Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 9, No. 1, February 2021, pp.242-252

An analyzing process on wireless protection criteria focusing on (WPA) within computer network security

Mustafa Raheem Neamah[1], Hasanian Ali Thuwaib [2], Baraa I. Farhan[3]
[1,3] Wasit University, Iraq
[2] Department of Law, Kut University College, Iraq

ABSTRACT

Network security from a long ago approaches to cryptography and hash functions which are tremendous and due to the weakness of different vulnerabilities in the networks and obviously there is a significant need for analyzes. In this manuscript, the state-of-the-art wireless environment is focused solely on the sensor technology, in which security needs to be integrated with the Wireless Protected Access (WPA) standards. Wireless networking includes numerous points of view from wireless sensor systems, ad hoc mobile devices, Wi-Max and many more. The authentication and dynamic encryption is modified by system managers so that general communication can be anchored without any sniper effort in order to perform higher degrees of security and overall execution. The key exchange mechanism in wireless systems such as forward cases is accompanied by the sophisticated cryptography so as to anchor the whole computer state. The manuscript carries out a significant audit of test points of view using the methodologies used for the cryptography angle for protection and honesty in the wireless case, stressing Wi-Fi Secure Protected (WPA) needs.

Keywords: Cryptography, Encryption, Network Security, Wi-Fi Protected Access, WPA, Wireless Security

Corresponding Author:

Hasanian Ali Thuwaib
Department of Law, Kut University College, Iraq
E-mail: hasaneenali43@gmail.com

1. Introduction

Since its introduction in the year 1880, wireless networking has grown immensely in creativity in numerous fields. Photophones were covered by A. Graham Bell and C. S. S. Spoiler. It was used for the communication during the underlying period of the emergence of wireless development. Today, cellular innovation targets multiple frequencies in order to reach corporate, personal and security applications. The wireless communication depends for convincing and rooted knowledge transmitting on radio invention and associated community dimensions [1].

1.1. Security and dynamic encryption in wireless networks

The methods and procedures that are developed and carried out for anchored communication on the clear networks are referred to cryptography. The encryption methods to deal with general transmission are historically related. Using secure devices, such as encryption or message confirmation plans, you can change security objectives [2, 3].

The symmetrical key-based architecture has the integration of a common key in the channel so that the connection can be protected, but less integrity can be understood in the unique implementation scenarios. The symmetric key-based encryption approach is the most widely used and prominently used Data Encryption Standard (DES) [4, 5].

Transposition cipher-based authentication implementation is the encryption method, using transposition operations in the matrix format and generating permutations in the text to enforce the maximum degree of safety and integrity. Another technique replaces the units of the character letters with the other characters and thus improves the degree of protection and encryption by more encryption, but nowadays this is very popular and not suited to high security applications.

The stream cipher relies more on time-based character analytics and then on encryption. This method encodes the plaintext or byte with the combination of the encryption security keys in various time intervals.

In addition, the block cipher technique uses the algorithm of the deterministic system with symmetrical key integration and with the integration of block-based encryption rather than character-by-character authentication in the character stream [6].

The mathematical formulations and functions of this asymmetric key method are used to associate multiple keys. Furthermore, mathematical operations are performed with fluffy association. RSA based encryption is one of the most popular asymmetrical key encryption approaches.

Classical cryptography involves the manipulation of characters and numbers, the authentication approach, the total anonymity exchange cryptosystem. Contemporary cryptography, on the other hand, involves binary operations and bit wise manipulation, computer science and mathematical functions use and Hidden Key integration [7, 8].

Steganography, which is synonymous with protection and dignity in big situations, is another approach. The major distinctions between encryption and steganography are as follows.

1.2. Wireless access secured (WPA)

The three security and safety certification systems developed by the Wi-Fi Alliance for secure wireless computer networks include WiFi Protected Access (WPA), WI-Fi Protected Access II (WPA2) and Wi-Fi Protection Access 3 (WPA3). The Alliance described this as a solution to serious shortcomings found by Wired Equivalent Privacy (WEP) researchers in the previous system [1].

WPA was available in 2003, also known as IEEE 802.11i draught standard. The Wi-Fi Partnership planned to include the most safe and complex WPA2, which was usable in 2004 and is a generic shorthold for the complete IEEE 802.11i (or IEEE 802.11i-2004) standard, for the interim measure [9, 10].

The Wi-Fi Alliance announced in January 2018 that WPA3 would be launched with many changes in the security of WPA2. WiFi Safe Access or WPA was developed in 2003 to strengthen the functions of WEP. This preliminary upgrade is still fairly insecure, but can be configured quickly. For safer encryption than WEP, WPA uses the Time Key Integrity Protocol (TKIP) [11, 12, 13].

With the transition from the WiFi Partnership to a more modern protocol, they must retain some of the same WEP elements so that older devices stay compliant. Unfortunately, this ensures that the WPA modified version also has bugs like the WiFi Safe Configuration feature, which can be exploited reasonably easily. The Wi-Fi Alliance required WPA to replace WEP as an interim step before the full specification for IEEE 802.11i is available. Upgrades to the wireless network interface cards for WEP that started shipping in the year 1999 could introduce WPA. However, because the necessary improvements in the AP are more substantial than those required on network cards, it has not been possible to update the majority of APs in support of WPA prior to 2003 [14].

The IEEE 802.11i specification is introduced in the WPA protocol. In specific, the WPA was adopted under the Temporary Key Integrity Protocol (TKIP). A 64-bit or 128-bit encryption key has been used for WEP which must be entered manually and does not alter at the wireless access points and computers. TKIP uses a package key to create a 128-bit key dynamically for each packet, while preventing WEP-complicator attack types.[3] TKIP uses a package key [15].

WPA also provides a Message Consistency Audit to guarantee that an attacker cannot change or re-send data packets. This replaces the WEP regular Cyclic Redundancy Search (CRC). The key flaw of CRC was to ensure the data confidentiality of the packets it handled did not have enough security.[4] There were well-tried message authentication codes, but it took too many measurements to use on older network cards. In order to validate the integrity of packets, WPA uses a message integrity check algorithm called TKIP. TKIP is slightly faster than a CRC, but not as powerful as the WPA2 algorithm. Since then, researchers have found a WPA bug based on old vulnerabilities in WEP and shortcomings of Michael's hash function for message integrity to recover short packages for reinjection and spoofing [15].

1.3. WiFi protected access (WPA2)

WiFi Safe Access 2 was released one year later, in 2004. WPA2 is more stable and configurable than the previous alternatives. WPA2 is primarily different from using the Advanced Encryption Standard (AES) rather than TKIP. AES will protect high-secret government information and is also a strong choice to ensure safe keeping of a personal computer or WiFi business. WPA2's only significant weakness is the potential to target other computers linked to the network until someone has network access. This is a challenge if an organization is threatened internally by an unsatisfied employee who breaks into the other computers on the network of the company [16].

1.4. WPA3

The identification of vulnerabilities leads to refinement and progress. The Wi-Fi Alliance officially launched WPA3 certification in 2018. The alliance specifies that the latest iteration provides 'new features that simplify Wi-Fi encryption, make authentication more secure and provide more cryptographic force for highly sensitive data markets.' It should be noted that WPA3 is used; however, WPA3-certified devices are uncommon [17].

Table 1. Taxonomy of wireless standards and key points

Taxonomy	**Authentication**	**Encryption**	**Suitability for Corporate WAN**
WEP	None	WEP	Poor
WPA2 (PSK)	PSK	TKIP	Poor
WPA2	PSK	TKIP	Poor
WPA (Full)	802.1x	TKIP	Better
WPA2 (Full)	802.1x	AES-CCMP	Best

The previous versions, namely, WPA2 and WPA, are the most used security schemes used to secure wireless networks. In light of this information, we have contrasted WPA2 with WPA so that the readers can identify the necessary standard for their setup.

The Wi-Fi Alliance announced WPA3 as the successor of WPA2 in January 2018. Certifications for the new standard began June 2018 [13]. The latest version employs a 192-bit equivalent cryptographic security in the WPA3-based enterprise mode [14] (AES-256 in GCM mode with SHA-384 as HMAC). The use of CCMP-128 (AES-128 in CCM mode) is still the officially required basic encryption level required for the personal mode of the WPA3 scheme [18, 19].

The Pre-Shared Key system used with the previous scheme has been replaced by Simultaneous Authentication of Equals under the WPA3 standard. This new system is defined by IEEE 802.11-2016 and aims to provide a highly-secure initial exchange of keys corresponding to the personal mode [15][16] and forward secrecy [17]. Furthermore, the Wi-Fi Alliance states that WPA3 is designed to address the security weaknesses concerning passwords and streamline device setup where the display interface is absent [20][21].

The IEEE 802.11w amends the process of protecting management frames; the WPA3 scheme also enforces this amendment.

1.5. Hardware perspective

Backward compatibility with legacy wireless hardware produced before creating the WPA protocol was one key design consideration for WPA [19]. The objective is to augment the security level offered by the previously-used WEP encryption scheme. It should be noted that several legacy devices provide support for WPA after a firmware update; therefore, several legacy devices cannot support WPA [22].

Wi-Fi devices certified beginning 2006 provide support for both WPA2 and WPA security schemes. The latest version, WPA3, is mandated for devices beginning July 1, 2020 [10]. There is a chance that some older Wi-Fi cards may not support WPA3 [23, 24].

1.6. Security issues

1.6.1. Weak password

WPA and WPA2 schemes used with a weak-password based Pre-shared Key (PSK) may potentially be vulnerable to password cracking. The SSID name and length are employed to seed WPA passphrase hashes. Rainbow hashing tables are available for the top 1,000 SSIDs and numerous commonly-used passwords; consequently, cracking the WPA-PSK scheme is speeded up massively using lookup tables [29].

Wi-Fi connections rely on a four-way handshake authentication when connecting or reauthenticating. The Aircrack Suite provides support for mounting brute-force attacks for weak passwords that may be stolen during packet exchange.

Password cracking is based on offline analysis of passwords; the WPA3 scheme mitigates this vulnerability by ensuring that any guessed password must interact with the network hardware. Consequently, there is a practical limit on the number of guess attempts used during a brute-force attack [11]. Nevertheless, attackers have identified design flaws in the WPA3 scheme that allows brute-force attacks to be mounted (refer to Dragonblood attack) [25, 26].

1.6.2. Lack of forward secrecy

Forward security provision is not present for WPA2 and WPA, which means that once the pre-shared key is known, it is possible to decrypt all the encrypted packets using that key. It should be noted that attackers can decrypt the packets transmitted in the past that may have been collected. Public Wi-Fi networks secured using the WPA scheme are vulnerable because attackers can collect several users' packets and attack those who have connected using the same password. It implies that the WPA scheme protects a user from others who are not aware of the password. Considering these limitations, the use of Transport Layer Security (TLS) or other security schemes may protect sensitive data from attack and theft. WPA3 has addressed and eliminated this issue [26].

1.6.3. WPA packet spoofing and decryption

Frank Piessens and Mathy Vanhoef worked towards stronger attacks on WPA-TKIP compared to those by Martin Beck and Erik Tews. The experimenters demonstrated a way to inject a seemingly random packet count where the payload size does not exceed 112 bytes. This demonstration comprised the use of a port scanner that allows this attack to be mounted on any system implementing WPA-TKIP. Moreover, the experiments also indicated how to decrypt random packets forwarded to a client [27, 28, 29]. It was mentioned that it is feasible to manipulate TCP connections where attackers can potentially embed JavaScript that executes when a website is opened.

On the other hand, the attack method devised by Beck-Tews was able to decrypt relatively smaller packets that consisted primarily of known content such as ARP messages; moreover, this attack allowed the injection of three to seven packets having a maximum size of 28 bytes per packet. Furthermore, the Beck-Tews attack that Quality of Service (as specified by 802.11e) enabled; in contrast, the Vanhoef-Piessens attack had no such restriction. It should be noted that none of these two attacks can recover the session key shared between the access point and the client. The authors have indicated that smaller re-keying intervals may shut out some

attacks; however, since all attacks cannot be stopped, they strongly suggested that the switch from CCMP to TKIP be made rapidly [30].

Halvorsen and others demonstrated a modified form of the Beck-Tews attack. It is possible to inject three to seven 569-byte packets [38]; however, executing this attack is relatively lengthier since it takes about 18 minutes and 25 seconds. Vanhoef and Piessens conducted a study to demonstrate that WPA-encrypted broadcast packets can be subject to the original attack [39]. This extension is noteworthy because many networks use the WPA scheme to secure the broadcast packets compared to unicast packets. In contrast to the initial Beck-Tews and Vanhoef-Piessens attack forms, this new form of attack requires about seven minutes compared to the original attacks' fourteen minutes.

The weaknesses of the TKIP scheme are critical since the WPA-TKIP combination was understood to be very safe. Numerous wireless networking devices from several hardware providers still offer an option to use the WPA-TKIP scheme. A 2013 survey indicated that about 71% of the devices permit TKIP, while about 19% used TKIP exclusively [31].

1.6.4. WPS PIN recovery

Stefan Viehböck discovered and brought to light a severe form of a security flaw in December 2011, where the Wi-Fi Protected Setup (WPS) feature offered by wireless routers can be attacked regardless of the type of encryption. Newer hardware typically has the WPS feature enabled by default. Several consumer-grade Wi-Fi manufacturers have tried to mitigate the problem of weak passwords by suggesting the use of an alternative technique that generate and distribute high-strength wireless keys when a wireless adapter or device is connected to the network. Among the standard techniques is to press a button or to specify an 8-digit code [32].

Wi-Fi Protected Setup comprised an integration of these three methods as per the Wi-Fi Alliance's suggestion; nevertheless, the commonly-used PIN function led to another security vulnerability. A remote device can be used to recover the WPS pin of the network device, which can then be used to determine the WPA2/WPA password of the device in a matter of hours [40]; therefore, users are suggested to keep this feature turned off if their device supports it. Furthermore, the PIN is typically specified on a sticker affixed on the WPS-based routers; it is not possible to modify the PIN if it has been compromised [33].

WPA3 provides a different way for configuring devices that do not have adequate user interface provisions for system configuration. The new standard provides that nearby devices can provide the UI required to set the initial configuration, thereby reducing WPS dependency [11].

1.6.5. MS-CHAPv2 and lack of AAA server CN validation

Numerous vulnerabilities have been associated with MS-CHAPv2. Some are critical since malicious users can exploit those to reduce brute-force attack complexity, thereby making it possible to hack devices using modern hardware. In 2012, Moxie Marlinspike and Marsh Ray worked towards reducing the breaking complexity of MS-CHAPv2, which was reduced to the equivalent of breaking one DES key. Moxie commented that "Enterprises who are depending on the mutual authentication properties of MS-CHAPv2 for connection to their WPA2 Radius servers should immediately start migrating to something else" [34].

PEAP and TTLS are used for encrypting MSCHAPv2 under tunnelled EAP techniques. The MSCHAPv2 scheme is used frequently for misusing this vulnerability. It should be noted that the existing WPA2 implementations set up during the 2000s could be exploited and misconfigured. In its early versions, Android did not have any way through which users could adequately set up AAA server certificates. Hence, the initial weakness found corresponding to MSCHAPv2 was extended, considering the MiTM attacks [35]. The WPA3 scheme requires compliance in addition to what was provided with WPA2. The new scheme requires that AAA certificate validation conforms to specific processes using certified software [36].

1.6.6. Hole196

Hole196 is an exploit pertaining to the WPA2 scheme that misuses the shared Group Temporal Key (GTK); using this exploit, hackers can mount denial-of-service or man-in-the-middle attacks. Nevertheless, the assumption is that the hacker has prior authentication with the Access Point and already has the GTK [37].

1.6.7. Predictable Group Temporal Key (GTK)

In 2016, it was brought to light that the WPA2 and WPA schemes had a vulnerability specific to an expository random number generator (RNG). Experiments indicated that if the hardware vendors implemented the proposed RNG, an attacker could determine the group key (GTK) created randomly by the Access Point (AP). Furthermore, it was also demonstrated that anyone in possession of the GTK could use the exploit for traffic injection. Subsequently, the attacker may be able to access unicast data sent by the wireless network.

The demonstration comprised an attack on an Asus RT-AC51U router that employs out-of-tree drivers from MediaTek; these can create the GTK that can be determined in less than two minutes. Another demonstration comprised a VxWorks5-based key created by Broadcom access daemons. The keys were shown to be recoverable in less than four minutes. In this regard, specific Apple AirPort Extreme routers and the Linksys WRT54G were deemed vulnerable. The use of secure RNGs can allow vendors to protect against such exploits. In such a case, Hostapd working on Linux kernels cannot be attacked using this technique; hence, LEDE or OpenWrt-based routers are typically free from this vulnerability [38].

1.6.8. Assault of KRACK

It is assumed that KRACK attack affects all versions of both the WPA and the WPA2; however, the security ramifications differ between the implementations due to the understanding by the individual developers of a loosely described portion of the specification. Specifics on the KRACC (Key Reinstallation Attack) attack on WPA2 have been released in October 2017. The vulnerability can be fixed through software fixes, but not all systems have access to them [39]

1.6.9. Assault of Dragon blood

A number of significant WPA3 architecture failures were discovered in April 2019 which allow attackers to carry out downgrades and side channel attacks, which can force the passphrase to brute, and which also allow Wi-Fi stations to launch denial-of - service attacks.

2. Results and discussion

2.1. Key analytics patterns of WPA2 standard

WPA2 replaced the WPA, which was ratified in 2004. The compulsory elements of the IEEE 802.11i are introduced by WPA2, which needs Wi-Fi Partnership testing and acceptance. The CCMP, an AES-based encryption scheme, was mandatory to support it.[7][8] Certification started in September 2004. WPA2 registration was compulsory for all new Wi-Fi-marked products from 13 March 2006 to 30 June 2020 [40].

The WPA2 version is improved and uses AES encryption and long passwords to create a stable network. WPA2 has personal and corporate options which make it suitable for home and corporate users. However, it needs tremendous computing power, so it can be sluggish or unworked if you have an old computer.

Whichever choice is the better for you, your computer must be held secure by protecting your Wi-Fi link properly. If the most reliable encryption approach does not help your router, try using a VPN to encrypt your searches

WPA has a less stable encryption system and wants a shorter password, which makes it the most insecure alternative. WPA is not designed to be safe enough to support enterprise use so there is no organization solution. However, WPA can be used with a minimum processor strength if you have an older programme, which may be a safer choice than WEP.

In comparison, the difficulty of the WPA2-Personal passphrase in the network was associated with the complexity of authentication cracks. So it was easier to breach encryption if the network used a basic password (as the majority assumed).

Another big weakness of WPA2 workers is that a passphrase user is able to snoop on the network traffic of another user and make attacks, particularly for business networks. Although WPA / WPA2 enterprise is secure from snooping, it involves the implementation of enterprise mode through a RADIUS server and cloud service.

Wi-Fi 's biggest shortcoming since it was developed was perhaps the lack of any integrated protection, encryption, or privacy on open public networks. Anyone with the right software will snub consumers in cafes, hotels and other public areas linked to Wi-Fi hotspots. This snooping may be passive, such as merely tracking visited websites or documenting unprotected email login credentials or aggressive attacks, such as hijacking for access to a user login page.

Centered on the wireless protection protocol 802.11i, terminated in 2004, WPA2 is enhanced by using the Advanced Encryption Standard (AES) to encrypt the most critical feature. AES provides enough (and has been) protections for the US Government to use to encrypt information known as high secret.

Table 2. Key demarcation WPA, WEP and WPA2

Protocol	**Authentication**	**Encryption**
WPA	PSK 128 & 256 bit	RC4 and TKIP
WEP	PSK 64-bit	RC4
WPA2	AES-PSK 256 bit	AES-CCMP

Table 3. Security based enable status in SIM, HSM and smartcard

Implementation	**CCID**	**PKCS #11**	**PC/SC**
libsodium	0	0	0
Bouncy Castle	0	1	0
cryptlib	0	1	0
wolfCrypt	0	1	0
Crypto++	0	0	0
Botan	0	1	0
Libgcrypt	1	1	1
OpenSSL	0	1	0

Table 4. Evaluation of cryptography hash approaches in network environment

Algorithm	**Word size**	**Rounds**	**Internal state size**	**Output size (bits)**	**Block size**
GOST	32	32	256	256	256
HAVAL	32	5	256	128	1024
MD2	32	18	384	128	128
MD4	32	3	128	128	512
MD5	32	64	128	128	512
PANAMA	32	32	8736	256	256
RIPEMD	32	48	128	128	512
RIPEMD-128/256	32	64	128/256	128/256	512
RIPEMD-160	32	80	160	160	512
RIPEMD-320	32	80	320	320	512
SHA-0	32	80	160	160	512
SHA-1	40	80	160	160	512
SHA-256	56	64	256	256	512
SHA-3	64	24	1600	512	3200
SHA3-224	64	24	1600	224	1152
SHA3-256	64	24	1600	256	1088
SHA3-384	64	24	1600	384	832
SHA3-512	64	24	1600	512	576
Tiger2	64	24	192	128	512
WHIRLPOOL	8	10	512	512	512
BLAKE2b	64	12	1024	512	512
BLAKE2s	32	10	512	256	256

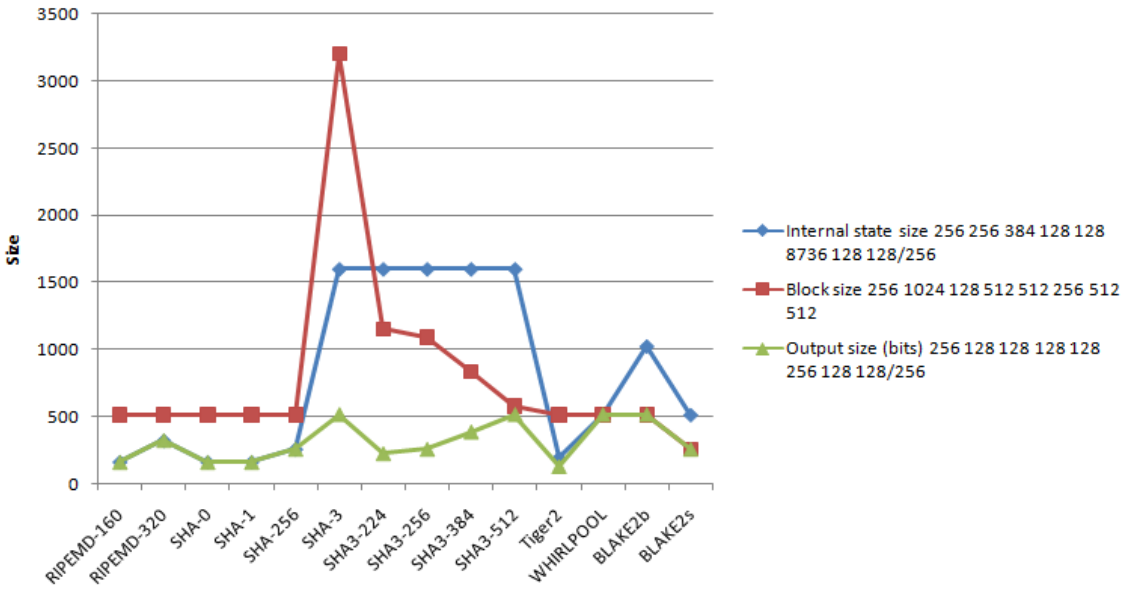

Figure 1. Evaluation of traditional cryptography hash approaches

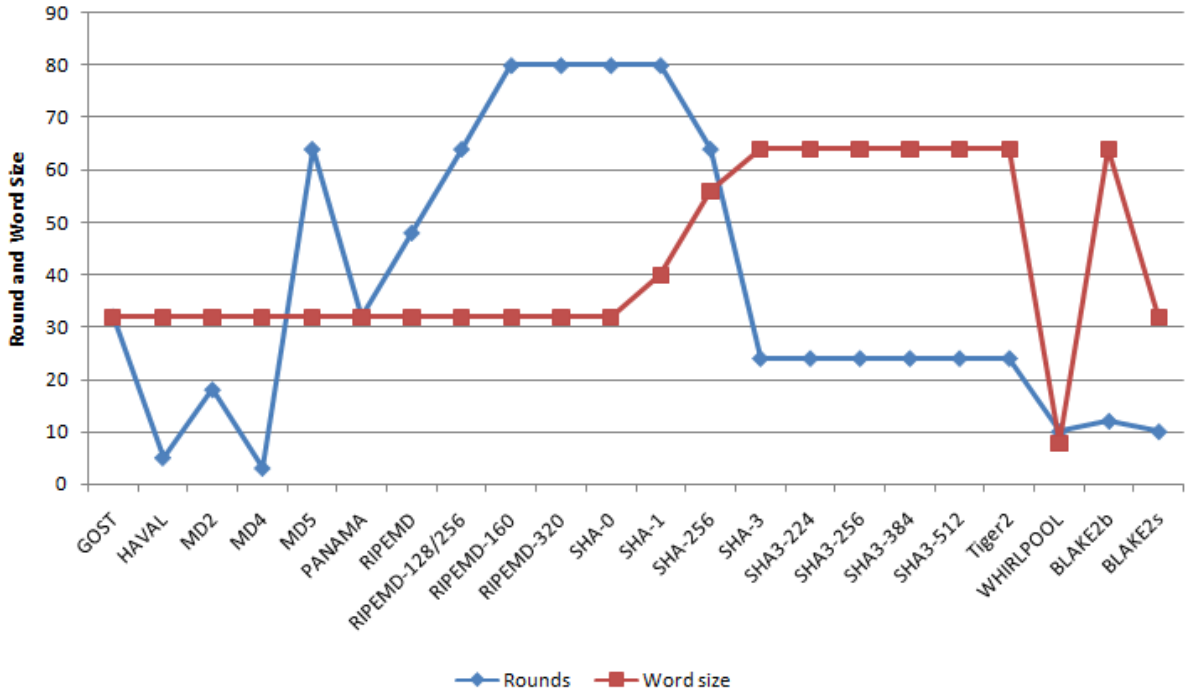

Figure 2. Evaluation on Approaches for Security

2.2. Assessment of core security cryptographic methods

The RSA, AES and MD5 equations based on XOR are performed in an immense review of the various key cryptography approaches. These variations are implemented because these techniques are commonly used in various phases, including Cloud, IoT, Fog, Mud, Edge and numerous others, for a higher degree of protection.

However, the others may be taken, which have a more extraordinary degree of empirical roles and meanings that boost overall protection. This are covered by measurements. This strategy results in better efficiency and accuracy in the overall rise. The emphasis points to the evaluations' scoring aspect. It is analyzed during the review of measurements in Big-O notation.

The analytical findings derived from the assessment results and the overall review of the implementation results follow, in order to measure the combined success of the approaches

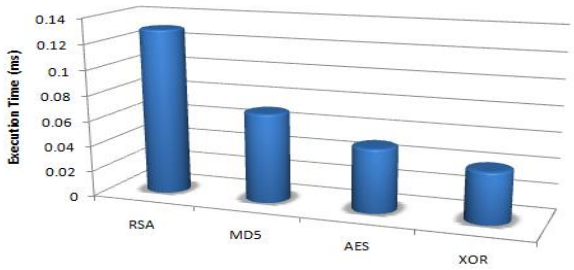

Figure 3. Comparative evaluation of the approaches (Evaluation time in ms)

Table 5. Analytics of algorithms

	XOR	**MD5**	**RSA**	**AES**
Execution Time (ms)	0.04	0.07	0.13	0.05
Complexity (Points)	27.74	40.17	71.16	32.19
Cost Factor (Points)	31	69	87	49
Performance (Points)	93	71	65	83

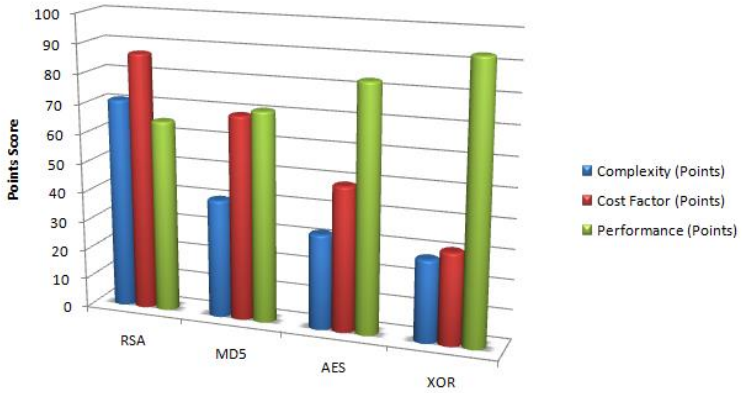

Figure 4. Comparative evaluation of the approaches

It is apparent from the findings and graphic view that the XOR-based cryptography method still operates on many parameters. The highly effective protection strategy, like quantum encryption, must be carried out so that the network environment can be safeguarded with greater network security and privacy.

3. Conclusion

It reflects on the analytical assessment of cryptography methods in the pre-accessible wireless scenarios like WPA standards by using the different approaches and analyzing the variety of research manuscripts in order to present the comprehensive benchmarking of work carried out. The Advanced Encryption Standard (AES) WPA2 protocol definitely fixed a few security bugs from the original WPA using the Temporal Key Integrity Protocol (TKIP) encoding protocol. WPA2 was much better than the WEP defense which was defeated for a long time. However, in the last decade, WPA2 also had big bugs. A crucial weakness of W PA2 is the potential to smash the WPA2 passphrase by brute-force attacks – effectively analyzing the password before a match is found. Worse still, after hackers have gathered the correct information on the airwaves, these password-assessing efforts may be carried out off-site, making it simpler for them. When broken, all data they have obtained before or after cracking will then be decrypted.

References

[1] D. Schepers, A. Ranganathan, & M. Vanhoef, “Practical Side-Channel Attacks against WPA-TKIP", In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (pp. 415-426), 2019.

[2] T. M. Alghamdi, Throughput analysis of IEEE WLAN ‘802.11 ac’Under WEP WPA and WPA2 security protocols. Int. J. Comput. Netw., vol.9, no.1, pp.1-13, 2019.

[3] M. E. Rana, M. Abdulla, and K. C. Arun, "Common Security Protocols for Wireless Networks: A Comparative Analysis", International Journal of Psychosocial Rehabilitation, vol.24, no.05, 2020.
[4] J. A. P. de Carvalho, C. F. R. Pacheco, H. Veiga, and, A. D. Reis, "Comparative Performance Studies of Laboratory WPA IEEE 802.11 b, g Point-to-Multipoint Links, In *2012 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, pp. 1-4. IEEE, 2012.
[5] F. Fikriyadi, R. Ritzkal, and B. A. Prakosa, "Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method", Jurnal Mantik, vol.4, no.3, pp.1658-1662, 2020.
[6] Y. Li, W. Guo, X. Meng, and W. Xia, "Charging wireless sensor network security technology based on encryption algorithms and dynamic model", International Journal of Distributed Sensor Networks, vol.16, no.3, 2020.
[7] E. Wahyudi, E. T. Luthfi, M. M. Efendi, and S. T. M. I. K. Mataram, "Wireless Penetration Testing Method to Analyze WPA2-PSK System Security and Captive Portal", Jurnal Explore STMIK Mataram, vol.9, no.1, 2019.
[8] U. Banerjee, C. Juvekar, A. Wright, A.P. Chandrakasan, "An energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in iot applications", In Solid-State Circuits Conference-(ISSCC), pp. 42-44, 2018.
[9] C. Thirumalai, H. Kar, Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive data over Cloud and IoT devices, In Power and Advanced Computing Technologies (i-PACT), 2017.
[10] Q. Huang, Y. Yang, L. Wang, "Secure data access control with Cipher-Text update and computation outsourcing in fog computing for Internet of Things", IEEE Access, pp.12941-12950, 2017.
[11] S. Challa, M. Wazid, A.K. Das, N. Kumar,,A.G. Reddy, E.J. Yoon, K.Y. Yoo, Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access, vol.5, pp3028-30243, 2017.
[12] Z. Liu, J. Großschädl, Z. Hu, K. Järvinen, H. Wang, I. Verbauwhede, "Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things", IEEE Transactions on Computers, vol.66, no.5, pp.773-785, 2017.
[13] M. Usman, I. Ahmed, M.I. Aslam, S. Khan, U.A. Shah, SIT: A lightweight encryption algorithm for secure internet of things. arXiv preprint arXiv:1704.08688, 2017 Apr 27.
[14] Q. Jiang, S. Zeadally, J. Ma, D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks", IEEE Access, vol.5, pp.3376-3392, 2017.
[15] A.A. Diro, N. Chilamkurti, N. Kumar, "Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing", Mobile Networks and Applications, vol.22, no.5, pp.848-858, 2017.
[16] D. Puthal, S. Nepal, R. Ranjan, J. Chen, A synchronized shared key generation method for maintaining end-to-end security of big data streams, In *Proceedings of the 50th Hawaii International Conference on System Sciences*. 2017.
[17] M.S. Farash, M. Turkanović, S. Kumari, M. Hölbl, an efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks, vol.36, pp.152-176, 2016.
[18] Raza S, Seitz L, Sitenkov D, Selander G. S3K: scalable security with symmetric keys—DTLS key establishment for the Internet of things. IEEE Transactions on Automation Science and Engineering. 2016 Jul;13(3):1270-80.
[19] X. Huang, P. Craig, H. Lin, Z. Yan, SecIoT: a security framework for the Internet of Things. Security and communication networks, vol.9, no.16, pp.3083-3094, 2016.
[20] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, Fair Access: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks, vol.18, pp.5943-5964, 2016.
[21] H. Kim, A. Wasicek, B. Mehne, E.A. Lee, A secure network architecture for the internet of Things based on local authorization entities. In Future Internet of Things and Cloud (FiCloud), pp. 114-122, 2016.
[22] J.L. Hernández-Ramos, A.J. Jara, L. Marín, A.F. Skarmeta Gómez, DCapBAC: embedding authorization logic into smart things through ECC optimizations, International Journal of Computer Mathematics, vol.93, no.2, pp.345-66, 2016.

[23] G.C. Bae, K.W. Shin, "An efficient hardware implementation of lightweight block cipher algorithm CLEFIA for IoT security applications", Journal of the Korea Institute of Information and Communication Engineering. 2016;20(2):351-8.
[24] K. Mahmood, S.A. Chaudhry, H. Naqvi, T. Shon, H.F. Ahmad, " A lightweight message authentication scheme for Smart Grid communications in power sector", *IEEE Transactions on Smart grid*, *vol.* 2, no. 4, pp.675-685, 2011.
[25] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti, OSCAR: Object security architecture for the Internet of Things. Ad Hoc Networks, vol.32, pp.3-16, 2015.
[26] V.L. Shivraj, M.A. Rajan, M. Singh, P. Balamuralidhar, One time password authentication scheme based on elliptic curves for Internet of Things (IoT). InInformation Technology: Towards New Smart World (NSITNSW), pp. 1-6, 2015.
[27] L. Marin, M.P. Pawlowski, A. Jara, Optimized ECC implementation for secure communication between heterogeneous IoT devices. Sensors. Vol.15, no.9, pp.21478-21499, 2015.
[28] D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, A. Biryukov, Triathlon of lightweight block ciphers for the internet of things. Journal of Cryptographic Engineering, pp.1-20, 2015.
[29] S.R. Moosavi, T.N. Gia, A.M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, vol.52, pp.452-459, 2015.
[30] S. Sciancalepore, Capossele A, Piro G, Boggia G, Bianchi G. Key management protocol with implicit certificates for IoT systems. InProceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems 2015 May 18 (pp. 37-42). ACM.
[31] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, W. Hu, Talos: Encrypted query processing for the internet of things. In Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, pp. 197-210, 2015.
[32] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, G. Ferrari, Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios, IEEE sensors journal. 2015 Feb;15(2):1224-34.
[33] H. Shafagh, A. Hithnawi, Security comes first, a public-key cryptography framework for the internet of things. InDistributed Computing in Sensor Systems (DCOSS), pp. 135-136, 2014.
[34] R. Hummen, H. Shafagh, S. Raza, T. Voig, K. Wehrle, Delegation-based Authentication and Authorization for the IP-based Internet of Things. In Sensing, Communication, and Networking (SECON), pp. 284-292, 2014.
[35] Y.B. Saied, A. Olivereau, D. Zeghlache, M. Laurent, Lightweight collaborative key establishment scheme for the Internet of Things. Computer Networks. Vol. 8, no. 64, pp. 273-95, 2014.
[36] P.N. Mahalle, N.R. Prasad, R. Prasad, Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT), In *proceedings of 7th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2013), Chennai–India*. 2013.
[37] L. Touati, Y. Challal, A. Bouabdallah, C-cp-abe: Cooperative Cipher-Text policy attribute-based encryption for the internet of things. In Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on 2014 Jun 17 (pp. 64-69). IEEE.
[38] K.N. Prasetyo, Y. Purwanto, D. Darlis, an implementation of data encryption for Internet of Things using blowfish algorithm on FPGA. InInformation and Communication Technology (ICoICT), 2014 2nd International Conference on 2014 May 28 (pp. 75-79). IEEE.
[39] M.A. Jan, P. Nanda, X. He, Z. Tan, R.P. Liu, A robust authentication scheme for observing resources in the internet of things environment. InTrust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on 2014 Sep 24 (pp. 205-211). IEEE.
[40] Lakkundi V, Singh K. Lightweight DTLS implementation in CoAP-based Internet of Things. InAdvanced Computing and Communications (ADCOM), 2014 20th Annual International Conference on 2014 Sep 19 (pp. 7-11). IEEE.