NaSTech
JOURNAL OF NATURAL SCIENCES AND TECHNOLOGIES
2025, 4(1), pp. 340-344, DOI: 10.5281/zenodo.16607575

ENSURING DATA SECURITY IN DATA COLLECTED FROM THE PRODUCTION AREA IN FACTORIES

Hasan Erdinç KOÇER[1] , Faruk BEYAZKAYA [2]

[1] Selçuk University / Faculty of Technology / Department of Electrical And Electronics Engineering / Division of Circuits And Systems

[2] Selçuk University, Institute of Science, Department of Electrical And Electronics Engineering, Konya, Turkey

ABSTRACT

Technological developments change the way of life of the society and new technological devices are introduced to the market every day. After the fourth industrial revolution, smart homes and factories are put into service with Internet of Things (IoT) devices, which are now in every aspect of people's lives. Smart homes and factories built with IoT devices collect data from daily used vehicles and systems and transmit them to the cloud environment or server hardware. One of the most important problems in these transactions is the risk of data being stolen and copied. In order to overcome these problems, it is essential to ensure the security of the data. With its simple and inexpensive devices, IoT has brought with it complex and costly security and privacy problems. IoT devices that cannot take adequate precautions due to their low resources become the primary target of attackers. IoT applications are exposed to many attack methods such as eavesdropping, copying, duplication and blocking.
In this paper, it is aimed to realize the software and hardware activities of the electronic device that encrypts the data with various encryption algorithms in order to overcome the data security problem such as listening and copying during data transmission in wired and wireless environment in the production area in factories. For this purpose, an interface unit was created using ESP 32 and the data from the sources will be encrypted on this electronic card and transmitted to the target in a wired or wireless way. The encrypted data is decrypted on the target device using USB Stick hardware.

Keywords: Data Security, Encryption-Decryption, Internet of Things

1. INTRODUCTION

IoT comprises billions of connected smart devices around the world that exchange information with minimal human intervention. IoT is progressing at an enormous pace with an estimated 27 billion IoT devices by 2025 (i.e., almost four IoT devices per person). IoT provides real-life smart applications that improve quality of life and they have become part of our daily activities. Wearable tools and gadgets help us monitor and take care of our health, vehicles interact with traffic centers and other vehicles to improve safety, and different home elements and appliances enhance our quality of life. The significant increase in the number of IoT devices, as well as the success of IoT services and applications, have contributed to the rapid growth in the amount of generated data. The International Data Corporation report has estimated that the amount of data will increase from 4 to 140 zettabytes between 2020 and 2025. The significant amount of personal data collected and shared by IoT is posing increasing concerns for user privacy. In this line, several recent reports identify the different security and privacy threats associated. Gartner estimates that around 15 billion smart devices will be connected to the computing network by the end of 2022. Not only could the devices be vulnerable but the enormous amount of not-secured data collected and stored online is a liability [1].

These devices, which we call IoT devices; smart homes, wearable devices, smart cities, healthcare, automotive, environment, smart water, smart grid, etc. It is growing its usage area day by day by optimizing production and transitioning industries to information technologies. However, many of these IoT devices are easy to compromise and the data they transmit is easy to alter. Typically, an IoT device is limited in terms of information processing, storage and network capacity, making it more vulnerable to attacks. The IoT middleware used to communicate between entities in IoT systems must be secure in order to provide services in a healthy way. If necessary, different designs, different interfaces or different environments should be included in the system to ensure this secure communication.

In the current century, the density of digital data in our lives has started to increase quite rapidly. This data is being used extensively to facilitate human beings' work, improve their quality of life and provide them with more active information about what is happening around them. And since this data is actively transmitted over the internet, it is constantly accessible. The technology that enables this intense data transfer between human beings and data is called IoT. This data, which will add value and information to human life, is collected through sensors. Although

this technology provides very important benefits to human life, it is still a question mark in terms of data security. If the accuracy and security of the data cannot be ensured, the data obtained from IoT devices will continue to remain a question mark in people's minds.

2. LITERATURE REVIEW

With the development of technology, huge amounts of data have been generated in recent years. Almost every device we use generates a certain amount of data and many of them transmit this data to a remote device. In enterprises operating in the manufacturing sector, the data generated from the devices operating in the production area contain commercial confidentiality and are intended to be captured by malicious people. Various devices that listen to and copy data transmitted over wired or wireless media are produced and sold. Although various devices that intercept signals have been produced in order to prevent listening and copying, it has also brought along problems such as the prevention of data transmission of other communication devices for internet, telephone purposes. Therefore, instead of preventing the data from being copied or stolen, it is more preferred to encrypt and send the data. When we look at the literature, we see that there are studies to ensure data security with various methods. Most of these are in the direction of encrypting and preserving the data in the hardware environments where the data is stored. We also see that there are studies to ensure data security during data communication. Although the term Internet of Things (IoTs), which is defined as “a communication network in which physical objects are connected to each other or to larger systems”, is becoming increasingly widespread, there is no consensus definition that reveals what this term actually includes.

In other words, the Internet of Things means that objects, devices or things can connect, communicate and interact with each other thanks to the developing communication technology (Altınpulluk, 2018) without the need for physical contact of the individual, i.e. touching and entering data. This concept entered the literature when Kevin Ashton used it in a presentation in 1999. With the developing technology, it has reached a level that can communicate and connect with each other through various communication protocols. As a result of the information shared, smart networks have been created. In the age of technology, there are rapid scientific developments and innovations. Every conceivable object, every electronic device that is currently used can be developed with an internet connection, and this allows devices to become smart objects (Abouzakhar et al., 2017).

İşiçelik, U. (2021) aimed to read the meter data with Raspberry-Pi hardware, match the data of the meter with the person and store it on the remote server. With this study, the security of the data recorded both at the hardware level and at the software level was examinedGüven, E. Y. (2018) introduces Edge Computing that works between Cloud Computing and Internet of Things devices. Kılıç Edge Computing Security Application, which runs on Edge Computing and provides security for Internet of Things devices, is proposed. Kılıç and its modules, which provide a variable security approach according to the threat level, are explained in detail. The attacks and threats that Internet of Things devices are exposed to are also analyzed. Against these attacks and threats, Kılıç provides real-time protection using rule- based and machine learning methods. Machine learning methods such as Decision Tree, Support Vector Machine, K-Nearest Neighbor, Deep Learning and Naive Bayes algorithms are used. In addition, a real-time industry application is demonstrated in the context of a Smart Factory to show the effective use of Kılıç.

Divarcı, S. (2018) Within the scope of the thesis, a secure gateway that works at the point where the Internet of Things systems are opened to the Internet and can encrypt the data to be transferred over the Internet and provide data integrity control has been designed. When a data from the IoT network is to be sent to another point over the Internet, this data will be transmitted over the designed gateway. The designed gateway protects the confidentiality and integrity of packets at the network level using the IPsec protocol. By providing IKEv2 protocol capability to the designed system, the crypto keys required for the encryption and digest extraction algorithms to be used in the secure gateway are automatically generated. Thanks to the IKEv2 protocol, IPsec has become a more flexible and scalable security protocol.

Mutlu, G. (2019) aimed to develop a cost-effective and secure IIoT gateway in his thesis. The gateway sends data collected from various devices with Modbus protocol to the relevant unit (server application, another device, etc.) via a Broker for processing. MQTT is the standard communication protocol in IIoT systems that allows data transfer over TCP/IP in the clear or encrypted with TLS protocol. In most factory environments, data is transmitted in the clear for processing power saving and speed reasons. However, sending data in the clear (unencrypted) can cause very serious problems due to theft/modification of information, which can cost lives. Future work could evaluate the use of other software implementations of ATAES132A and SPI connection interfaces for more efficient communication between the processor and the integrated. Also, ARM Cortex-M3 (STM32F217VGT6)

with encryption algorithms such as AES, MD5, SHA-1 can be used. ÇALIŞKAN, M. In his thesis written in 2014, many studies have been carried out on determining the methods of effective use of intrusion detection and prevention systems and increasing their performance. Although IDPS accuracy and hardware (CPU, RAM) utilization performance values have not reached the desired level, serious progress has been made. The use of virtualization technologies in IDPS continues, and the performance increases that will occur as a result of the use of virtualization technologies and IDPS together are being monitored. Considering the low intrusion detection rate of intrusion detection systems as the most important problem, M. Alshawabkeh et al. (2011) proposed a new feature selection algorithm using virtual server environments. The proposed algorithm consists of numbers weighting the features of subsets of the system and a "tolerance number" that is generated according to the best hypothesis learned from these features. An evaluation function is run on the "tolerance number" and an intrusion detection decision is made. As a result of this algorithm, it was observed that the detection rates of IDSs running on VMM increased successfully. While selecting the subset features, "greedy search strategy" from artificial intelligence applications was used.

3. METHODOLOGY

In this study, LED, LDR, temperature and humidity sensors were used to represent the devices used in smart factories with continuous data generation. In addition, with the ESP 32 microcontroller system integrated with these devices, data is read, processed, encrypted and displayed decrypted on the server. To ESP32 Microprocessor;
- Three LEDs in Red, Yellow, Green Colors are connected. These LEDs were turned on / off remotely using Bluetooth.
- One LDR Sensor is connected. This sensor gives a value between 0 - 4095. As the ambient light value increases, the value approaches 4095.

- One DHT11 Temperature / Humidity Sensor is connected. All of the data belonging to these components connected to ESP32 were collected in a single place in JSON data format in the programming section and this data was converted to String format and published through a single Topic (jsonPub) and sent to the MQTT Broker server.

A sample JSON data is below:

{"ledStates":"0,0,0","ldrSensor":"2678","tempSensor":"29.30",'humiditySensor':"61.00"}

For example, when the Red LED is turned on, the ledStates variable takes the value "1, 0, 0". Then, when the Green LED is also turned on, the ledStates variable takes the value "1, 0, 1". When the Red LED is turned off again, the ledStates variable takes the value "0, 0, 1". MQTT Broker, Node-RED and InfluxDB applications were installed on Ubuntu Server. Ubuntu Server was installed on a virtual computer using VMware Workstation program and settings were made. In the project, we said that ESP32 converts the data in JSON format into String format and sends it to the MQTT Broker via a specific Topic (jsonPub). On the Node-RED side, the "mqtt in" node was created to Subscribe to this Topic (jsonPub). The data from the MQTT Broker Server is received through this node. The "mqtt in" node receives data in JSON data structure in String format. In order to use the features of the JSON data structure, the JSON data must be parsed (parse). After parsing, a new String data was created for easier reading of the data. Original JSON Data (String) from ESP32:

{"ledStates":"0,0,0","ldrSensor":"2678","tempSensor":"29.30",'humiditySensor':"61.00"}

Newly created String Data: ledStates: 0, 0, 0, 0 - LDR: 2678 - Temperature / Humidity: 29.3 / 61Then the "Encryption" node was used to encrypt this String data. AES-256-CBC algorithm with the key 1q1w1e2a2s2d3z3x was used for encryption. This node uses the Javascript Crypto library for encryption (https://flows.nodered.org/node/node-red-contrib-crypto-js). The key value can be changed via the "Encryption" node if desired. Sample Encrypted Data:

U2FsdGVkX1+sNNwyU2+nvMSwju8YZzrbDqScDJlT+cIDYBKBoCcsfQGUUUNdFEkYk6/XUvldhVXXm5
q7X6lDIhBS+vW3BasOioVUuWjkLj7qaq3VPpxNEo4RlXeVW+Xb
The "InfluxBatch" node was used to save this encrypted data to the InfluxDB database.

JOURNAL OF NATURAL SCIENCES AND TECHNOLOGIES
2025, 4(1), pp. 340-344, DOI: 10.5281/zenodo.16607575

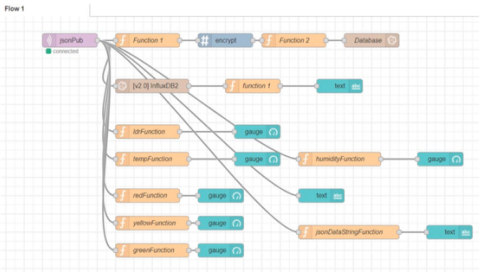

Figure 1. All Nodes and Functions Created in Node-RED

Figure 2. Graphical İnterface

The JSON Data (String) section shows the original data from ESP32. To the right of it is the String data we just created and the encrypted version of this String data is shown in the Encrypted Data (Database) section and this encrypted data is also instantly saved to the database. The graphical interface updates the data every two seconds. In the project, Python programming language was used to connect to the database, retrieve the encrypted data and decrypt it using the key we set. Python was preferred due to its library support and simple writing language. In the Python program, firstly, the encrypted data was received by connecting to the database and saved to a file in 'csv' format (encryptedData). The encrypted data was then decrypted using the key. The timestamp of when the data was added to the database was also obtained. The decrypted data was saved in a 'csv' file with dates. This Python program is saved on a Flash drive and does not require Python to be installed on the computer where the Flash drive is installed. The key information is stored in the '.env' file inside the Flash drive. The '.env' file is also used by the Python program. Technically, a person without a Flash Drive will not be able to decode the data in the database. The control of the LEDs was provided by the 'Serial Bluetooth' application obtained free of charge from the Google Play Store.

4. CONCLUSION

As a result; in this study, the machines that produce in smart factories are simulated. it is aimed that the wired and wireless data transfer of these machines can be secure. USB is used as a key for data access. For those who do not have a USB key, the data is intended to be secured.

REFERENCES

[1] Rodríguez, E., Otero, B., & Canal, R. (2023). A survey of machine and deep learning methods for privacy protection in the Internet of Things. Sensors, 23(3), 1252.

[2] Y. Yang, L. Wu, G. Yin ve H. Zhao, «A Survey on Security and Privacy Issues in IoT» cilt 4, no. 5,2017.

[3] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. . A. Savikko ve H. Leppäkoski, «Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey,» cilt 5, 2017).

[4] Agarwal, P., Tipaldi, G., Spinello, L., Stachniss, C., and Burgard, W. Robust mapoptimization using dynamic covariance scaling, in Robotics and Automation (ICRA), 2013 IEEE International Conference on, pp. 62–69,

[5] F. Ivan, T. Taleb, Y. Khettab ve J. Song, «A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems,» cilt 21, no. 1, 2019.

[6] G. Zhan, Y. Jiang, X. Yin ve S. Li, «Research on security of NB-IoT based on cryptography,» 4th Int. Conf. on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE),China, 2021.

[7] Güven, E. Y. (2018). Kenar bilişim için siber saldırıları tespit ve önleme yöntemleri (Master's thesis, Fatih Sultan Mehmet Vakıf Üniversitesi, Mühendislik ve Fen Bilimleri Enstitüsü).

[8] İşiçelik, U. (2021). Dar bant nesnelerin interneti uygulamalarında veri güvenliği (Master's thesis, Maltepe Üniversitesi, Lisansüstü Eğitim Enstitüsü).

[9] Divarcı, S. (2018). Nesnelerin interneti için güvenli ağ geçidi tasarımı (Master's thesis, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü).

[10] Mutlu, G. (2019). Endüstriyel Nesnelerin Interneti Için Güvenli Ağ Geçidi (Doctoral dissertation, Bursa Uludag University (Turkey).

[11] Kurt, A. (2021). Ağ Tabanlı Saldırı Tespit Sistemlerinde Topluluk Öğrenme Yöntemlerinin Karşılaştırmalı Performans Analizi (Master's thesis, Sakarya Üniversitesi).

[12] Çalışkan, M. (2014). B. M. A. B. D. Sanallaştırma Teknolojilerinin Saldırı Tespit ve Önleme Sistemlerinin Performansı Üzerine Etkisi. (Hava Harp Okulu Havacılık ve Uzay Teknolojileri Enstitüsü)

[13] Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). Materials Today: Proceedings, 80, 3554-3559.

[14] Panahı, U. (2022). Nesnelerin interneti için hafif siklet kriptoloji algoritmalarına dayalı güvenli haberleşme modeli tasarımı= Design of a lightweight cryptography-based secure communication model for the internet of things.

[15] Savaştürk, P., Aydın, Ö., & Dalkılıç, G. (2022). AES Encrypted Real-Time Video Stream and Image Transmission from ESP32-CAM. Celal Bayar University Journal of Science, 17(4), 447-452.