Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 7, S. 75-80, 9, 2023

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 7, pp. 75-80, 9, 2023

Research Article

New Cybersecurity Scheme for Electrical Substation using Wifi Protected Access 3 and Local Authenticator

Firas S. Alsharbaty*, Qutaiba I. Ali[2]

[1]*Electrical Department/Engineering College, Mosul University, Iraq*
[2] *Computer Department/Engineering College, Mosul University, Iraq*

(alsharbaty@uomosul.edu.iq) Email of the corresponding author

(Received: 25 September 2023, Accepted: 05 October 2023)

(3rd International Conference on Innovative Academic Studies ICIAS 2023, September 26-28, 2023)

ATIF/REFERENCE: Alsharbaty, F. S. & Ali Q. I. (2023). New Cybersecurity Scheme for Electrical Substation using Wifi Protected Access 3 and Local Authenticator. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(9), 75-80.

Abstract **–** The wireless local area network technologies are attractive solutions to upgrade the communication network of the traditional electrical substation toward smart electrical substation. Unfortunately, the wireless communication network suffers from additional drawbacks compared to wired technologies such as cyber threats in particular the common wireless channel. The current work suggests a cybersecurity model for the wireless communication network (WCN) that serves the substation automation system (SAS) of electrical substations. The adopted model protects the wireless communication between the high-voltage devices and the switched access point (S-AP) in the electrical substation using wifi protected access 3 (WPA3) security scheme. This work proposes a new architecture scheme to provide a secure and reliable key management module based on WPA3. Hence, a local authenticator is responsible for distributing the keys safely rather than the remote authentication dial-in user service (RADIUS) server. In addition, a lightweight security scheme as possible is handled to overcome the challenges of SAS system performance requirements. The results indicated that the adopted ciphering algorithms do not break the latency requirements of real-time protection of SAS (less than 4 msec).

Keywords – Advanced Encryption Standard (AES); Cybersecurity; Local Authentication Server; Real Time Performance; Wireless Network; Wifi Protected Access3

I. INTRODUCTION

In the electrical substation, there are many types of intelligent electronic devices (IEDs) such as merging unit (MU), actuators (AC), local controller (LC), and global controller (GC). On the other side, the dominate standard of communication in the substations is IEC 61850 which defines specific types of messages: generic object-oriented substation event (GOOSE), sampled measured values (SMV), and manufacturing message specification (MMS). Hence, easier communication with intelligent electronic devices (IEDs) could be achieved with the IEC–61850 to manipulate the equipment of the field devices [1]. This mechanism may be exploited by attackers and it makes the substations more vulnerable to cyber threats. As a result, confidentiality, availability, and data integrity of the substation data may be broken by many potential cyber vulnerabilities in terms of the devices and the networks of the substation. Further, when the attackers could gain access to the network of the substation, they could harm the operational processes of the substation and they can cause catastrophic damage. In general, the attacks may be implemented from either within the substation or

outside the substation. To implement any attack within the substation, the attackers need to gain access to the intranet of the substation network. In such cases, attackers may take advantage of physical access to IEDs or insert malware in any device such as update patches. At this level, the attackers could spoof, inject, analyze, and transmit malicious packets [2].

However, in the suggested network of the electrical substation in the previous work [3], the cyber data of the power system is classified into many types as shown in Fig1.

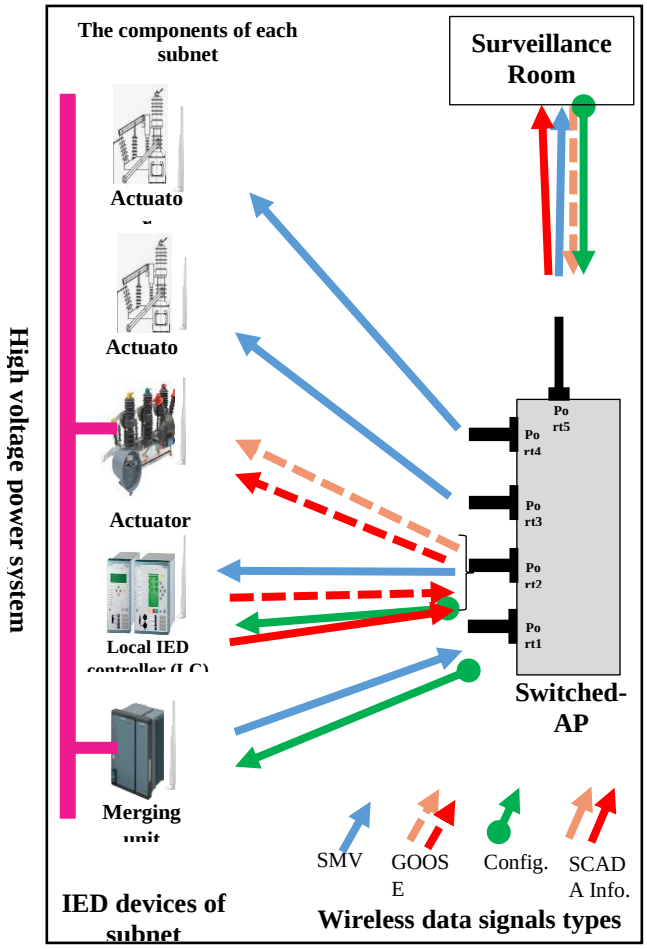

Fig. 1 The message flow of the wireless architecture design in the electrical substation

To build a robust security model for the suggested network, it is essential to discuss the essence of substation data traffic. In this context, sampled measured values are periodic successive messages that are sent from MU to four destinations (LC, Actuator1, Actuator2, and GC). SMV messages represent sampled values for the current or voltage that reflects the status of the power line. Based on the concluded information from SMV messages, LC and GC send periodic GOOSE messages to protect the power line. If SMV messages carry bad information about the power line (fault occurring), LC sends a trip GOOSE message to the circuit breaker (CB) to isolate the corresponding feeder bay. Therefore, a trip GOOSE message that is sent from LC or GC to CB leads to an outage of the electricity on a feeder bay directly. In contrast, a trip GOOSE message from LC or GC to CB can reload the electricity on the isolated feeder. The decision of LC or GC to send the trip GOOSE message depends on the information of SMV that reached LC or GC.

Furthermore, LC and GC send periodic information messages to the SCADA system at the Human Machine Interface (HMI). Whereas, HMI (SCADA system) could send configuration messages to LC, GC, and/or MU. All cyber data of the substation wireless network passes via the access point of the bay level (Switched-AP) and the access point of the station level (MWD-AP). Table 1 summarizes the expected attacks and threats inside the electrical substation [1] [4] [5].

Table 1. Possible threats to the electrical substation.

Attack	Description
Replay attack	Resending a previously sent message without modifying its content
Message injection	Build modify, and transmit false and malicious messages into the network
Masquerade attack	Old messages are captured, they are adulterated to mimic a legitimate behavior (get fresh and valid values for SqNum and StNum)
Poisoning attack	Harming the communication between publisher and subscriber devices by preventing the subscriber from processing subsequent legitimate GOOSE messages or forcing subscribers to process fabricated GOOSE messages
Jamming attacks	Filling wireless communication channels with noise
Wireless eavesdropping attack	Intercept unsecured network communication
Denial of service (DoS) attacks	Overloading networks by using various techniques where the attacker sends large volumes of traffic to flood the network

Concerning the literature, Y. Xiao et al. in [6] discussed and investigated the countermeasures against cyber-attacks in the electrical substation based on a fuzzy analytical hierarchy process. N. Moreira et al. in [7] explored current security methods and they studied their applicability to the environment of substation automation systems. In the same context of substation automation, the researchers in [8] and [9] proposed anomaly detection methods for the IEC 61850 communication standard in the electrical substation. On the other hand, the issue of key management for cryptographic algorithms in electrical substations is addressed by the work in [10]. The delay attacks on precision time protocol in power substations are considered in the work [11], where the researchers submitted a new method for detecting delay attacks.

This work adopts the WPA3 security method for the WLAN technologies in industrial applications to protect the smart electrical substation from cyber threats, it deals with layer 2 security level and provides a robust security level in terms of encryption, authentication, and integrity. Moreover, this work designs a novel architecture model for a secure and reliable key distribution from a local authentication server (authenticator) in the wireless network of an electrical substation rather than a RADIUS server via the WAN network.

II. Materials and Method

As explained in the previous work [3], the suggested network of substations consists of multiple subnets. Each subnet depends on switched AP based on WLAN standards to offer the wireless coverage area. Moreover, one of the privileges of the suggested substation network is built according to the five layers TCP/IP stack model (physical, data link, network, transport, and application layers). Therefore, it can employ the available and advanced security techniques to protect the transferred data. In addition, the architecture of Switched-AP includes many sub-access points, some of these access points may stay spare for cases of damage to any sub-access point for any reason to handle the availability and reliability.

In the sense of cybersecurity, the mentioned expected attacks target confidentiality, authentication, and integrity. The suggested design of the cybersecurity system aims to protect the wireless intranet of electrical substations and it takes into account the specificity of this system. Therefore, the current work proposes a WLAN layer 2 security scheme in terms of confidentiality, authentication, and integrity. WiFi Protected Access 3 is the most sophisticated and protected scheme in terms of WLAN technologies.

A. The proposed model of WPA3

WPA3 is a subset and the latest improvement of the 802.11i security standard of WLAN technology for personal and enterprise networks. WPA3 enhances the encryption of wireless networks using a new encryption protocol called Galois Counter Mode Protocol (GCMP) with Advanced Encryption Standard (AES) [12]. In addition, WPA3 improves the authentication of wireless networks by dealing with Simultaneous Authentication of Equal (SAE is defined as a secure key establishment protocol) with a length key equal to 128 or 192 bits to submit stronger defenses against password guessing where WPA2 was dealt with pre-shared key (PSK). Further, WPA3 deals with GCMP and the secure hash algorithm (HMAC-SHA 384) [13]. Therefore, WPA3 offers encryption (Elliptical Curve Cryptography with 192-bit security suite), authentication (SAE), and data integrity (SHA-1 or SHA-2),

WPA3 supports multi-operation modes and the best mode that addresses the design of substation networks is WPA3 enterprise mode because this mode is specialized to the industry environment and enforces robust secret security standards compared to other secret security standards [14].

In the enterprise mode, according to Opportunistic Wireless Encryption (OWE), the conversations between the APs and the wireless clients in open networks are encrypted with different keys for different connections. The encryption on each wireless connection is different. It employs a Protected Management Frame (PMF) mandatory to support the protection of management frames between APs and wireless clients.

In terms of encryption, Advanced Encryption Standard (AES) represents a strong secret key (symmetric key) based on block ciphering, it could protect and secure the data between wireless IED devices and AP against unauthorized access. The AES uses cryptographic keys of 128 and 192 bits to encrypt and decrypt data in blocks of 128 bits. WPA3 supports advanced AES that could employ 384 or 512 bits to encrypt and decrypt data [15]. The combination of AES-GCM is a block cipher

operation mode that provides high speed of authenticated encryption and data integrity. It has two main functions block cipher encryption and multiplication over the Galios field. Initialization Vector (IV), additional authenticated data, secret key, and plaintext are used as input in 128-bit and give a 128-bit ciphertext and authentication tag. AES-GCM algorithm can encrypt or decrypt with a 128-bit or 192-bit of cipher key [12]. Fig 2 shows the ciphering algorithms of WPA3.

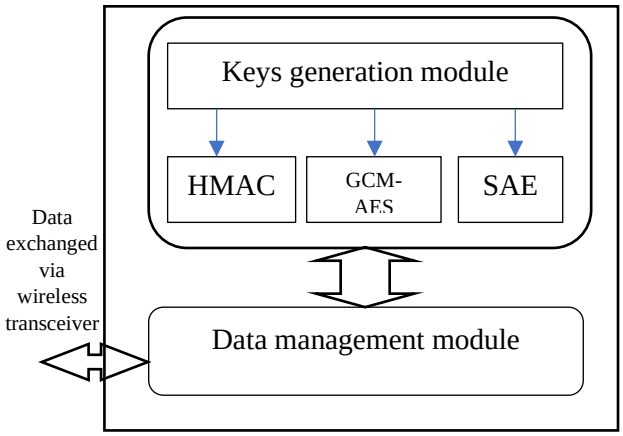

Fig. 2 The general module of WAP3 ciphering.

The algorithm that is adopted to provide the authentication and integrity in WPA3 is the hash message authentication code (HMAC). HMAC depends on cryptographic hash functions. The famous version of a hash function is secure hash function-1 (SHA1) that designed by NIST. SHA-1 creates a digest of length N from a multiple- 512 block message. Hence, the hash function guarantees the integrity of the data message.

In the case of WPA3, it is likely difficult for an adversary to steal the wireless traffic of the clients who are protected by WPA3. Even if an attacker has successfully guessed a client's password, he cannot get the session keys used for encryption and decryption.

B. The suggested model of authentication and key distribution

In the traditional method of keys generation and distribution of enterprise mode, Switched-AP includes multi sub-access points, and each sub-access point covers one or two IEDs as shown in Fig. 1. For instance, it is assumed that wireless IED device represents MU, LC, AC, or GC.

Any sub-access point of Switched-AP connects to one or two IEDs, hence the basic service set of such a network is protected by WPA3 by devoting a unique key (192 bits) based on enterprise mode to provide a robust authentication. The authentication messages are exchanged among sub-access points of Switched-AP, IED, and the server of RADIUS (Remote Authentication Dial-In User Service) [16, p. 3]. Firstly, the access point broadcasts a beacon message, and then, the wireless IED negotiates the access point to receive the keys of authentication and encryption based on ECDH (Elliptic curve Diffie-Hellman) rather than 4-way handshaking to secure the transferred data after addressing the phases of establishments, authentication, and association.

Unfortunately, the exchanged information between the RADIUS server and the access point may be compromised by an intruder because the path of data passes WAN. However, an intruder likely claims the position of the authentication server. Consequently, the security procedures will be for nothing.

To compensate for the issue of receiving the security parameters from the RADIUS server via WAN to receive the ciphering keys of the WPA3 security scheme, this work suggests an authentication server scheme by employing a local server of authentication be placed in the electrical substation rather than RADIUS server via WAN. In this context, the design and procedures of the novel scheme of local authentication server are explained as follows:

Firstly, it is installed and written the software of the authentication server based on the MAC addresses of wireless IED clients to serve the authentication establishment according to WPA3. The appropriate platform that is exploited to serve as a local authentication server is the Raspberry Pi Compute Module for industrial applications. For more details, KUNBUS RevPi based on Raspberry Pi is an open, modular, and inexpensive industrial-embedded PC. It is composed of open hardware and software, capabilities according to EN61131-2 standard as well as supplemented by digital or analog I/O modules and processing frequency up to 1.2 GHz quad-core.

One local authentication server is embedded in each MWD-AP and Switched-AP to handle the requests of authentication and deliver the ciphering keys for the wireless communication network of the electrical. The authenticator server enables the electrical substation to maintain IED profiles in a

local database without sharing them with outside servers. Having a local database provides better security and enables the substation to set up a policy in a self-manner.

Henceforth, one embedded KUNBUS module is connected to each Switched-AP and MWD-AP in the suggested network. Fig. 3 shows the negotiations between any IED devices and the embedded authentication server.

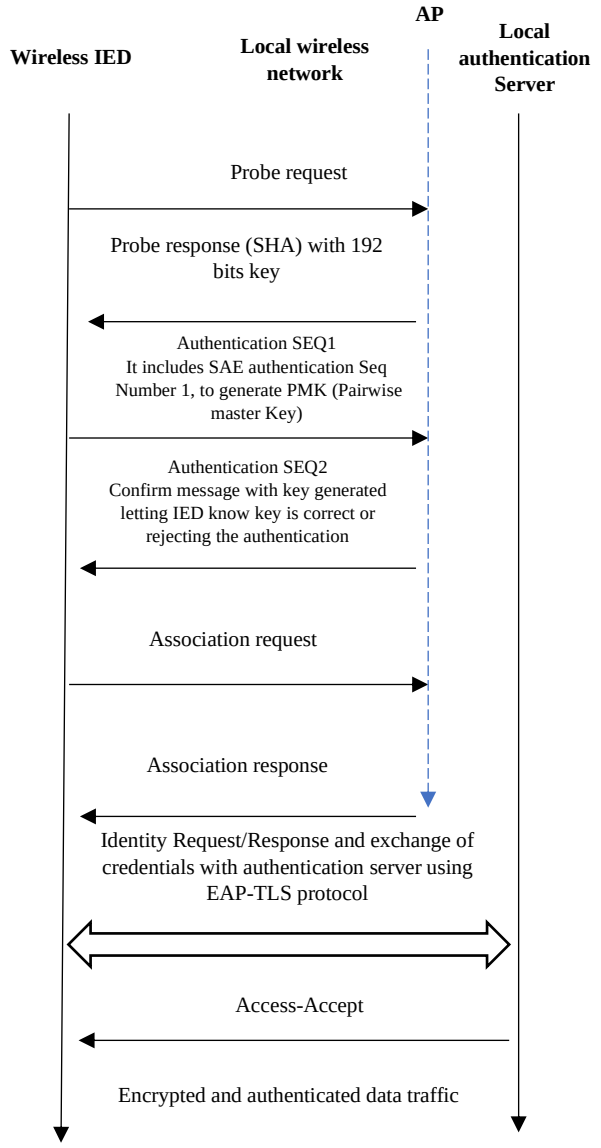

Fig. 3 New authentication structure based on local authentication server.

C. *The effect of WPA3 on the System Performance*

It is essential to discuss the performance of the suggested system in terms of latency which represents a vital factor in the industrial environment of the substation automation applications.

The complete model assumptions of the electrical substation communication network are shown in [3], while the effect of the AES-128 algorithm on the processing rate of IED is illustrated in [17]. This work adopts the AES 128 algorithm for encryption and decryption and hash message authentication code (HMAC) based SHA1 for data integrity. The reason behind these assumptions (lightweight ciphering algorithms as possible) is to mitigate the effect of the processing delay of IEDs on the overall latency of system performance.

To explain the effect of WPA3 cryptography, Fig. 4 explains the effect of the WPA3 cryptographic on the real-time protection of substation automation in the case of MU = 1600 sample/sec.

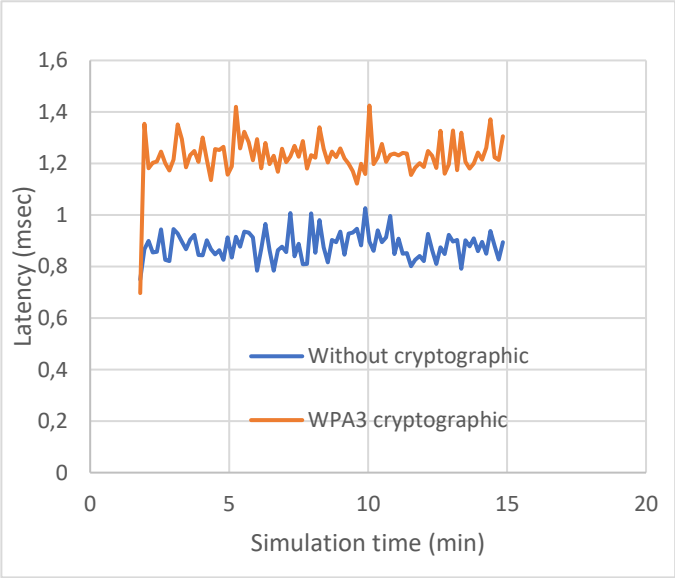

Fig. 4 The effect of WPA3 ciphering algorithms on the real-time performance of electrical substation in the case of MU=1600 sample/sec.

The results indicate that the maximum latency in the case of using WAP3 does not exceed 1.425 msec.

III. CONCLUSION

As mentioned before, this work designed a cybersecurity model to secure the electrical substation wireless network using WPA3 and a local authenticator. In the industrial environment of an electrical substation, the real-time protection of SAS is a time-sensitive application that requires as lightweight traffic as possible to never smash the requirement of the real-time protection application in terms of latency. The privilege points of adopting the WPA3 security scheme (layer 2 security

scheme) with a local authenticator relate to causing less delay compared to layer 3 and layer 4 security schemes as well as offering robust authentication behavior. Hence, WPA3 mitigates the consumed processing of cryptographic algorithms on the central processing unit that affects the system performance. Because WPA3 cryptography is implemented in network interface cards. The results indicate that adopting WPA3 with lightweight cryptographic schemes such as AES-128 bits and HMAC-SHA1 does not exceed the threshold of real-time protection of the operational technologies and provides robust protection.

ACKNOWLEDGMENT

The authors are very grateful to the University of Mosul / College of Engineering for their provided facilities, which helped to improve the quality of this work.

REFERENCES

[1] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," *Computer Networks*, vol. 184, p. 107679, Jan. 2021, doi: 10.1016/j.comnet.2020.107679.

[2] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *ISGT 2014*, Feb. 2014, pp. 1–5. doi: 10.1109/ISGT.2014.6816375.

[3] F. S. Alsharbaty and Q. I. Ali, "An Enhanced Industrial Wireless Communication Network for Hard Real Time Performance Substation Automation Purposes," *Al-Rafidain Engineering Journal (AREJ)*, vol. 27, no. 2, pp. 216–226, Sep. 2022, doi: 10.33899/rengj.2022.133860.1173.

[4] S. Hussain, J. Hernandez Fernandez, A. K. Al-Ali, and A. Shikfa, "Vulnerabilities and countermeasures in electrical substations," *International Journal of Critical Infrastructure Protection*, vol. 33, p. 100406, Jun. 2021, doi: 10.1016/j.ijcip.2020.100406.

[5] F. Holik, L. H. Flå, M. G. Jaatun, S. Y. Yayilgan, and J. Foros, "Threat Modeling of a Smart Grid Secondary Substation," *Electronics*, vol. 11, no. 6, Art. no. 6, Jan. 2022, doi: 10.3390/electronics11060850.

[6] Y. Xiao, L. Yang, J. Li, J. Xu, and K. Liu, "Valuing the cyber-attacks budget in high voltage power substations to increase cyber-security; providing a method based on Fuzzy Analytical Hierarchy Process," *Energy Reports*, vol. 7, pp. 8322–8331, Nov. 2021, doi: 10.1016/j.egyr.2021.08.002.

[7] N. Moreira, E. Molina, J. Lázaro, E. Jacob, and A. Astarloa, "Cyber-security in substation automation systems," *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 1552–1562, Feb. 2016, doi: 10.1016/j.rser.2015.10.124.

[8] L. Yang, Y. Zhai, Y. Zhang, Y. Zhao, Z. Li, and T. Xu, "A new methodology for anomaly detection of attacks in IEC 61850-based substation system," *Journal of Information Security and Applications*, vol. 68, p. 103262, Aug. 2022, doi: 10.1016/j.jisa.2022.103262.

[9] P. Kreimel, O. Eigner, F. Mercaldo, A. Santone, and P. Tavolato, "Anomaly detection in substation networks," *Journal of Information Security and Applications*, vol. 54, p. 102527, Oct. 2020, doi: 10.1016/j.jisa.2020.102527.

[10] N. Wang, R. Yao, Y. Liu, Y. Wu, and D. Mou, "A Key Management Method For Smart Substation," *Energy Procedia*, vol. 156, pp. 337–342, Jan. 2019, doi: 10.1016/j.egypro.2018.11.152.

[11] M. Moradi and A. H. Jahangir, "A new delay attack detection algorithm for PTP network in a power substation," *International Journal of Electrical Power & Energy Systems*, vol. 133, p. 107226, Dec. 2021, doi: 10.1016/j.ijepes.2021.107226.

[12] N. Ahmad, L. M. Wei, and M. H. Jabbar, "Advanced Encryption Standard with Galois Counter Mode using Field Programmable Gate Array.," *J. Phys.: Conf. Ser.*, vol. 1019, no. 1, p. 012008, Jun. 2018, doi: 10.1088/1742-6596/1019/1/012008.

[13] C. Cazan and M. Y. Mansour, "WPA3 is the latest generation of Wi-Fi security, bringing simplicity, backward compatibility, and enhanced security. Intel Wi-Fi clients are certified and industry-tested—ready to equip your organization with higher network protection and minimal deployment effort.," p. 4.

[14] L. Wang, J. Yang, and P.-J. Wan, "Educational modules and research surveys on critical cybersecurity topics," *International Journal of Distributed Sensor Networks*, vol. 16, no. 9, p. 1550147720954678, Sep. 2020, doi: 10.1177/1550147720954678.

[15] K. Kumar, K. R. Ramkumar, and A. Kaur, "A lightweight AES algorithm implementation for encrypting voice messages using field programmable gate arrays," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, Part B, pp. 3878–3885, Jun. 2022, doi: 10.1016/j.jksuci.2020.08.005.

[16] C. P. Kohlios and T. Hayajneh, "A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3," *Electronics*, vol. 7, no. 11, Art. no. 11, Nov. 2018, doi: 10.3390/electronics7110284.

[17] Q. Ali, "An Embedded Securıty Center For Internet Of Thıngs (IOT) Infrastructure," Aug. 2017.