ACTA INFOLOGICA 2020;4(2):65-76
dergipark.org.tr/acin

İSTANBUL UNIVERSITY PRESS

DOI: 10.26650/acin.779547

RESEARCH ARTICLE

An Effective Security Method Based on Combining 802.1x, DMZ and SSL-VPN for IoT Network Security

IoT Ağ Güvenliği için 802.1x, DMZ ve SSL-VPN Birleştirme Tabanlı Etkili bir Güvenlik Yöntemi

İlhan Fırat Kılınçer[1], Fatih Ertam[1], Orhan Yaman[1], Abdulkadir Şengür[1]

ABSTRACT

IoT applications appear in many areas due to their flexible structures and many advantages they provide. The increase in IoT applications brings many security vulnerabilities. In order to close these security gaps and ensure the security of the created system, some measures should be taken by combining existing technologies with new technologies. In this study, a method that uses various security technologies together is proposed to ensure the security of the IoT application network. Accordingly, 802.1x technology was used to connect wireless sensor devices to a Wi-Fi network. Thus, in the first step, unauthorized users are not allowed to connect to this network. In the second step, IoT data was collected on a central server, and this server was taken to the DMZ zone in the firewall. Thus, access to the server is both restricted, and server access is logged. In the last step, with SSL-VPN configured in the firewall, data can be safely monitored from the external environment. The biggest advantages of the proposed approach are that it can be used easily in existing Wi-Fi networks, provides communication security, and is low cost. Considering these advantages, it is considered to be an important work in the field of IoT network security..

Keywords: IoT, IEEE 802.1x, DMZ, SSL-VPN, Wireless Sensor Networks, Network Security, Wi-Fi Security

ÖZ

IoT uygulamaları, sahip oldukları esnek yapıları ve sağladıkları birçok avantajdan dolayı birçok alanda karşımıza çıkmaktadırlar. IoT uygulamalarındaki artış, birçok güvenlik açığını da getirmektedir. Bu güvenlik açıklarını kapatmak ve oluşturulan sistemin güvenliğini sağlamak için mevcut teknolojiler, yeni teknolojilerle birleştirilerek bazı önlemler alınmalıdır. Bu çalışmada, IoT uygulama ağının güvenliğini sağlamak için, çeşitli güvenlik teknolojilerini bir arada kullanan bir yöntem önerilmiştir. Buna göre, kablosuz sensör cihazlarının, Wi-Fi ağına bağlanması için 802.1x teknolojisini kullanıldı. Böylelikle, ilk adımda yetkisiz kullanıcıların bu ağa bağlanmasına izin verilmez. İkinci adımda IoT verileri merkezi bir sunucu üzerinde toplanmış ve bu sunucu güvenlik duvarındaki DMZ bölgesine alınmıştır. Böylece, sunucuya erişim hem kısıtlanır hem de sunucu erişimlerinin günlüğü tutulur. Son adımda, güvenlik duvarında konfigüre edilen SSL-VPN ile dış ortamdan verilerin güvenli bir şekilde izlenmesi sağlanmıştır. Önerilen yaklaşımın en büyük avantajları, mevcut Wi-Fi ağlarında rahatlıkla kullanılabilir olması, haberleşme güvenliğini sağlaması ve düşük maliyetli olmasıdır. Bu avantajları göz önünde bulundurulduğunda, IoT ağ güvenliği alanında önemli bir çalışma olduğu düşünülmektedir.

Anahtar kelimeler: IoT, IEEE 802.1x, DMZ, SSL-VPN, Kablosuz Sensör Ağları, Ağ Güvenliği, Wi-Fi Güvenliği

[1]Firat University, Department of Computer Technology, Elazığ, Turkey

ORCID: İ.F.K. 0000-0001-8090-4998;
F.E. 0000-0002-2306-6008;
O.Y. 0000-0001-9623-2284;
A.Ş. 0000-0002-2306-6008

Corresponding author:
Orhan YAMAN,
Firat University, Department of Computer Technology, Elazığ, Turkey
Telephone: +90 424 237 00 00
E-mail address: orhanyaman@firat.edu.tr

Submitted: 12.08.2020
Revision Requested: 05.12.2020
Last Revision Received: 11.12.2020
Accepted: 16.12.2020

Citation: Kılınçer, İ. F., Ertam, F., Yaman, O., & Şengür, A. (2020). An effective security method based on combining 802.1x, DMZ and SSL-VPN for IoT network security. *Acta Infologica, 4*(2), 65-76. https://doi.org/10.26650/acin.779547

1. INTRODUCTION

A. Background

The International Telecommunication Union (ITU) published a report on IoT in 2005. In this report, attention was drawn to the communication between objects. According to this report, a super network covering the whole world can be created by using existing standards and new protocols to be developed. *(Union 2005)(Li et al., 2011).*

One of the most critical areas of IoT is wireless data communication. Wireless networks are technology that communicates one or more wireless devices in the same environment. In addition to wireless communication, data communication can be made with electromagnetic waves in an air environment (Hucaby 2014). In this article, Wireless Local Area Networks (IEEE802.11) technology, one of the wireless data communication technologies, will be studied. WLAN technology, which is one of the wireless network technologies, operates in the microwave spectrum in the frequency spectrum. Fig.1 shows the frequency spectrum.

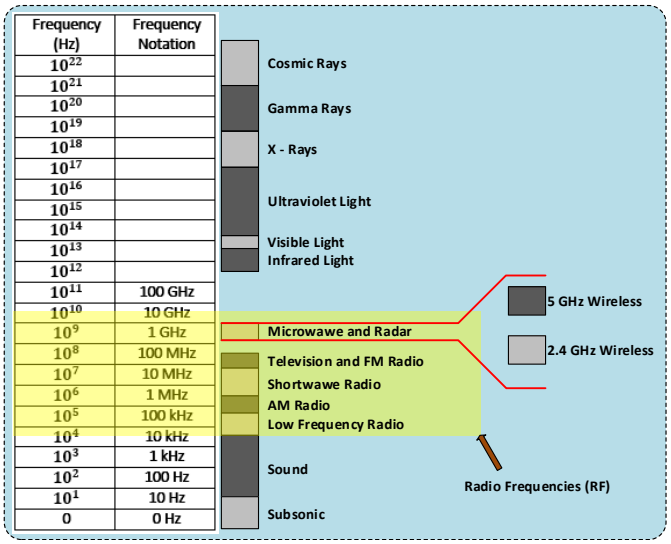

Figure 1. Frequency Spectrum (Hucaby 2014)

As can be seen in Fig.1, WLAN technology broadcasts from the 2.4 GHz and 5 GHz bands. However, not all of the frequency regions in these bands have been used. For the 2.4 GHz band; Frequencies between 2.400 GHz - 2.4835 GHz are used. For 5 GHz band, 5.150 GHz - 5.250 GHz, 5.250 GHz - 5.350 GHz, 5.470 GHz - 5.725 GHz, 5.725 GHz - 5.825 GHz 50 frequencies are used (Hucaby 2014)(Kilinçer et al. 2017).

B. Research Motivation

In addition to traditional Wi-Fi networks, Wi-Fi sensor networks are widely used in many applications that require low power consumption. Studies with Wi-Fi sensor networks are frequently used in IoT applications. Wireless sensors have been widely used in many areas such as personal health monitors, location detection with sensor networks, motion detection, and intrusion detection for military applications. Wireless sensor networks typically consist of small nodes. These nodes have sensing, computing, and wireless communication features. (García-Hernández et al. 2007).

Mendez et al. designed an intelligent wireless sensor network (WSN) for an agricultural area. In their study, Mendez et al. obtained data that affect agriculture, such as temperature, humidity, and water level, with wireless sensor modules. WSN802G model wireless sensors were used in the study. According to the study, data from the WSN802G model sensors were collected on a server, and then various analyses were made from this collected data. The topology of the study is given in Fig. 2 (Mendez and Mukhopadhyay 2013).

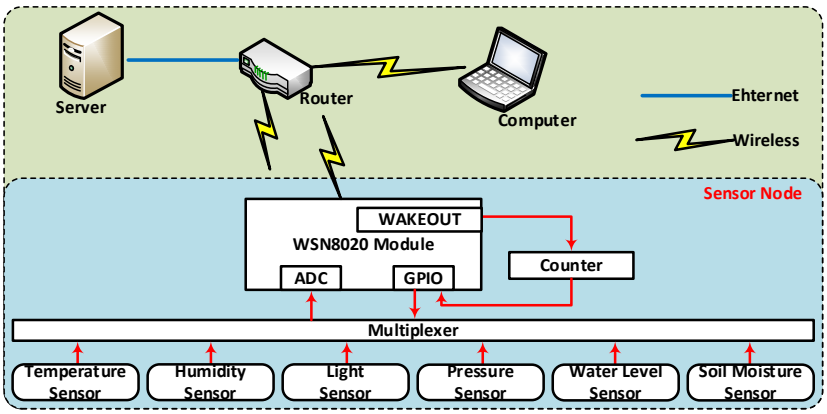

Figure 2. The topology of the system developed by Mendez et al. (Mendez and Mukhopadhyay 2013).

İzzat Din Abdul Aziz et al. have provided automatic control of the greenhouse temperature, which requires a lot of time and effort in traditional farming. Their study developed a system that can monitor and predict temperature and humidity values in greenhouses remotely. For this purpose, they have developed a remote temperature monitoring system by using wireless sensors together with the Short Message Service (SMS). Besides this, they developed an alarm mechanism to keep farmers aware of temperature change with the method they proposed (Aziz et al., 2009).

(Thaker 2016) used the ESP8266 module to implement wireless sensor networks with a Linux-based web service. Raspberry Pi is used as a master server in the system and connects sensor nodes via Wi-Fi on the wireless sensor network. It collects sensor data from different sensors. Data is displayed through an embedded Linux-based Web Server. The block diagram of the wireless sensor network system proposed in the literature is given in Fig. 3.

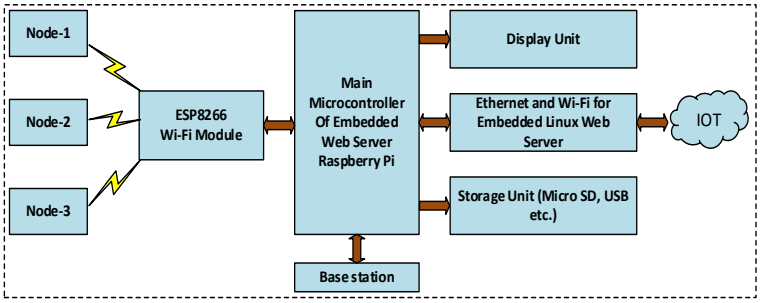

Figure 3. Block diagram of the wireless sensor network system proposed in the literature (Thaker 2016).

Singh et al. have developed an Arduino-based intelligent irrigation system using a water flow sensor, a soil moisture sensor, a temperature sensor, and an esp8266 Wi-Fi module. In this study, an economical and relatively easy-to-use Arduino-based controlled irrigation system has been proposed. The designed system utilizes sensors such as water flow sensors, temperature sensors, and soil moisture sensors to address various environmental factors such as the amount of moisture, temperature, and water needed by the products. Data is collected by Arduino, which can connect to an interactive website that shows real-time values. In this way, the user can control the irrigation pumps from a website and meet the standard values that will help the farmer obtain maximum and quality products (Singh and Saikia 2017).

Saha et al. proposed a data center temperature monitoring and real-time warning system, using an ESP8266-based wireless sensor network. The proposed IoT system has been developed to monitor the temperature at different points in the data center. Temperature data is made visible via the cloud-based dashboard to send SMS and e-mail alerts to pre-defined recipients. The proposed method informs the relevant users when the environment temperature rises above the desired level. In this study, a wireless sensor network was created using a ESP8266 module, a temperature sensor, and a Wi-Fi module (Saha and Majumdar 2017).

Srivastava et al. used ESP8266 to control the hybrid energy system. The ESP8266 regulates the transition between solar and wind energy sources through a website using a Wi-Fi module. Data is wirelessly transmitted to the ESP8266 module that controls energy sources via the website. The transmitted data is controlled remotely using IoT. This system helps the user to control remote energy sources using a smartphone or personal computer (Srivastava et al., 2018).

Srivastava et al., in another study, proposed an IoT-based garden irrigation method using a ESP8266 module. In this study, a sensor module was formed using a water flow sensor, a soil moisture sensor, a temperature sensor, and a pH sensor. The data from the sensor module can be monitored remotely via the ESP8266 module with an Arduino device. The user can run a remote irrigation system (Srivastava et al. 2018b). Pukhanov developed a Wi-Fi-based application for drought detection and early warning system in his master's thesis. A sensor network has been set up using ESP8266 modules to detect over-arid regions in the African continent (Pukhanov 2015). There are a lot of researches developed by using the ESP8266 module in this study (Lin et al. 2014; Kodali and Mahesh 2016b, 2016a; Mahali 2016; Thaker 2016; Pandey et al. 2017; Saha and Majumdar 2017; Škraba et al. 2017; Srivastava et al. 2018b; Tonage et al. 2018)

C. Contributions

In this study, an end-to-end method was proposed for IoT security by combining security technologies such as 802.1x, DMZ, and SSL-VPN, prioritizing privacy. Thus, the security requirements that an IoT network must have have been provided. In this study, a corporate Wi-Fi network was used for both a more flexible and less costly structure. The contributions of this article are as follows;

- Due to the dynamic nature of the proposed sensor network, it is suitable for expansion and can be widely used quickly,
- Communication between nodes is performed safely due to 802.1x, and nodes can secure roaming in different physical areas within the same campus network.
- The server where the data is collected is located in the De Militarized Zone (DMZ) zone configured on a Next-Generation Firewall (NGFW), thereby preventing common cyber-attacks in IoT applications. Behind this, server and node access is done only by users authorized by the firewall.
- A Secure Socket Layer Virtual Private Network (SSL VPN) is used for secure access from outside the campus network.
- An economic model has been created with the low cost of the sensors and the use of a ready-made Wi-Fi network

D. Study Outline

The next sections of the article are planned as follows. In Section 2, information about the IoT network's security and the recommended security standards are given. In Section 3, information is given about the materials used in the IoT system. Data transmission, data collection, and monitoring steps are explained in Section 4. In the data transmission step, the communication steps of the ESP8266 modules using the IEEE 802.1x standard are explained. Also, a flow chart of the proposed method is given. Experimental results are given in Section 5. In Section 6, a comparison of the proposed method with the literature is given. In Section 7, the conclusion of the article is given.

2. IoT SECURITY

A smart home has become an indispensable element in many areas such as smart cities, smart libraries, modern health systems, agriculture, and industrial systems. In addition to the advantages it brings, IoT technology has many security vulnerabilities. One of the most critical issues today is to close these security vulnerabilities. In order to ensure the security of the IoT systems created, there have been studies into developing new technologies and sometimes combining existing security technologies (Amanullah et al. 2020).

There are many studies on IoT security in the literature. Aly et al. conducted a systematic review of IoT security. In this study, security threats in different layers of IoT systems are comprehensively covered (Aly et al., 2019). Sha et al. conducted a review of edge-based security designs for the security of IoT applications. In this study, firewalls, intrusion detection

systems, authentication, and authorization structures are discussed. (Sha et al., 2020). Hussain et al. reviewed encryption and decryption techniques used for IoT security (Hussain and Abdullah 2018). Noor et al. analyzed recent IoT security studies between 2016 and 2018 (Mohamad Noor and Hassan 2019). Amanullah et al. conducted a study with deep learning and big data technologies to process high-volume data generated by IoT applications. Also, the possibilities of combining deep learning and big data technologies for IoT security were investigated in their work (Amanullah et al. 2020). Juma et al. ensured IoT security by combining IPSec VPN and OpenSSL VPN technologies to connect IoT objects (Juma et al., 2020).

Due to the IoT architecture, devices connected to the IoT network can transfer their data to a remote server. In addition, authorized users can connect to the IoT network and perform some operations such as reporting and configuration. Besides such advantages, it also has the problem of IoT security. For this purpose, the following requirements must be met for the IoT network to be secure (Amanullah et al. 2020), (Khattak et al. 2019), (Cho et al. 2011), (Hossain et al. 2015).

- Confidentially: It provides secure communication between all points connected to the IoT network. For this purpose, transactions such as authentication and accounting are critical.
- Integrity: Checks whether the data in the IoT network is changed during communication.
- Availability: Indicates that authorized users can access the IoT network and unauthorized users are denied
- Access Control: Shows users who are authorized to access the IoT network with different security levels (only read, read and write)

In this study, 802.1x, DMZ (Demilitarized Zone), and SSL-VPN (Secure Socket Layer- Virtual Private Network) technologies were used to provide the above security requirements.

- IEEE 802.1x Standard: It is a standard developed for wired networks in the first stage. Later, it was also used in wireless networks due to its security. The main feature of the 802.1x standard is the secure authentication mechanism. With this mechanism, servers and clients can join the network only after their identity is verified. It uses security protocols such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access 1), WPA2 (Wi-Fi Protected Access 2), and WPA3 (Wi-Fi Protected Access 3) for 802.1x standard encryption. WEP is the first produced of these protocols. Also, since the encryption is clear text, passwords can be obtained easily. WPA has emerged due to security vulnerabilities in WEP. Together with WPA, MIC (Message Integrity Check) and TKIP (Temporal Key Integrity Protocol) security mechanisms have been developed. While the MIC mechanism makes the message content more secure against hackers, the switching system has been changed for each data packet with TKIP. Instead of TKIP, AES (Advanced Encryption Standard) was used after a while. Later, the WPA2 standard, which was more secure than the WPA standard, was used. WPA2 used new encryption and authentication mechanisms such as AES and CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) to provide more secure networks. WPA3 security mechanism has been created with the arrival of the latest 802.11ax (Wi-Fi 6) standard. (KILINÇER et al., 2020).

In this study, the WPA3 security mechanism was not used because the campus network does not support the 802.11ax standard. The WPA2-AES security mechanism was used.

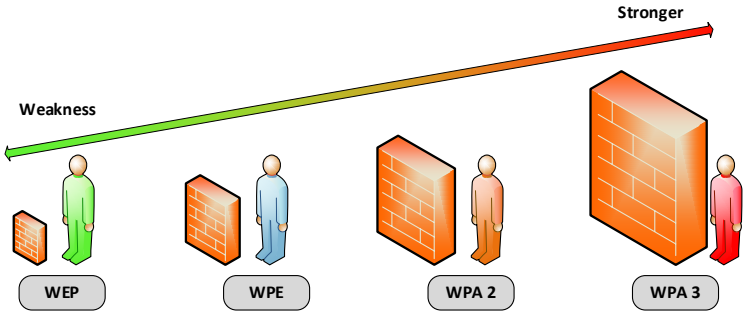

Figure 4. Wireless Security Protocols

• DMZ: It is a security layer that allows servers to be physically or logically separated from the internal network. Thus, access to the server network is controlled by access lists defined on the firewall or router. In this study, to ensure the security of the WIFI_SENSOR_SERVER server, the server was taken to the DMZ zone. Thus, access to this server is both controlled and logged.

• SSL-VPN: It is a virtual private network technology that provides secure access over SSL or TLS protocols. SSL VPN connection is encrypted end-to-end, allowing the data transferred between endpoint devices and the institution's data sources to be transferred over the internet. SSL-VPN encrypts all traffic. For this reason, connecting to the corporate network by SSL-VPN even in a public area does not create any security problems. Many institutions also use it due to its fast, easy installation and stable operation. In this study, SSL-VPN was used to secure access of external users to the IoT network and IoT server.

3. MATERIALS

In this study, a new method has been proposed using Wi-Fi access points and sensor networks. A dynamic wireless sensor network has been developed by connecting ESP8266 Wi-Fi modules to wireless access points in campus networks. The characteristics of the ESP8266 Wi-Fi module, DHT11, and MQ135 sensors are given in Table 1.

Temperature, humidity, and air quality are measured with the ESP8266 module using DHT11 and MQ135 sensors. Relays and buzzers are triggered as the output unit. The data received from the sensors is transferred to the WIFI_SENSOR_SERVER server and stored. Accessing the server via any device connected to the local network, the temperature, humidity, and air quality values in the sensor nodes are monitored. To test the proposed method, temperature, humidity, and air quality sensor nodes are formed. These sensor nodes are shown in Fig. 5.

Table 1

Features of the ESP8266 Wi-Fi module, DHT11, and MQ135 sensor

Module / Sensor	Parameters	Values
ESP8266	MCU	32bit TenSilica
	Clock Speed	80MHz/160MHz
	RAM	<36Kb
	Operating Voltage	3.0V ~ 3.6V
	Operating Current	80mA (Average)
	Available GPIO pins	10
DHT11	Humidity Range	20-80%
	Temperature Range	0°C ~ 50°C
	Accuracy	±5% (Humd), ±2°C
	Repeatability	±1% (Humd), ±1°C
MQ135 Air Quality	Circuit voltage	5V±0.1
	Heater resistance	33Ω±5%

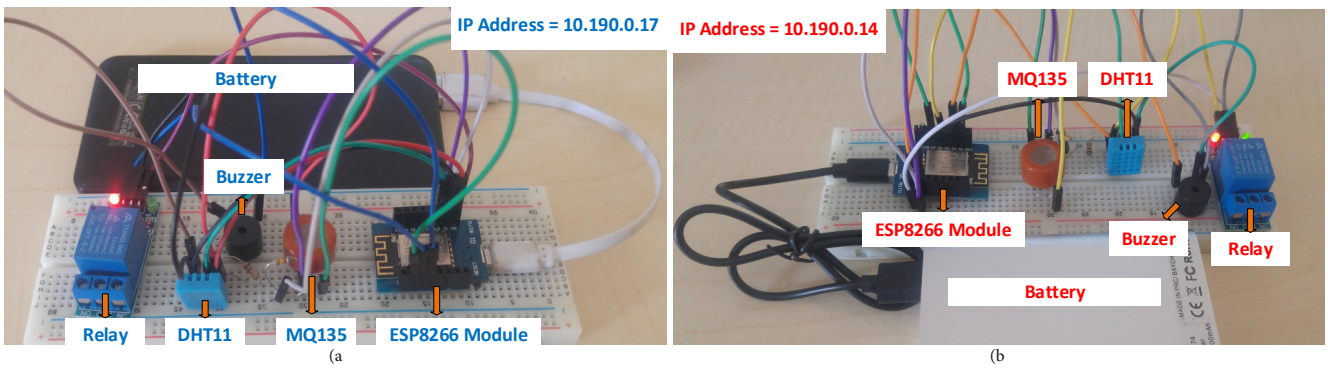

Figure 5. Sensor nodes developed in this study a) Node 1 b) Node 2

The sensor nodes, shown in Fig. 5, make IEEE 802.1x authentication to connect the Wi-Fi campus network. With this authentication method, the wireless sensor network infrastructure is secured. TTLS and PAP protocols are used for IEEE

802.1x authentication. Identity information and password are defined for each node. The ESP8266 modules use these credentials when connecting to the wireless LAN. Thus, the security of the local wireless network is ensured.

4. PROPOSED METHOD

The general topology of the proposed system is given in Fig. 6. The Fırat University campus Wi-Fi network was used for the proposed system. The proposed system generally consists of data transfer, data collection, and the display of collected data. The flow diagram in Figure 7 is used in the data transfer step, which is the first step of the system.

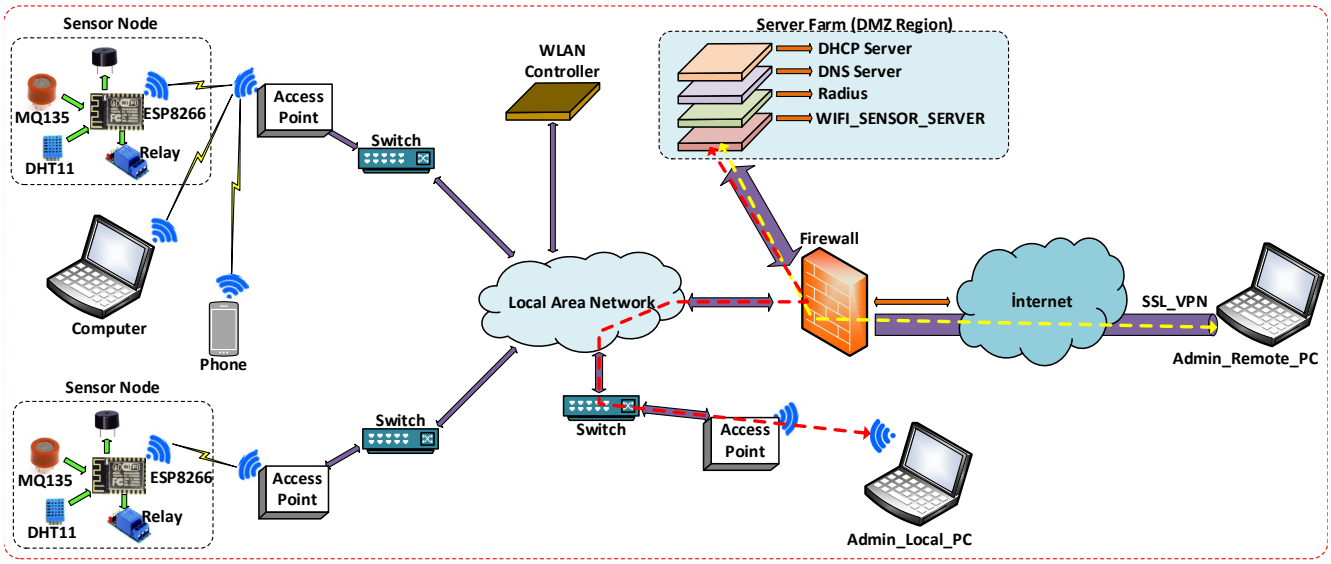

Figure 6. The topology of the proposed system

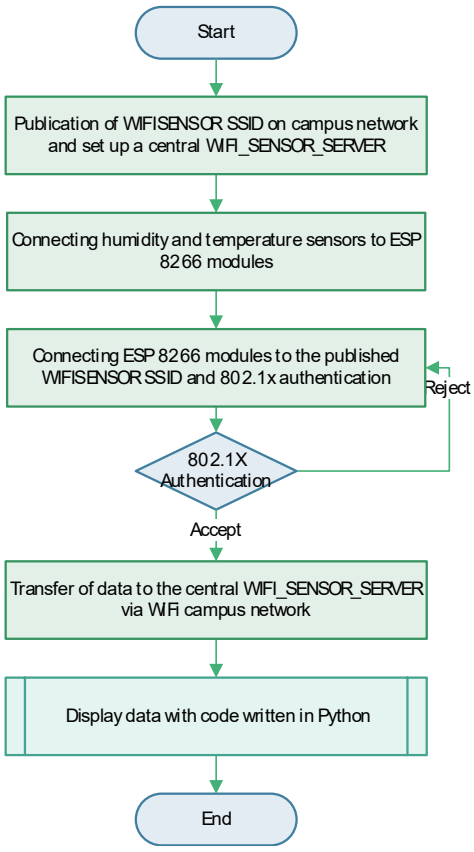

Figure 7. Algorithm of data transmission

The flow chart given in Fig. 7 generally consists of 3 steps. In the first step, according to the flow chart, WIFI_SENSOR SSID was created on the access points to transmit the sensor traffic to the server. Also, the ESP8266 module is integrated into the DHT11 and MQ135 modules, which are humidity, temperature, and air quality sensors. The Microsoft Windows Server 2012 operating system has been installed on the WIFI_SENSOR_SERVER server, which is located on the central server farm, to provide both data collection and IEEE 802.1x authentication.

In the second step, IEEE 802.1x authentication was performed for data transmission. There are three main components in the IEEE 802.1x protocol: the authenticator, the authentication server, and the client to be authenticated. In this study, the Radius server was used as the authentication server. Network Policy Server (NPS) and Active directory features on the Windows Server 2012 operating system were activated. Fig. 8 shows the general 802.1x messaging steps (Chen and Wang 2005; Chen et al. 2005; Fantacci et al. 2007; Gu and Zhang 2010; Zha and Ma 2010; Alabdulatif et al. 2013; Hermaduanti and Riadi 2016).

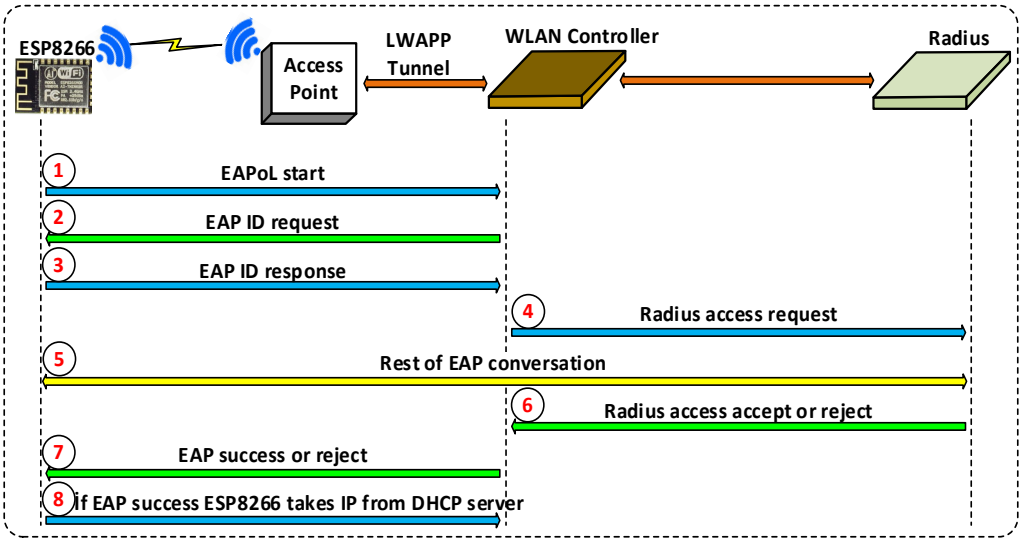

Figure 8. Algorithm of data transmission

When Fig. 8 is examined, the client connects to the wireless network and sends the EAPoL start message to the authenticator device. The authenticator device between the client and the authentication server requests the client to identify itself by sending an EAP-ID Request packet to the client. The client responds to the authenticator device with the EAP-ID Response package. The authenticator encapsulates this package and sends it to the authentication server (Radius Server). As a result of a series of subsequent EAP messaging, the authentication server sends an access-to-accept message to the authentication device if the client has the required user authority. Thus, the authentication device allows the client to join the network. Connected to the WIFI_SENSOR network after the 802.1x authentication step, the ESP 8266 Wi-Fi module gets an automatic IP address through the DHCP server.

The ESP 8266 module sends the humidity, temperature, and air quality data to the central WIFI_SENSOR_SERVER server in the data collection step.

In the last step, the data coming from the sensors to the WIFI_SENSOR_SERVER server is displayed. A code has been written in the python language to display the data.

In this study, after taking the necessary security measures on the local network with 802.1x, the server was moved to the DMZ region of the NGFW. Thus, server security is provided. New generation firewalls (NGFWs) can detect attacks with security principles at application and protocol levels. Thanks to modules such as the Intrusion Prevention System (IPS) on the NGFW, it constantly examines traffic flows and detects vulnerability exploits. Server accesses are restricted to Access-lists defined on the NGFW. Thanks to the NGFW's features such as threat prevention, URL filtering, and antivirus, the server is prevented from being hacked by an attacker. Thus, the server is protected against threats from internal and external

networks, and server accesses are logged. Authorized users are defined on the NGFW, so authorized users can access nodes and servers securely. An SSL VPN is used for authorized users to access sensors and servers from external networks.

5. EXPERIMENTAL RESULTS

The ESP8266 module is connected to the WIFI_SENSOR network. The Wireshark program is used to listen to the packet.

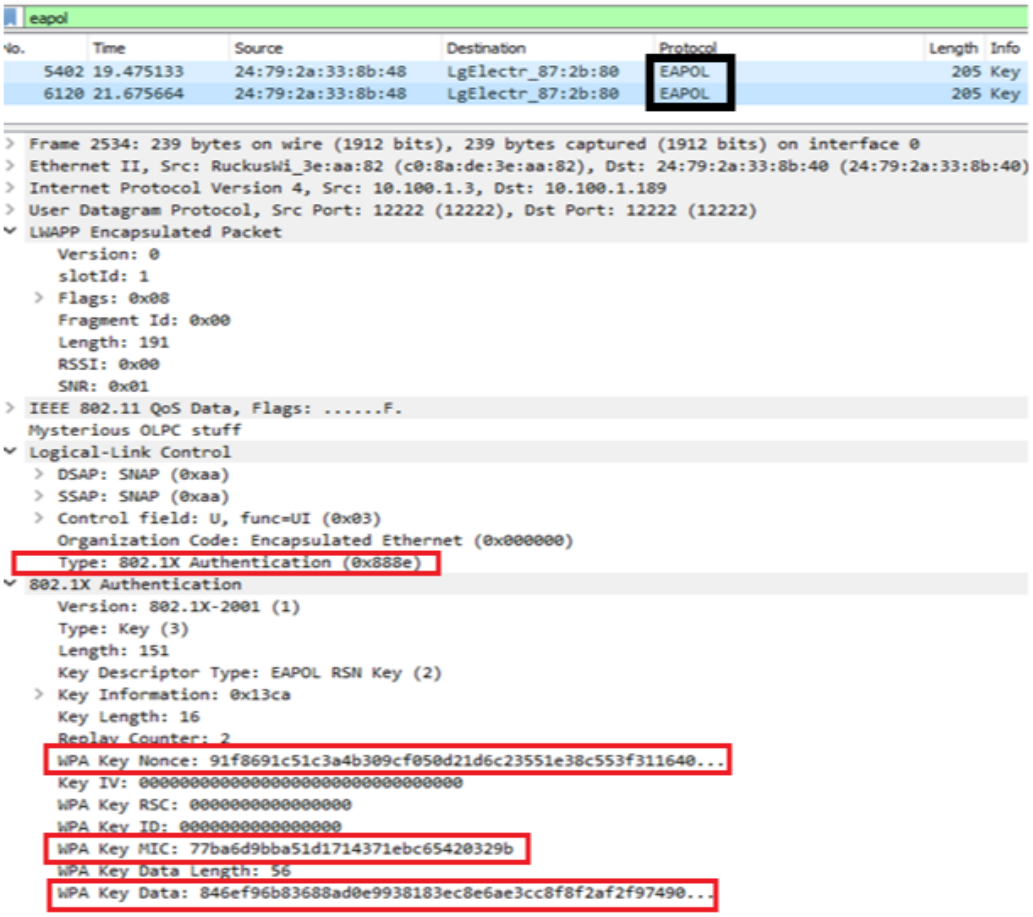

Figure 9. Connection of ESP8266 module to WIFI_SENSOR network and authentication of 802.1x

As shown in the Wireshark output of Fig. 9, each sensor node is connected wireless network using the 802.1x protocol. Once the authentication is complete, the nodes transmit data to the server. A status monitoring interface was developed using the Python programming language and Google Chart technology on the server. This interface is given in Figure 10.

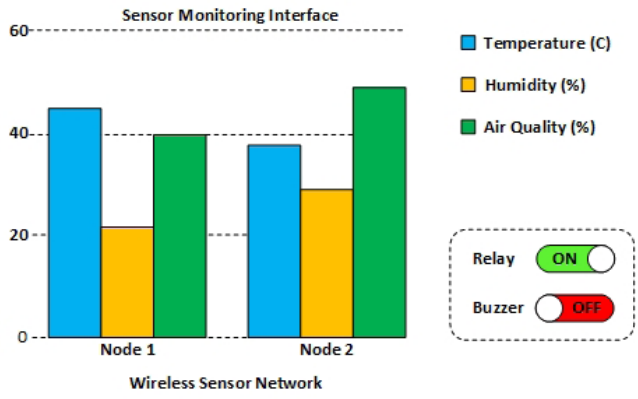

Figure 10. Monitoring of data from sensor nodes

In Fig. 10, the temperature, humidity, and air quality values of each sensor node are monitored. The proposed study is compared with the literature in Table 2.

Table 2
Comparing the proposed method with the literature

Features	Proposed Method	Singh et al	Saha et al	Ocal	Ravi et al	Juma et al
Dynamic Network	✓	X		X	X	X
802.1x	✓	X	X	X	X	X
DMZ Zone	✓	X	X	X	X	X
VPN	✓	X	X	X	X	✓
Add a Dynamic Node	✓	X	✓	X	X	✓
Mutual Device Authentication	✓	X	X	X	X	X
Sensors Used	Temperature, humidity, Air quality, Relay, Buzzer	Water flow Soil moisture Temperature	Temperature, Humidity	Temperature, Gas	Temperature	X

As can be seen in Table 2, five important advantages of the proposed method, according to the literature, are remarkable. Firstly, the proposed method is suitable for the dynamic network structure. The dynamic network is that the wireless sensor nodes can be connected to access points located at any point in the campus network. In the recommended method, the ESP8266 Wi-Fi modules are connected to the local network by connecting to wireless access points on the campus network instead of creating a wireless network by connecting to each other. Thus, even if the sensor nodes move within the campus, they are connected to another access point by roaming. With the roaming feature, the connection of the sensor nodes continues without interruption. The ESP8266 Wi-Fi modules connect to any wireless device within the campus network and communicate with the server very easily. Thus, a portable sensor node is designed within the campus network. The fact that the proposed method has a dynamic structure contributes to the studies conducted earlier. Another advantage of the proposed method is the IEEE 802.1x technology. When the sensor nodes communicate with the central server, the data transfer needs to be done securely. When the studies in the literature are examined, there is no security infrastructure such as 802.1x protocol in data communication between nodes and server. The use of the 802.1x protocol in this study is thought to significantly contribute to the literature. The third advantage of the proposed method is that the server where the data is transferred is in the DMZ region defined on the NGFW. In this way, the system is ensured to be minimally affected by the malware or other attack types in both local and external networks. The fourth advantage of the proposed method is that the logins can be logged through the NGFW. The last advantage of the proposed method is to provide secure access to the systems with an SSL VPN wherever there is internet.

6. DISCUSSION

Continuous expansion and growth of IoT networks have brought many security vulnerabilities. In most of the literature studies, there are no concrete solutions to secure the IoT network. In this study, our priority is to ensure the security of the IoT network. Some types of attacks that can be done on a network are given in Table 3. With the 802.1x technology we use in this study, many attacks such as MiTM, arp spoof, DHCP snooping, and DNS spoofing are prevented as we do not take users into the network without authentication. In addition, by making the 802.1x standard with WPA2-AES, precautions have been taken against de-authentication attacks, which are the most common attack type in Wi-Fi networks. Because even if there is a de-authentication attack on this prepared Wi-Fi network, the data is encrypted with the WPA2 protocol. The server where the IoT data is collected, and the IoT network is protected by the NGFW. Therefore, the IoT network and server are protected against harmful traffic such as malware, DoS, and spyware from outside.

Table 3
Comparing the proposed method with the literature

Atack-types	Proposed Method	Singh et al	Saha et al	Ocal	Ravi et al	Juma et al
Malware	✓	X	X	✓	X	✓
DoS	✓	X	X	✓	X	✓
MiTM	✓	X	X	X	X	X
Deauthentication Attack	✓	X	X	X	X	X
Arp spoof	✓	X	X	X	X	X
DHCP Snooping	✓	X	X	X	X	X

7. CONCLUSIONS

In this study, using wireless access devices in campus networks with wireless sensor networks has been developed. The proposed method uses the DHT11 temperature and humidity sensor and the MQ135 air quality sensor with the ESP8266 Wi-Fi module. The ESP8266 Wi-Fi module connects wireless access points on campus networks with the 802.1x protocol. Temperature, humidity, and air quality values from sensors are transferred to the server and stored. Also, in this study, a secure IoT network was created by using 802.1x, DMZ, and SSL-VPN technologies together. Thus, the IoT system is prevented from being easily captured from attackers' traffic. Compared to the literature, it is clear that the proposed method is original.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazarlar çıkar çatışması bildirmemiştir.
Finansal Destek: Bu çalışma FUBAP (Fırat Üniversitesi Bilimsel Araştırma Projeleri Birimi) tarafından hibe no: TEKF.20.18. kapsamında desteklenmiştir.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The authors have no conflict of interest to declare.
Grant Support: This work was supported by the FUBAP (Firat University Scientific Research Projects Unit) under Grant No: TEKF.20.18.

References

Alabdulatif A, Ma X, Nolle L. Analysing and attacking the 4-way handshake of IEEE 802.11i standard. In: 2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013. 2013. p. 382–7.

Aly M, Khomh F, Haoues M, Quintero A, Yacout S. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. Internet of Things. 2019;6:100050.

Amanullah MA, Habeeb RAA, Nasaruddin FH, Gani A, Ahmed E, Nainar ASM, et al. Deep learning and big data technologies for IoT security. Vol. 151, Computer Communications. 2020. p. 495–517.

Aziz IA, Hasan H, Ismail J, Mehat M. Remote Monitoring in Agricultural Greenhouse Using Wireless Sensor and Short Message Service (SMS). Int J Eng Technol IJET. 2009;9(9):1–12.

Chen JC, Jiang MC, Liu YIW. Wireless LAN security and IEEE 802.11l. IEEE Wireless Communications. 2005.

Chen JC, Wang YP. Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience. IEEE Commun Mag. 2005;

Cho JS, Yeo SS, Kim SK. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Comput Commun. 2011;34(3):391–7.

Fantacci R, Maccari L, Pecorella T, Frosali F. Analysis of secure handover for IEEE 802.1X-based wireless ad hoc networks. IEEE Wirel Commun. 2007;

García-Hernández C, Ibargüengoytia-González P, García-Hernández J, Pérez-Díaz J. Wireless Sensor Networks and Applications: a Survey. IJCSNS Int J Comput Sci Netw Secur [Internet]. 2007;7(3):264–73. Available from: http://campus.cva.itesm.mx/jdperez/documentos/IJCSNS-WSN-publicado-03-2007.pdf

Gu YH, Zhang JX. Research on the security of IEEE 802.1x authentication mechanism in wireless LAN. In: 2nd International Conference on Information Science and Engineering, ICISE2010 - Proceedings. 2010.

Hermaduanti N, Riadi I. Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN. J Theor Appl Inf Technol. 2016;

Hossain MM, Fotouhi M, Hasan R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In: Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015. 2015. p. 21–8.

Hucaby D. CCNA wireless 640-722 official cert guide [internet]. 2014. Available from: https://www.safaribooksonline.com/library/view/ccna-wireless-640-722/9780133445725/

Hussain R, Abdullah I. Review of Different Encryptionand Decryption Techniques Used for Security and Privacy of IoT in Different Applications. In: 2018 6th IEEE International Conference on Smart Energy Grid Engineering, SEGE 2018. 2018. p. 293–7.

Juma M, Monem AA, Shaalan K. Hybrid End-to-End VPN Security Approach for Smart IoT Objects. J Netw Comput Appl. 2020;158.

Khattak HA, Shah MA, Khan S, Ali I, Imran M. Perception layer security in Internet of Things. Futur Gener Comput Syst. 2019;100:144–64.

KILINÇER İF, ERTAM F, ŞENGÜR A. Automated Fake Access Point Attack Detection and Prevention System with IoT Devices. Balk J Electr Comput Eng. 2020;

Kilinçer IF, Ertam F, Yaman O, Akbal A. Automatic fault detection with Bayes method in university campus network. In: IDAP 2017 - International Artificial Intelligence and Data Processing Symposium. 2017.

Kodali RK, Mahesh KS. A low cost implementation of MQTT using ESP8266. In: Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016. 2016a.

Kodali RK, Mahesh KS. Low cost ambient monitoring using ESP8266. In: Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016. 2016b. p. 779–82.

Li L, Hu X, Chen K, He K. The applications of WiFi-based Wireless Sensor Network in Internet of Things and Smart Grid. In: Proceedings of the 2011 6th IEEE Conference on Industrial Electronics and Applications, ICIEA 2011. 2011. p. 789–93.

Lin Y, Kong R, Guan M, She R. Design and implementation of smart home intranet based on ZigBee. Res J Appl Sci Eng Technol. 2014;

Mahali MI. Smart Door Locks Based On Internet Of Things Concept with Mobile Backend as a Service. J Electron Informatics, Vocat Educ. 2016;

Mendez GR, Mukhopadhyay SC. A Wi-Fi based smart wireless sensor network for an agricultural environment. In: Smart Sensors, Measurement and Instrumentation. 2013. p. 247–68.

Mohamad Noor M binti, Hassan WH. Current research on Internet of Things (IoT) security: A survey. Comput Networks. 2019;148:283–94.

Pandey RC, Verma M, Sahu LK. Internet of Things (IOT) Based Gas Leakage Monitoring and Alerting System with MQ-2 Sensor. Int J Eng Dev Res. 2017;

Pukhanov A. Wi-Fi Extension for Drought Early-Warning Detection System Components by. 2015;

Saha S, Majumdar A. Data centre temperature monitoring with ESP8266 based Wireless Sensor Network and cloud based dashboard with real time alert system. In: Proceedings of 2nd International Conference on 2017 Devices for Integrated Circuit, DevIC 2017. 2017. p. 307–10.

Sha K, Yang TA, Wei W, Davari S. A survey of edge computing based designs for IoT security. Digit Commun Networks. 2020;

Singh P, Saikia S. Arduino-based smart irrigation using water flow sensor, soil moisture sensor, temperature sensor and ESP8266 Wi-Fi module. In: IEEE Region 10 Humanitarian Technology Conference 2016, R10-HTC 2016 - Proceedings. 2017.

Škraba A, Koložvari A, Kofjač D, Stojanović R, Stanovov V, Semenkin E. Prototype of group heart rate monitoring with NODEMCU ESP8266. In: 2017 6th Mediterranean Conference on Embedded Computing, MECO 2017 - Including ECYPS 2017, Proceedings. 2017.

Srivastava P, Bajaj M, Rana AS. IOT based controlling of hybrid energy system using ESP8266. In: 2018 IEEMA Engineer Infinite Conference, eTechNxT 2018. 2018a. p. 1–5.

Srivastava P, Bajaj M, Rana AS. Overview of ESP8266 Wi-Fi module based smart irrigation system using IOT. In: Proceedings of the 4th IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB 2018. 2018b.

Thaker T. ESP8266 based implementation of wireless sensor network with Linux based web-server. In: 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016. 2016.

Tonage S, Yemul S, Jare R, Patki V. IoT based home automation system using NodeMCU ESP8266 module. Int J Adv Res Dev. 2018;

Union IT. ITU Internet Reports 2005: The Internet of Things. Vol. 4, Communications Engineer. 2005.

Zha X, Ma M. Security improvements of IEEE 802.11i 4-way handshake scheme. In: 12th IEEE International Conference on Communication Systems 2010, ICCS 2010. 2010. p. 667–71.

Wireless Security Protocols [Internet]. Available from: https://ipcisco.com/lesson/wireless-security-protocols/