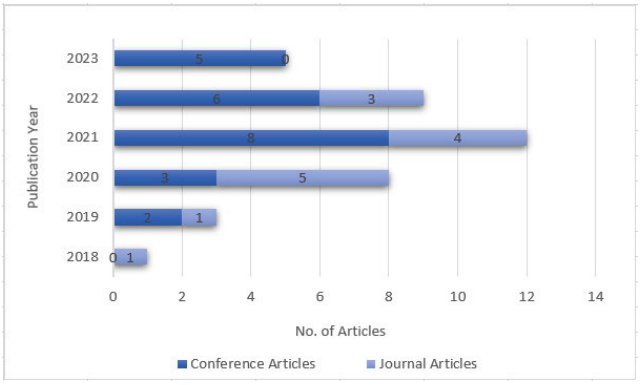

FIGURE 6. Number of articles based on publication type.

D. PAPERS SELECTION PROCESS

To perform the selection process, the papers were chosen based on the search string, title, abstract, and keywords. From 416 papers, authors investigated papers that have security certificate WPA3 in their title and abstract, and the result was 68 papers. This is because some papers have WPA3 in their title or abstract, but it does not represent the network security protocol. It is either referring to a chemical factor or a symbol for different topics. Out of 68 papers, 25 were excluded because of duplication between digital libraries, 4 as review papers, 1 as a white paper, and 2 as Bachelor's degree projects, which leaves us with 36 articles. The selection process is shown in Figure 4.

E. DATA EXTRACTION

The aim of this step is to analyze the final list of papers to extract the required information to answer our research questions. To avoid bias in the data extraction process, a data extraction form was developed. The following information was extracted from each paper: title of the paper, the publication year of the paper, publication type, RQ1, RQ2, and RQ3.

F. DATA SYNTHESIZING

The data that is collected from the selected papers have to be synthesized in a certain manner to provide answers to our research questions. Section IV exhibits the obtained data in different formats such as tables and figures.

IV. RESULTS AND DISCUSSION

A. RESULTS

This section elaborates the outcomes of the review. An overview of the selected papers is first presented. The outcomes of each research question are explained in detail in the following sections. Table 2 shows the selected papers based on research article number, title, publication type, and year of publication.

The publication years of the selected papers from 2018 to 2023 regarding the security certificate WPA3 per year are shown in Figure 5. The figure shows the number of papers that discussed or mentioned the research question, knowing that some selected papers discussed more than one RQ, and in the figure it will be counted under each RQ. As shown in Figure 5, most of the articles were about RQ3 that focuses mainly on attacks in WPA3. Then, RQ2 focuses on the operation mode and encryption method in WPA3. Finally, the RQ1 focuses on the reason for implementing WPA3. The year 2021 received the highest number of publications, where it has 12 publications. Figure 6 shows the number of journal and conference papers published from 2018 to 2023. 24 articles were conference papers, which represent 63% of the total selected articles. The rest were journal papers (14 articles), which represent 37%.

1) RESEARCH QUESTION 1 - WHAT ARE THE REASONS FOR THE EMERGENCE OF THE SECURITY CERTIFICATE WPA3?

The first research question aims to show the need and the importance of the emergence of the security certificate WPA3. There are many security flaws in the existing wireless LAN that attackers might exploit to wreak a wide range of harm or obtain unwanted control. The release of WPA3 was mainly to address the security flaws and vulnerabilities in its predecessors and to enhance the current state of security. According to Wi-Fi organization [16], the main reasons for

TABLE 2. Selected research articles.

ID	TITLE	TYPE	YEAR	REF.
M1	A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3	Jour.	2018	[1]
M2	An Overview of Protocols-Based Security Threats and Countermeasures in WLAN	Conf.	2023	[6]
M3	WPA 3 - Improvements over WPA 2 or broken again?	Jour.	2020	[10]
M4	Securing home Wi-Fi with WPA3 personal	Conf.	2021	[12]
M5	Dragonblood A Security Analysis of WPA3's SAE Handshake	Jour.	2019	[14]
M6	WPA3: The Greatest Security Protocol That May Never Be	Conf.	2021	[17]
M7	Will WPA3 really provide Wi-Fi security at a higher level?	Conf.	2019	[18
M8	Disruption and Protection of Online Synchronous Learning Environments via 802.11 Manipulation	Conf.	2021	[19]
M9	Bad-Token: Denial of Service Attacks on WPA3	Conf.	2019	[20]
M10	Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd	Conf.	2020	[21]
M11	Understanding Server Authentication in WPA3 Enterprise	Jour.	2020	[22]
M12	WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique	Conf.	2021	[23]
M13	How is your Wi-Fi connection today? DoS attacks on WPA3-SAE	Jour.	2022	[24]
M14	WPA3 Connection Deprivation Attacks	Conf.	2020	[25]
M15	A Wireless Intrusion Detection System for 802.11 WPA3 Networks	Conf.	2022	[26]
M16	RIDS: Real-time Intrusion Detection System fWPA3-enabled Enterprise Networks	Conf.	2022	[27]
M17	A Chosen Random Value Attack on WPA3 SAE Authentication Protocol	Jour.	2022	[28]
M18	Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3	Conf.	2022	[29]
M19	Stateless Re-Association in WPA3 Using Paired Token	Jour.	2021	[30]
M20	Active Dictionary Attack on WPA3-SAE	Conf.	2021	[31]
M21	Dragon Shield: An Authentication Enhancement for Mitigating Side-Channel Attacks and High Computation Overhead in WPA3-SAE Handshake Protocol	Conf.	2022	[32]
M22	A Time-Memory Trade-Off Attack on WPA3's SAE-PK	Conf.	2022	[33]
M23	Dragonblood is Still Leaking: Practical Cache-based Side-Channel in the Wild	Jour.	2020	[34]
M24	On the Robustness of Wi-Fi deauthentication Countermeasures	Conf.	2022	[35]
M25	Simultaneous Deauthentication of Equals Attack	Conf.	2021	[36]
M26	ComPass: Proximity Aware Common Passphrase Agreement Protocol for Wi-Fi Devices Using Physical Layer Security	Conf.	2021	[37]
M27	Physical Layer Encryption for Wireless OFDM Communication Systems	Jour.	2020	[38]
M28	PoEx: Proof of Existence for Evil Twin Attack Prevention in Wi-Fi Personal Networks	Conf.	2021	[39]
M29	Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset	Jour.	2021	[40]
M30	Towards Understanding and Enhancing Association and Long Sleep in Low-Power WiFi IoT Systems	Jour.	2021	[41]
M31	Evolution of Wi-Fi Protected Access: Security Challenges	Jour.	2020	[42]
M32	The COVID-19 pandemic and remote working did not improve WLAN security	Jour.	2022	[43]
M33	From Dragondoom to Dragonstar: Side-Channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake	Conf.	2023	[44]
M34	Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11n	Conf.	2023	[45]
M35	Battery Drain using WiFi Beacons	Conf.	2023	[46]
M36	Owfuzz: Discovering Wi-Fi Flaws in Modern Devices through Over-The-Air Fuzzing	Conf.	2023	[47]

releasing and developing WPA3 is that WPA3 makes authentication more reliable, boosts the cryptographic strength for highly sensitive data markets, and keeps mission-critical networks resilient. [17], [18] sought to spread awareness, importance, and why people should deploy WPA3 in their networks. Both researchers believed that WPA3 is an excellent security protocol and excels its predecessors, and not only the technical issues that affect the security of a network but also socio-technical activities of how people behave. References [10] and [19] showed how WPA3 can solve vulnerabilities in the previous wireless security protocols and be a viable replacement. According to our selected articles, 9 out of the selected papers mentioned the need for the emergence of WPA3 due to several reasons such as avoidance of attacks, improvements of authentication and encryption methods, and others, as shown in Table 3.

2) RESEARCH QUESTION 2 - WHAT IS THE ENCRYPTION METHOD USED IN WPA3 THAT DIFFERS FROM ITS PREDECESSORS?

Based on end users' requirements, there are two modes of operations in WPA3: home and business, as known as

TABLE 3. Reason for the emergence of WPA3.

ID	Reasons
M1, M6, M15	Avoid attacks in its predecessors
M11	WPA3 Enterprise prevents supplicant setup settings such as "skip certificate validation"
M4, M7	WPA3 Personal authentication mechanism makes it hard to break the passwords and to decrypt data captured
M8, M31, M32	The improvements in WPA3 in terms of authentication, encryption, management frames, and strong default settings make it more resilient and robust

TABLE 4. Articles based on the operation mode and encryption method.

ID	Mode of Operation and Encryption
M1, M3, M9, M10, M13, M14, M17, M18, M19, M22, M23, M26, M31	WPA3-Personal
M10, M23, M31	WPA3-Enterprise
M1, M3, M10	WPA3-Transition
M1, M3, M10, M24, M31	Dragonfly handshake

WPA3-Personal and WPA3-Enterprise. Although there is not much difference between them, WPA3-Enterprise considered being more secure as it is designed to protect more sensitive data. The encryption method in WPA3 depends on its mode of operation. WPA3-Personal is used when a Wi-Fi device only supports WPA3 and is called WPA3-SAE as it supports SAE as an encryption method [1]. WPA3-Enterprise is used in enterprise environments such as industrial and government networks and the encryption in this mode uses 192-bit and is called EAP-pwd [20]. In addition, there is also a transition mode, which is indicated as WPA3-SAE transition. This mode allows Wi-Fi devices that only support WPA3 to connect to the WPA2 network.

WPA3-SAE, a variation of the Dragonfly key exchange specified in RFC 7664, replaces the so-called Open System authentication before network association [1]. The Dragonfly handshake protects against offline dictionary assaults while providing forward secrecy, and it was utilized in practice by both WPA3 and EAP-pwd [21].

In EAP-pwd, the devices will store passwords in plaintext or in hashed forms, and all ciphers must offer at least 192 bits of security. In this mode, the access point initiates the handshake, commit and confirm frames are encapsulated in 802.1X frames [21].

Since the transition mode is used to accommodate devices that support WPA3 and WPA2 using the same password, AP offers Management Frame Protection (MFP) as an optional feature in this mode, where the older clients connect using WPA2 without MFP and the newer ones using WPA3-SAE with MFP enabled [21].

Based on Table 4, most of the published articles are based on a personal mode of operation, WPA3-SAE. Some are in transition mode and only one article (M10) had all the modes, in addition to a description of the Dragonfly encryption method.

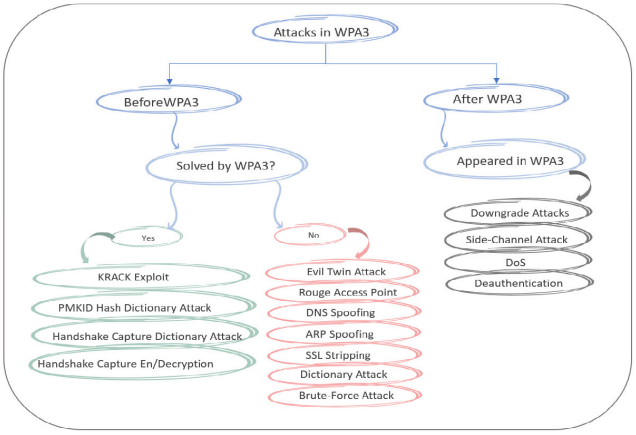

FIGURE 7. Attacks before and after the release of WPA3.

3) RESEARCH QUESTION 3 - WHAT ARE THE ATTACKS THAT WPA3 WAS ABLE TO PREVENT, AND THE ATTACKS STILL COULD NOT PREVENT?

Until the discovery of the KRACK attack on WPA2 in 2017, WPA2 was considered the most secure wireless protocol [11]. WPA3 came to fix all the shortcomings of its predecessors, as it was released to address the vulnerabilities in the previous protocols and improve the present level of security. With all the improvements in design, WPA3 was proven to be vulnerable to some types of attacks [14]. WPA3 can prevent some attacks, but it is still vulnerable against other attacks. In addition, there are attacks that appeared after the release of WPA3.

During the research on WPA3, the articles that were found are the articles that are explaining the attacks in WPA3 and included the articles that are trying to find a solution to avoid attacks and intrusions. In this research question, the attacks that are still affecting WPA3 and attacks that have been prevented are presented. From the selected articles in Table 2, there were 24 articles that provided an explanation of WPA3 attacks in different ways. For example, out of these 24 articles, 19 articles imitate how attacks happen in WPA3 and 5 articles provided a brief description of the attacks. Out of 24 articles, 20 articles proposed an update and solution to avoid attacks in the WPA3 protocol.

From the previous articles, the attacks in WPA3 were found. Figure 7 shows the attacks before and after the deployment of the WPA3 protocol. In terms of attacks *Before WPA3*, the attacks were divided into two sections, one that was solved by WPA3 and the other one is still unsolved. For attacks *After WPA3*, it shows the attacks that occurred due to the encryption methods in WPA3.

Figure 8 illustrates the occurrence of attacks in the selected articles, which are still affecting WPA3. DoS and downgrade attacks got the highest repetition where they were mentioned seven times in the selected articles, followed by

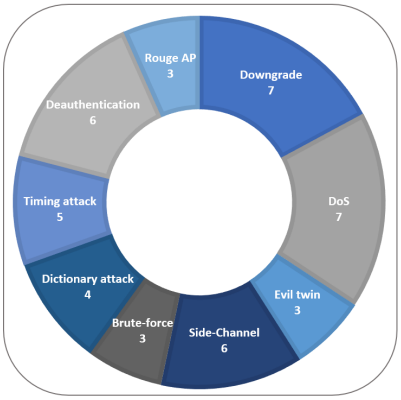

FIGURE 8. Attacks in WPA3 based on chosen articles.

deauthentication attacks and side-channel attacks (six times). Timing attacks along with dictionary attacks were mentioned five times and four times, respectively. Three times appeared in evil twin, rogue AP, and brute-force attacks. There are other types of attacks that were mentioned in the selected papers only one time, such as DNS spoofing and SSL stripping in [1], time-memory trade-off attacks in [33], Miscellaneous Leaks in [34], and Ghost attacks in [37].

B. DISCUSSION

This work applied a systematic procedure to provide a proper understanding of the wireless security certificate WPA3. There are three research questions that were formulated and answered to achieve the objective. From the research that has been done, the main ideas in the articles were the effect of the attacks, how to avoid attacks, imitate attacks, software used to perform attacks, software used to avoid attacks, solutions, and updates to improve WPA3 certificate.

This part of the paper intends to exhibit what other researchers did regarding their work on WPA3. The results can be useful in highlighting the direction of future research. This part provides the following information:

- Tools and software used to generate attacks and monitor the channels.
- The impact of different attacks on WPA3.
- Techniques that were added to WPA3 to provide more security.

There are different tools and methods used to generate attacks that affects WPA3 for different purposes and to monitor the channel, such as Aircrack-ng that is used to launch and generate WPA3 attacks [19], [23], [40], MDK3 to gather information [19], Hostapd-2.9 used to perform attacks in [20], [24], [26], and [35]. Dragondrain used to generate attacks in [21] and authors used MicroWalk to detect the attacks. On the other hand, authors developed a software to create attacks, such as [31] proposed software to perform active attacks by picking up passwords from the dictionary file and trying different passwords until they connect with the access point. [33] performed attacks by precomputing a table that converts an SAE-PK password into a valid modifier and public key for which the private key is known.

Several research have been implemented to test the ability of WPA3 to prevent attacks and to study the effects of these attacks. Researchers in [19] and [29] tested the ability of Management Frame Protection (MFP) in WPA3, where they showed the ability of WPA3 to prevent disassociation and deauthentication attacks, in addition to increase its efficiency in preventing attacks. On the other hand, [35] showed that un-enabling of MFP, allowed for deauthentication attacks and made WPA3 vulnerable.

An evaluation of the efficiency of dragonfly handshake and SAE in WPA3 was done in [14], [20], [21], [24], [28], [33], and [36], where researchers sought to analyze these features and explore the vulnerabilities in WPA3's handshake and SAE. In [14], timing or cache-based side-channel leaks were exploited to recover the password of WPA3 by downgrade from WPA3-SAE to WPA2-PSK. Reference [20] discovered bad-token vulnerability in SAE causing DoS attacks. Reference [21] proved that the minor changes in password encoding would prevent vulnerabilities in dragonfly handshake.

Reference [24] showed that if attacker is persistent enough, then SAE is vulnerable to all DoS attacks. Reference [28] proved that SAE protocol is weak to a chosen random value attack and its extension attacks. Finally, WPA3Fuzz strategy is used to identify the vulnerabilities in SAE and MFP against DoS attacks. To prove weakness in SAE, [34] implemented Cache attack to show that this attack is able to leak some information on the password and [25] presented three DoS attacks that affect the availability of WPA3 networks.

Reference [44] presented a collection of side-channel vulnerabilities called Dragondoom by targeting password conversion methods in order to help attackers to recover WPA3 passwords. Owfuzz, an over-the-air fuzzing approach implemented by [47] to test all three types of WPA3 Wi-Fi frames (management, control, and data).

References [1] and [23] worked on comparing the attacks in WPA2 and WPA3 and both concluded that WPA3 can provide more security than any of its predecessors. The previous works were on personal mode of WPA3, the effects of attacks on WPA3- transition mode is found in [12], and [22] presented the defensive power and potential impact to mitigate the risk of attacks in WPA3- enterprise mode. Reference [45] concluded that WPA3 offered higher security than WPA2, even though the CPU utilization of WPA3 is higher. Reference [46] found two attacks on Wi-Fi beacons that have an effect on the battery life of wireless devices and proved that WPA3 is still vulnerable against them.

There was a group of researchers that worked to add more security and reliability to WPA3 such as in [26], [27], [30], [32], [37], [38], [39], [40], and [41]. An intrusion detection System (IDS) was used in [26] and [27] to add more security to WPA3 networks, where authors implemented a signature-based IDS to detect WPA3 attacks. In [40], authors

TABLE 5. Articles based on WPA3 attacks.

ID	DESCRIPTION	ADVANTAGES	LIMITATIONS
M1	An analysis of WPA2 and WPA3 attacks and determine how these attacks exploited wireless security protocols. Authors suggested solutions to avoid some of these attacks.	Novel attack model is presented to provide a comprehensive view of the attacks on Wi-Fi security protocols.	No analysis to any attack related to SAE was done, which is the main feature of WPA3.
M4	An investigation was done to check if there is a way that downgrade attacks are not feasible in WPA3-transition mode.	Recommendations were proposed to make WPA3 more secure and show the techniques to prevent downgrade attacks	If there is no mutual authentication, the network will be less secure.
M5	Authors discovered a set of vulnerabilities in SAE named Dragonblood.	Authors were able to show that such attacks can recover WPA3 passwords and downgrade the network from WPA3 to WPA2. They also proposed some countermeasures to mitigate these attacks.	For resource-constrained devices, the countermeasures will not be effective as it will be costly on lightweight processors.
M8	Authors created an online learning environment to study the impact of disassociation and deauthentication attacks, where they collected information through Aircrack-ng suite and MDK3 to launch a disassociation attack against an instructor's router.	Authors suggested potential mitigation and prevention strategies to overcome these attacks.	The deployment of PMF in WPA3 makes disassociation and deauthentication attacks obsolete.
M9	Hostapd-2.7 and wpa-supplicant-2.7 were used to implement attacks and show the vulnerabilities of WPA3 such as DoS attacks.	Authors proposed a time-based countermeasure to mitigate the attack.	Raspberry Pi does not support WPA3-SAE, so a wireless card is added to fulfill the requirements.
M10	Authors evaluated the security of Dragonfly handshake through generating attacks using Dragondrain and detecting attacks using MicroWalk.	Authors were able to analyze the complexity of leaked information and proposed backward-compatible defenses to prevent attacks such as downgrade, DoS, and side-channel.	The patched implementations made by authors are still vulnerable to side-channel attacks due to: - Authors were not able to fully analyze the handshake due to the variety of cryptographic groups in Dragonfly. The attacks generated only abuse the password encoding method.
M11	Authors studied the second version of WPA3 that was released by Wi-Fi Alliance in December 2019.	Authors were able to present the defensive power and potential impact of this version to mitigate the risk of attacks, especially in enterprise Wi-Fi network.	The new mechanisms of WPA3 allow to minimize the risk by providing different security–cost trade-offs, and the minimal cost does not provide a strong defensive power.
M12	Aircrack-ng is used to perform attacks on the WPA3 network and see the effect of the attacks compared to other security networks.	Authors concluded that WPA3 is more secure than its predecessors.	- Authors could only perform the attacks on one smartphone because of its ability to be downgraded from WPA3 to WPA2.
M13	Wi-Fi 6 Along with OpenBSD hostapd were used to address the vulnerability of SAE against DoS attacks.	- Authors provided an appraisal on the mechanism of SAE against DoS.	To perform effective DoS attacks, authors had to send a spray of spoofed SAE frames in high-speed burst.
M14	Three denial-of-service attacks were presented by authors that have affected the availability of WPA3 networks.	Authors proved these attacks were able to deprive users of connecting to the networks. They also presented countermeasures to avoid such attacks.	The countermeasures presented by authors suggested users should not reply when receiving the first probe, and by doing this, the user will spend longer time than usual to respond.
M15	Proposed a signature-based intrusion detection system based on WPA3 attacks.	- The model could detect and prevent attacks. Provided schemes for mitigating the impact of some attacks	Not all WPA3 attacks have been examined in their work.
M16	an Intrusion Detection System of a two-stage solution to detect attacks in WPA3 networks based on a Machine Learning controller.	- Authors were able to achieve 99% accuracy when applying their dataset to the Random Forest classifier. - Provide their dataset for public use.	They did not include all of WPA3's attacks in their work and dataset.
M17	Authors showed the weaknesses of SAE to a chosen random value attack and its extension attacks.	Authors proved a way of attacking SAE and then provided some suggestions for protection.	The attacks are effective only if the password is short where the random space is small.
M18	The capability of Protected Management Frame (PMF) against deauthentication attacks were tested.	Identifying the reasons behind deauthentication attacks despite enabling PMF and suggested countermeasures to avoid such attacks.	Authors only investigate the effect on WPA3-Personal mode, no Enterprise or transition mode were tested.
M20	A software is used to perform active attacks by collecting passwords from the dictionary file and virtual machines that act as legitimate wireless clients to speed up attacking.	Authors proposed a method to attack WPA3 to recover the password.	If the access point has a rule where each client can try with limited attempts, the access point will reject this client and send a deauthentication response after some incorrect attempts.
M22	Authors analyzed the impact of the SAE-PK protocol through time-memory trade-off attacks by precomputing a table that converts an SAE-PK password into a valid modifier and public key for which the private key is known.	Authors were able to reduce the computational costs of attacking from 48 CPU years to roughly two weeks by targeting an SSID used by large number of networks.	The attack will be not feasible if the PKHash is updated to start with a single byte that represents the length of the SSID.

TABLE 5. *(Continued.)* **Articles based on WPA3 attacks.**

M23	Authors applied attacks on two open-source projects: iwd and FreeRADIUS to show how attackers can use cache attacks in order to leak some information on the password.	Provided a full Proof of Concept for their vulnerability on Intel's implementation and showed that this vulnerability allows recovering more bits of information with fewer measurements.	If there is no branch-free implementation of the loop, there is a possibility for residual leakage.
M24	Inspect the robustness of WPA3 against deauthentication attacks.	Presented countermeasures to better defend against deauthentication attacks.	Proved that Management Frame Protection is insufficient to prevent deauthentication attacks.
M25	WPA3Fuzz Strategy was used to identify vulnerabilities and errors in the Simultaneous Authentication of Equals process and Protected Management Frames mechanism.	Their strategy discovered vulnerabilities that are exploited into Denial-of-Service attacks.	To avoid the vulnerabilities discovered, manual intervention is required by the end users.
M26	ComPass protocol is used to protect users from guessing attacks by replacing the user-selected passphrases with automatically generated ones.	ComPass protocol was able to increase the number of guesses required for the automatic passphrase to be cracked using dictionary attacks more than the one generated by a human.	The protocol works with Wi-Fi devices within 3m only.
M28	Proof of Existence (PoEx) scheme is presented to detect Evil twin attacks.	PoEx scheme was able to make lifetime forging difficult as the computations required are high and reduced the overhead on the network's throughput.	PoEx scheme works on networks using the lifetime hashing calculation.
M29	Authors created a dataset that has a wide variety of attacks to help build an intrusion detection system.	Authors included attacks from IEEE 802.3 networks, IEEE 802.1X Extensible Authentication Protocol (EAP) environment, and 802.11-oriented attacks such as in WPA2 and WPA3.	Their work focused on attacks from previous security protocols WPA/WPA2. Not much attacks on WPA3.

created a dataset that contains few numbers of WPA3 attacks in order to be used later for different purposes.

ComPass is a protocol created by [37] to supplement WPA2/WPA3 by replacing user-selected passphrases with automatically generated ones to avoid guessing attacks. Reference [38] increased the security of WPA3 through implemented encryption techniques in the physical layer based on frequency induction for OFDM signals. Proof of Existence (PoEx) scheme introduced in [39] is used to protect the network against Evil Twin attacks, where authors witnessed besides protecting the network, there are improvements done on the network through the lifetime forging and network's throughput.

Reference [30] applied Paired Token scheme to replace Pairwise Master Key (PMK) with the onetime authenticated key establishment to deliver high performance to a larger number of clients using WPA3 networks. For the purpose of deriving a high entropy shared secret key, [32] used the standard generator for the cyclic group and proposed Block Encryption-based Password Authenticated Diffie-Hellman Key Establishment (BEPAKE) protocol between the access point and the client. Reference [41] did an analysis to minimize the association overhead caused by key computation in WPA2 and WPA3 and proved that the beacon listen interval and channel utilization influence the wake-up delay of low-power stations.

In the end, from the previous discussion, it was shown that most of the researchers tried to test the capability of WPA3 protocol to provide security to either personal or enterprise networks. Previous researchers tried to find a way to penetrate WPA3 protocol by performing and creating attacks through Aircrack-ng, hostapd, Dragondrain, etc. They used software to detect attacks such as MDK3 and MicroWalk. Most of their research was done on cutting the connection from WPA3's access point or preventing users from entering a WPA3 network. Downgrade attacks, deauthentication attacks, and DoS attacks were the major concerns for numerous researchers to provide countermeasures, as they showed the vulnerability of WPA3 against these attacks. From here, we conclude that the main issues in WPA3 are due to encryption and encoding methods, where most of the previous works tried to recommend solutions to avoid attacks related to encryption and encoding methods.

From the research that has been done, to make WPA3 more secured to be used and to reduce the probability of users and networks being hacked, an improvement on WPA3 itself or on WPA3 environment can be done, which can be summarized as follows:

- The improvement on WPA3 protocol can be done in the way of generating the password. The previous work [36], [37] focused on generating passwords automatically to increase security. To provide more security to the WPA3 network, we believe that the WPA3 password should be generated using a computer and then changing this password automatically from time to time. Such action would increase the number of guesses required to crack the password, which results in reducing the probability of the network being hacked.
- The improvement of the WPA3 environment can be implemented through adding an intrusion detection system (IDS) capable of detecting and preventing attacks. The previous works [25], [26] added IDS based on knowing few attacks of WPA3. We believe that

implementing IDS-based machine learning would allow for better detection and prevention of WPA3 attacks. Machine learning models proved their ability through the years in different aspect of life, and so, developing machine learning model that has full awareness of WPA3 attacks would provide more reliability and security to WPA3 networks, where the model will be trained and tested on all WPA3 attacks, which will then prevent them from causing harm on the network.

Finally, despite the attacks on the WPA3 protocol, all the existing works proved the capability and ability of WPA3 protocol to provide security more than its predecessors. More explanation of the works that focused on providing details of WPA3 attacks and how to prevent them is given in Table 5.

V. LIMITATION OF THE STUDY

This systematic literature review was conducted with a focus on selected studies on wireless security certificate WPA3. The search process was performed using a limited number of keywords, which resulted in a limited number of selected papers that sought to purely focus on WPA3 to help researchers who want to know more about this protocol. The articles were limited to journal and conference articles between the years 2018 and 2023. Several non-relevant research articles were excluded based on our inclusion/exclusion criteria.

VI. 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. From the research conducted, it is concluded that most of the related works of WPA3 are focusing on finding attacks, generating attacks, and on testing how WPA3 is capable of preventing attack. Researchers used different tools and methods to achieve their goal such as Aircrack-ng, MDK3, Hostapd-2.9, MicroWalk, and Dragondrain. Other researchers sought to improve WPA3 by adding different approaches and methods to the wireless security protocol, such as Intrusion Detection System, ComPass approach, Paired Token scheme.

The review investigated the related studies that were published between the years 2018 and 2023. Thirty-six articles were studied to answer three research questions, and the results achieved as follows: For RQ1, the main reason behind the release of the WPA3 protocol is to provide more security and to overcome attacks in its predecessors. The results of RQ2 show how implementing Simultaneous Authentication of Equals (SAE), which is the Dragonfly handshake process in WPA3 and Protected Management Frame (PMF), played an important role in increasing the security in WPA3. The findings of RQ3 show that despite the improvement of WPA3, there are still some attacks that WPA3 cannot prevent. In this research question, the attacks that were prevented and the attacks that were unsolved are shown. Finally, a discussion on the selected papers was addressed.

Lastly, it can be concluded that the WPA3 protocol is a recent security protocol that excels the previous protocols. Based on this review, a recommendation to researchers to conduct more research on ways to improve this protocol, as follows: exploiting the capability of computer-generated passwords to work on the WPA3 protocol itself or by taking advantage of Machine Learning ability to build an Intrusion detection model capable of detecting attacks with high accuracy and low false alarm rate.

REFERENCES

[1] C. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for Wi-Fi and WPA3," *Electronics*, vol. 7, no. 11, p. 284, Oct. 2018.

[2] K. Moissinac, D. Ramos, G. Rendon, and A. Elleithy, "Wireless encryption and WPA2 weaknesses," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 1007–1015.

[3] B. I. Reddy and V. Srikanth, "Review on wireless security protocols (WEP, WPA, WPA2 & WPA3)," *Int. J. Scientific Res. Comput. Sci., Eng. Inf. Technol.*, vol. 5, pp. 28–35, Jul. 2019.

[4] I. S. Al-Mejibli and D. N. R. Alharbe, "Analyzing and evaluating the security standards in wireless network: A review study," *Iraqi J. Comput. Informat.*, vol. 46, no. 1, pp. 32–39, Jun. 2020.

[5] D. Faíscas, "(In) security in Wi-Fi networks: A systematic review," *ARIS2-Adv. Res. Inf. Syst. Secur.*, vol. 2, no. 2, pp. 17–23, 2022.

[6] N. K. Ojha and E. Baray, "An overview of protocols-based security threats and countermeasures in WLAN," in *Proc. 4th Int. Conf. Emerg. Technol. (INCET)*, May 2023, pp. 1–6.

[7] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature reviews in software engineering version 2.3," *Engineering*, vol. 45, no. 4, p. 1051, 2007.

[8] A. Sari and M. Karay, "Comparative analysis of wireless security protocols: WEP vs WPA," *Int. J. Commun., Netw. Syst. Sci.*, vol. 8, no. 12, pp. 483–491, 2015.

[9] G. Mironov, "Challenges of wireless security in the healthcare field: A study on the WPA3 standard," Bachelor Degree Project, Linnaeus Univ., Sweden, 2020.

[10] M. Appel and I. S. Guenther, "WPA 3-Improvements over WPA 2 or broken again?" *Network*, vol. 7, pp. 1–4, Nov. 2020.

[11] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1313–1328.

[12] E. Lamers, R. Dijksman, A. van der Vegt, M. Sarode, and C. de Laat, "Securing home Wi-Fi with WPA3 personal," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2021, pp. 1–8.

[13] B. Scheuermann, "Model based fuzzing of the WPA3 Dragonfly handshake," M.S. thesis, Humboldt-Universität zu Berlin, Germany, 2019.

[14] M. Vanhoef and E. Ronen, "Dragonblood: A security analysis of WPA3's SAE handshake," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 383, Apr. 2019.

[15] D. Clarke and F. Hao, "Cryptanalysis of the dragonfly key exchange protocol," *IET Inf. Secur.*, vol. 8, no. 6, pp. 283–289, Nov. 2014.

[16] wi-fi.org. *Security | Wi-Fi Alliance*. Accessed: May 18, 2020. [Online]. Available: https://www.wi-fi.org

[17] G. Sagers, "WPA3: The greatest security protocol that may never be," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2021, pp. 1360–1364.

[18] M. Bednarczyk and Z. Piotrowski, "Will WPA3 really provide Wi-Fi security at a higher level?" in *Proc. 12th Conf. Reconnaissance Electron. Warfare Syst.*, Mar. 2019, pp. 369–376.

[19] M. Tigner and H. Wimmer, "Disruption and protection of online synchronous learning environments via 802.11 manipulation," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Apr. 2021, pp. 1–6.

[20] K. Lounis and M. Zulkernine, "Bad-token: Denial of service attacks on WPA3," in *Proc. 12th Int. Conf. Secur. Inf. Netw.*, Sep. 2019, pp. 1–8.

[21] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of WPA3 and EAP-pwd," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 517–533.

[22] A. Bartoli, "Understanding server authentication in WPA3 enterprise," *Appl. Sci.*, vol. 10, no. 21, p. 7879, Nov. 2020.

[23] E. Baray and N. K. Ojha, "'WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique,'" in *Proc. 5th Int. Conf. Comput. Methodolog. Commun. (ICCMC)*, Apr. 2021, pp. 23–30.
[24] E. Chatzoglou, G. Kambourakis, and C. Kolias, "How is your Wi-Fi connection today? DoS attacks on WPA3-SAE," *J. Inf. Secur. Appl.*, vol. 64, Feb. 2022, Art. no. 103058.
[25] K. Lounis and M. Zulkernine, "WPA3 connection deprivation attacks," in *Proc. Int. Conf. Risks Secur. Internet Syst.*, Hammamet, Tunisia: Springer, Oct. 2020, pp. 164–176.
[26] N. Dalal, N. Akhtar, A. Gupta, N. Karamchandani, G. S. Kasbekar, and J. Parekh, "A wireless intrusion detection system for 802.11 WPA3 networks," in *Proc. 14th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2022, pp. 384–392.
[27] R. Saini, D. Halder, and A. M. Baswade, "RIDS: Real-time intrusion detection system for WPA3 enabled enterprise networks," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2022, pp. 43–48.
[28] S. Sun, "A chosen random value attack on WPA3 SAE authentication protocol," *Digit. Threats, Res. Pract.*, vol. 3, no. 2, pp. 1–8, Jun. 2022.
[29] K. Lounis, S. H. Ding, and M. Zulkernine, "Cut it: Deauthentication attacks on protected management frames in WPA2 and WPA3," in *Proc. Int. Symp. Found. Pract. Secur.* Paris, France: Springer, Dec. 2021, pp. 235–252.
[30] B. Lee, "Stateless re-association in WPA3 using paired token," *Electronics*, vol. 10, no. 2, p. 215, Jan. 2021.
[31] M. Patel, P. Amritha, and R. S. Jasper, "Active dictionary attack on WPA3-SAE," in *Advances in Computing and Network Communications*, vol. 1. Cham, Switzerland: Springer, 2021, pp. 633–641.
[32] R. C. Hansdah, J. Jamwal, and R. B. Gudivada, "Dragonshield: An authentication enhancement for mitigating side-channel attacks and high computation overhead in WPA3-SAE handshake protocol," in *Proc. 23rd Int. Conf. Distrib. Comput. Netw.*, Jan. 2022, pp. 188–197.
[33] M. Vanhoef, "A time-memory trade-off attack on WPA3's SAE-PK," in *Proc. 9th ACM ASIA Public-Key Cryptogr. Workshop*, May 2022, pp. 27–37.
[34] D. De Almeida Braga, P.-A. Fouque, and M. Sabt, "Dragonblood is still leaking: Practical cache-based side-channel in the wild," in *Proc. Annu. Comput. Secur. Appl. Conf.*, Dec. 2020, pp. 291–303.
[35] D. Schepers, A. Ranganathan, and M. Vanhoef, "On the robustness of Wi-Fi deauthentication countermeasures," in *Proc. 15th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, May 2022, pp. 245–256.
[36] S. Marais, M. Coetzee, and F. Blauw, "Simultaneous deauthentication of equals attack," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Nanjing, China: Springer, Dec. 2020, pp. 545–556.
[37] K. Reaz and G. Wunder, "ComPass: Proximity aware common passphrase agreement protocol for Wi-Fi devices using physical layer security," in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.* Cham, Switzerland: Springer, 2022, pp. 263–275.
[38] M. Jacovic, K. Juretus, N. Kandasamy, I. Savidis, and K. R. Dandekar, "Physical layer encryption for wireless OFDM communication systems," *J. Hardw. Syst. Secur.*, vol. 4, no. 3, pp. 230–245, Sep. 2020.
[39] K. Murugesan, K. K. Thangadorai, and V. N. Muralidhara, "PoEx: Proof of existence for evil twin attack prevention in Wi-Fi personal networks," in *Proc. 8th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2021, pp. 92–98.
[40] E. Chatzoglou, G. Kambourakis, and C. Kolias, "Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset," *IEEE Access*, vol. 9, pp. 34188–34205, 2021.
[41] V. K. Ramanna, J. Sheth, S. Liu, and B. Dezfouli, "Towards understanding and enhancing association and long sleep in low-power WiFi IoT systems," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 4, pp. 1833–1845, Dec. 2021.
[42] S. Kwon and H.-K. Choi, "Evolution of Wi-Fi protected access: Security challenges," *IEEE Consum. Electron. Mag.*, vol. 10, no. 1, pp. 74–81, Jan. 2021.
[43] S. Lindroos, A. Hakkala, and S. Virtanen, "The COVID-19 pandemic and remote working did not improve WLAN security," *Proc. Comput. Sci.*, vol. 201, pp. 158–165, Jan. 2022.
[44] D. De Almeida Braga, N. Kulatova, M. Sabt, P.-A. Fouque, and K. Bhargavan, "From dragondoom to dragonstar: Side-channel attacks and formally verified implementation of WPA3 dragonfly handshake," in *Proc. IEEE 8th Eur. Symp. Secur. Privacy (EuroS&P)*, Jul. 2023, PP. 707–723, doi: 10.1109/EuroSP57164.2023.00048.
[45] D. Cahyadi, I. F. Astuti, and N. Nazaruddin, "Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 N," *AIP Conf. Proc.*, vol. 2482, no. 1, 2023, Art. no. 030006.
[46] A. Raj and Dr. S. Sankaran, "Battery drain using WiFi beacons," in *Proc. 11th Int. Symp. Digit. Forensics Secur. (ISDFS)*, May 2023, pp. 1–6.
[47] H. Cao, L. Huang, S. Hu, S. Shi, and Y. Liu, "Owfuzz: Discovering Wi-Fi flaws in modern devices through over-the-air fuzzing," in *Proc. 16th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, May 2023, pp. 263–273.

ASMAA HALBOUNI (Graduate Student Member, IEEE) received the B.Eng. degree in telecommunication engineering from An-Najah National University, Palestine, and the M.Sc. degree in computer and information engineering from International Islamic University Malaysia, Malaysia. Currently, she is pursuing the Ph.D. degree in information technology with Multimedia University, Malaysia. Her research interests include intrusion detection, network security, and deep learning.

LEE-YENG ONG (Senior Member, IEEE) received the M.Eng.Sc. and Ph.D. degrees in computer vision from Multimedia University, Malaysia, in 2009 and 2020, respectively. She is currently a Senior Lecturer with the Faculty of Information Science and Technology, Multimedia University. Her research interests include image processing, data science, and big data analytics.

MENG-CHEW LEOW (Senior Member, IEEE) received the Doctor of Philosophy degree from Multimedia University. His research interests include game-based learning, specifically in role-playing game-based learning, system science, practical spirituality, and philosophy.