Next Generation Cloud-Based IoT Technology of Smart Home Systems

Sevcan Kahraman[*], İsmail Selçuk Çınar[**], Münir Türk[***]

[*] Asst. Prof. Dr., Istanbul Commerce University, Faculty of Engineering, Computer Engineering Department, Istanbul, TÜRKİYE. E-mail: skahraman@ticaret.edu.tr ORCID: 0000-0003-2173-7821

[**] Istanbul Gelişim University, Faculty of Engineering and Architecture, Electrical Electronics Engineering Department, Istanbul, TÜRKİYE. E-mail: 190409015@ogr.gelisim.edu.tr ORCID: 0000-0001-7951-1222

[***] Simya Software Development, Istanbul, TÜRKİYE. E-mail: m.trk485200@gmail.com ORCID: 0009-0003-1478-351X

[*]Corresponding Author; E-mail: skahraman@ticaret.edu.tr ORCID: 0000-0003-2173-7821

Received: 09.04.2025 Accepted: 05.01.2026

Abstract- Today, building control systems are becoming a common part of modern life to provide easier management of large-scale buildings and to make all systems work more efficiently. In building control systems, various systems such as control panels, PLC, KNX, and BACnet protocols are used for process control. Building automation includes the building's heating, ventilation, air conditioning (HVAC), electricity, lighting, security camera systems, doors inside the building, elevators, and many more processes involved in control systems. However, all these systems cannot be managed from a single platform. As the demand for advanced automation systems increases, existing control systems become insufficient. In order to construct an effective automation control system, all these devices must easily communicate, integrate, and exchange information with different subsystems. The centralization of device management and the interaction of these devices with various subsystems to form an Internet of Things (IoT) ecosystem lead to the emergence of multiple security vulnerabilities. Consequently, the IoT ecosystem becomes highly susceptible to external threats, particularly cyberattacks. In this context, the integration of additional security protocols into these systems is essential to ensure the protection and reliability of the ecosystem. In this study, the design of a cloud-based smart home automation system with adding a novel security protocol has been carried out based on MQTT protocol. A prototype has been developed to test the operability of the system, and this product has been integrated into the system for operability and analysis. The system also controls and monitors the home and its surroundings through a system that works on all platforms and a mobile app.

Keywords: Cloud, Internet of Things (IoT), MQTT Protocols, Security, Smart Home Automation, TLS.

Akıllı Ev Sistemlerinin Yeni Nesil Bulut Tabanlı IoT Teknolojisi

Öz- Günümüzde, büyük ölçekli binaların daha kolay yönetilmesini sağlamak ve tüm sistemlerin daha verimli çalışmasını sağlamak için bina kontrol sistemleri modern yaşamın yaygın bir parçası haline gelmektedir. Bina kontrol sistemlerinde, proses kontrolü için kontrol panelleri, PLC, KNX ve BACnet protokolleri gibi çeşitli sistemler kullanılmaktadır. Bina otomasyonu, binanın ısıtma, havalandırma, klima (HVAC), elektrik, aydınlatma, güvenlik kamera sistemleri, bina içindeki kapılar, asansörler ve kontrol sistemlerinde yer alan daha birçok prosesi içerir. Ancak, tüm bu sistemler tek bir platformdan yönetilemez. Gelişmiş otomasyon sistemlerine olan talep arttıkça, mevcut kontrol sistemleri yetersiz kalmaktadır. Etkili bir otomasyon kontrol sistemi inşa etmek için, tüm bu cihazların farklı alt sistemlerle kolayca iletişim kurması, entegre olması ve bilgi alışverişinde bulunması gerekir. Cihaz yönetiminin tek bir merkezde toplanması ve bu cihazların farklı alt sistemlerle etkileşim içerisinde bir Nesnelerin İnterneti (IoT) ekosistemi oluşturması, çeşitli güvenlik açıklarının ortaya çıkmasına neden olmaktadır. Bu durum, IoT ekosistemini dış tehditlere, özellikle siber saldırılara, karşı önemli ölçüde savunmasız hale getirmektedir. Bu bağlamda, söz konusu sistemlere ilave güvenlik protokollerinin entegre edilmesi ve ekosistemin güvenliğinin sağlanması zorunlu hâle gelmektedir. Bu çalışmada, MQTT protokolüne dayalı bulut tabanlı yeni bir güvenlik protokolü eklenmiş bir akıllı ev otomasyon sisteminin tasarımı gerçekleştirilmiştir. Sistemin çalışabilirliğini test etmek için bir prototip geliştirilmiş ve bu ürün çalışabilirlik ve analiz için sisteme entegre edilmiştir. Sistem ayrıca, tüm platformlarda çalışan bir sistem ve bir mobil uygulama aracılığıyla evi ve çevresini kontrol etmekte ve izlemektedir.

Anahtar Kelimeler: Bulut, Nesnelerin İnterneti (IoT), MQTT Protokolleri, Güvenlik, Akıllı Ev Otomasyonu, TLS.

1. Introduction

Recently, the Internet of Things (IoT) has become a rapidly growing concept in terms of the transformation from the physical world into computer-based systems. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration and management of devices. According to the statistics provided by Cisco, approximately 30 billion IoT devices will be in use around the world till 2030 [1]. Today, solutions developed with the IoT have found more and more application areas to make human life easier, such as smart home applications, smart cities, agriculture, industrial automation, healthcare, etc. IoT solutions, which include many different types of advanced technologies, will be very useful. The IoT technology can be used for new innovation concepts that can be widely used for developing and improving smart home systems in order to provide intelligence, comfort, safety and improved quality of life [2]. Therefore, IoT plays a critical role in generating a more interactive and intelligent lifestyle [3].

In recent years, urban lifestyle has become very popular. It is expected that thisupward urbanization trend will continue in the following years [4]. Due to the increasing population and increasing migration to cities, buildings are also developing day by day. While buildings are a basic need that ensures human life, they have turned into a highly sophisticated structure today. With the development of buildings, the development of automation systems has become inevitable to control the systems. Building automation consists of many sub-systems such as electromechanical and electrical systems, heating, ventilation, air conditioning, electricity and lighting, security and camera systems, doors inside the building and etc. Since an autonomous smart home is equipped with embedded devices that are designed to detect and respond to a person’s presence, it requires certain instruments such as light detection devices, fingerprint readers, gas detection systems, smoke sensors, temperature monitoring devices, motion detection systems, home surveillance cameras, etc. These devices are interconnected for a variety of reasons, including energy conservation, cost savings and user protection [5].

Therefore, it is very important that these systems work in harmony with each otherin terms of ensuring the integrity of the system and the comfort of the household [6]. However, as diversity increases, integration of existing automation devices into the system decreases and it becomes impossible to manage from a single platform. Users want to be able to use interface devices such as a remote control, computer, or smartphone to manipulate different sensors and devices connected with these systems [7]. In order to meet the requirements of each user, building automation systems have adopted the IoT methods, which are more innovative technologies compared to existing systems [8]. IoT is defined as a comprehensive network that has the capacity to auto-organize, share data and sources of information, react, act and make changes in the environment [9]. IoT is a cutting-edge technology that changes the way we live. In recent years, there have been many advances in IoT technologies which provide a very powerful tool in home automation to perform different tasks. The latest development in IoT technology comes with an opportunity to gain popularity in Building Automation and Control Systems (BACS) to automate buildings’ operations such as climate control, lightning and access control [10]. In addition, it presents a network architecture that automates smart homes to cloud services. It is considered as a viable alternative to the conventional home environment [1]. To illustrate, smart homes use IoT systems. Technology and innovation trends have encouraged people to adapt to a comfortable lifestyle carried out by smart home devices. Smart home technology can monitor temperature, detect smoke, regulate lighting automatically, and install smart locks. The term "smart home" refers to a variety of elements, technologies and tools that might produce useful data for forecasting environmental and domestic activities. There are various design issues of smart home systems. Such as serviceability, scalability, programmability, auto-configuration, heterogeneity, neutrality or transparency principle, security, robustness, energy efficient protocols, etc. [11]. Additionally, there are numerous frameworks available on the market for creating IoT - based apps such as creating standards for interoperability, making systems highly scalable, facilitating secure API’s and management API’s, abstracting hardware and software complexities, integrating various technologies, communication protocols & applications, device management, supporting multiple platforms and boards, ease of use, user-friendly interface, etc [11]. However, smart home security concern is a difficult task. It also poses additional security and privacy risks, such as accessing user data through surveillance equipment or false fire alarms [5]. Since smart homes entail unprecedented security vulnerabilities, there are lots of studies that address these security problems [5]. Although smart home devices are convenient to use and relate several advantages for security and safety concerns, they are prone to Cybersecurity risks [12], [13].

Many standard IoT platforms are proposed to connect and communicate with IoT devices easily and securely such as oneM2M, Google Weave and Apple Home Kit [14]. In this study, instead of making separate applications for different systems, a main system has been developed that gathers all these as systems. This system can easily transfer data and integrate with all other systems.

The design and development of a smart home automation system produces remarkably effective performance when the concept of machine learning is combined with IoT technologies. Many successful studies on IoT have been carried out using machine learning algorithms [15],[16],[17],[14],[18],[19]. The cloud stands out with its important advantages, such as low cost, scalability, easy management and subsystem control and easy access. Using cloud-based solutions in the IoT automation system plays an important role in increasing the potential of this technology and achieving better results. Because IoT automation collects huge amounts of data, this data needs to be analyzed and processed. The cloud provides the necessary infrastructure to process and store large amounts of data. Data stored in the cloud becomes accessible from any device anywhere. Cloud technology supports and facilitates easy transfer, management and analysis of data across various platforms. In this way, IoT systems can work more efficiently and effectively. In addition, Cloud-based IoT automation provides a great advantage in terms of scalability. Cloud-based IoT technology also offers remote access and management. Users can access and manage IoT systems from any device as long as they have a working internet. Cloud system service providers remotely accesses to simplify maintenance and troubleshooting processes [20].

Enhancing surroundings control, energy management, home security, and other areas of smart home automation systems has been the focus of several research studies and published literature. IoT-supported home automation systems have grown in popularity over the past few years, which has improved smart homes' energy management systems. Due to the multidisciplinary nature of IoT, much of academic research covering a wide range of topics, including security, technology, architectural design, and energy efficiency, has been conducted on this topic [21].

Home automation systems have included a variety of technology over the past 20 years; each one has pros and cons. For instance, a Bluetooth-based home automation system [22] is affordable, quick, and easy to install, and yet it can only communicate over short distances. Wireless long-distance communication methods, however, include GSM (Global System for Mobile communication) and ZigBee. For battery-powered devices used in wireless control and monitoring applications, Zigbee [23][24][25] is a wireless mesh network standard. It is designed to have a low cost and low power consumption. However, it has slow data transmission speeds and low network stability. It has been observed that Zigbee and similar protocols have vulnerabilities that negatively affect system security. In the later stages of the article, the problem is explained with examples.

Message Queue Telemetry Transport (MQTT) is one of the most popular protocols that implement IoT communications. MQTT is a publisher and subscriber messaging system that contains a message topic and message content. The topic is a unique string that serves as the identifier for a type of message. A publisher is any client that sends messages, and a subscriber is any client that listens for incoming messages of a particular topic. The term client or node determines to any system/device that connects to a broker and publishes and/or subscribes to topics while the broker relays the messages between clients [26]. There are several studies about smart home IoT technologies using MQTT Protocol based on Cloud services in literature [27][28][29][30][31][32]. Our research aimed at studying the system design cloud-based intelligent home automation system has been carried out based on MQTT protocol. Section 3 elaborates on the details of the suggested method.

The proposed architecture remotely controls and manage a smart home environment that was previously impossible or highly impractical to establish system integrity with subsystems. The service area of the product has been expanded by ensuring that the developed prototype product, hardware and software work in harmony with other automation control systems. With this architecture, it will be extended to more reliable applications for safe and secure building automation and control system. The proposed framework is reproducible, portable, and affordable. Objectives of this work are as follows:

1. To develop a system design of the IoT technology, which is larger than the typical process monitoring, and management systems used in building automation systems, continuously monitoring and analyzing the condition of devices.
2. To construct a sensor-based automation system that also gathers all process data in one center and enables devices to communicate with one another.
3. To ensure the secure centralized management of data by implementing layer of advanced security protocols that protect the IoT ecosystem against external cyber threats.
4. To implement the latest version of IoT-based commercial smart home applications.
5. To develop a mobile application for the remote control of basic electrical appliances, monitoring and displaying environmental factors in the home and its surroundings.

The rest of this paper is structured as follows: Section 2 describes related works, including Cloud Based IoT Technology of Smart Home Systems. Section 3 addresses the proposed IoT-based framework. System reliability models, database and data structure are explained in Section 4. In section 5, mobile applications for proposed architecture is introduced. Finally, Section 6 concludes the paper.

2. Proposed Cloud-Based IoT System

Smart homes provides comfortable lifestyle in modern life. The term "smart home" refers to a variety of elements, technologies, and gadgets that produce useful data for forecasting activities in the home and environment. Recently, substantial attention has been received to state-of-the-art systems (e.g. industrial control and automation systems). Automation system describes a wide range of technologies that can reduce human intervention in the processes involved. IoT supported home automation system has gained its popularity in a couple of decades. Many proposed IoT platforms allow developers and producers to come up with innovative products and intelligent services to improve human life by leveraging cutting-edge technologies. In this section, it has been addressed the proposed architecture based on the MQTT protocol and Cloud- based IoT system and has been discussed the details of components of the architecture.

2.1. System Design

Concise and informative IoT-based home automation systems have been proposed by a number of researchers over the past two decades [33-38]. In home automation systems, Process Control Systems (PCS) periodically monitor the data coming from the devices. After a certain period of time, automation devices, whose diversity has increased over time, cannot be integrated into existing process control systems. This has led to a new system design.

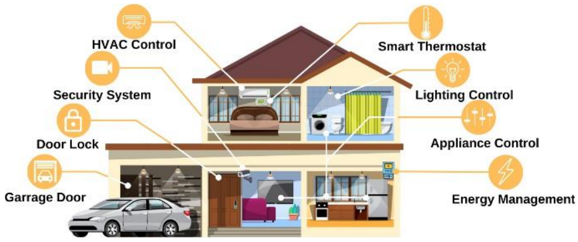

Fig. 1: Designed Automation System

Therefore, gateway, router and cloud systems are used to store and transfer the big data collected from the existing PCS. For example, building automation systems collect data in air-conditioning systems, lighting condition, ventilation, heating and cooling, pressure and temperature, etc. In addition to this data, it collects data about the condition of the machines in the building. Previously, this data was collected manually. With the rapid development of internet and computer systems since the 1990s, it has become possible to remotely control and access the system [39]. As an IoT-based architecture, proposed system aims at auto-monitoring and control, cross-platform, communication protocol, object access control, user interface, auto-configuration, device management, data analysis and visualization.

In this study, a system is designed to communicate, integrate and exchange information with different subsystems. Proposed framework enables efficient remote controlling for several application areas. It has been shown the designed prototype automation system in Figure 1. This system tried to show what a home user can do with the automation system and examples of use in smart home systems. For example, proposed smart home system provides lots of opportunities as detailed below.

- The user can remotely open and close the garage door and automate it.
- Therefore, the management of the door control is made easily.
- In order to ensure the security of the house, the user can lock, open and close the exterior or interior doors of the house, In addition, since the locking and non-locking situations will be reported to the user, the user will be able to enquire "Have I locked the house?" in order not to face such suspicious situations.
- The user can integrate the cameras in or around his house into the system to ensure home security. In this way, the owner could monitor the house remotely and increase security. The mentioned system could be developed, particularly in case of an unexpected situation, such as a movement that may occur in the house, theft, etc. The automation system can detect such movements and give feedback to the user, lock all the doors of the house and call the police.
- All of the home's HVAC (heating, ventilation, and air conditioning) systems can be controlled by the user.
- The user can be able to monitor the sensor measurements in the house. In addition, using this sensor data information, the management of devices in the building can be automated. For example, assume that 45 degrees temperature data is read from the thermostat. When the system sees the temperature of 45 degrees, the automation system will automatically operate the air conditioning system and set the temperature to a certain degree.
- The user can be able to manage the lighting systems in the house. For example, the lighting can be activated automatically in the evening hours, it can activate the lighting in the rooms where the user is constantly active to save energy, or it can turn off the lighting when the user is not in the room.
- The user can be able to manage the devices in the house (TV, washing machine, television, refrigerator, etc.). Thus, control of devices can be automated.
- The user can also carry out energy management. It is also possible to observe the amount of energy used in the building as well as which devices consume how much energy. The user can remotely cut and turn on the electricity of the building. In addition, this system can be made smart. For example, a device that consumes too much power can be detected and the user can be informed about this situation, Idle devices can be turned off to minimize energy consumption when the user is not at home, etc.

2.2. MQTT vs Zigbee, BACnet and KNX

State-of-the-art trends in technology and innovation have encouraged people to change their lifestyles to one that is comfortable in homes. Therefore, new and secure goods can be created using cutting-edge smart home system techniques and protocols. In this section, first of all Zigbee, BACnet and KNX protocols are briefly introduced with their advantages and disadvantages. And then MQTT protocol is explained in detail with its superior features. In this study, MQTT protocol is utilized to increase the security for effective communication of many devices. TLS is also used for secure communication with Cloud. Furthermore, cloud security concern is also mentioned shortly with the introduction of Transport Layer Security (TLS) in this section.

2.2.1. Zigbee Protocol

Smart home systems are intensively used in the management of HVAC control systems, lighting and security systems. The goal is to create products that are highly dependable, affordable, energy efficient, and ideal for setting up networks for management and monitoring for smart home automation systems (Graveto et al., 2022). Several automation products sold in the current market consist of the Zigbee protocol. The purpose of the Zigbee protocol is to transfer low-dimensional data to short and close distances with low power consumption [40]. However, there are some security vulnerabilities in this protocol, such as the Touch link Commissioning method. With this method, especially in home systems, users are able to make an easy installation by just connecting the node. An experimental environment has been established to detect the vulnerability of the Zigbee protocol [41].

2.2.2. BACnet and KNX

With the spread of Ethernet and IP communication, Building Automation and Control network (BACnet) protocol emerged and started to be used. Building automation systems, which include communication networks and control systems, are covered by the worldwide standard and communication protocol known as BACnet [42]. BACnet is a protocol that enables compatible devices or systems to be gathered together to manage them using a single platform. These devices include all devices compatible with BACnet are basically Analog Inputs, Analog Outputs, Binary Inputs, Binary Outputs and Timer etc. systems [43]. BACnet enables these devices to communicate with each other, apart from building automation and integration of devices inside the building. In addition to the BACnet protocol, another protocol used in building automation is the KNX protocol. Both of them are utilized in industry standards. Although the idea behind the procedure of BACnet and KNX protocol is the same, there is only one difference between them. BACnet has been specially designed to fulfill all the requirements of building automation systems. As the demand for advanced automation systems and the variety of devices increases, these devices cannot be easily configured to the BACnet protocol. The KNX protocol solves this problem and gathers together decentralized devices. In this way, devices can communicate with each other and can be managed from a central point. However, it has been observed that these systems also have security weaknesses. If an example of weakness is given [44];St. Regis Shen Zhen Hotel, located on the top floors of a 100-story skyscraper, provides its guests with the convenience of using an iPad to control variousroom facilities such as music, blinds, lights, TV, temperature, and do-not-disturb settings. However, the hotel's BACS system had vulnerabilities that allowed the creation of a remote-control device capable of accessing all hotel rooms, even from a different country.The Building Automation and Control System (BACS) employed devices with the KNX standard, and the KNX twisted pair network was connected to the local WiFi network to communicate with the iPad app via a KNX/IP router. The attacker established a connection with the target IP and maintained it to send various KNX commands to the network. These addresses corresponded to other devices connected to the KNX network, beyond those in the guest rooms. Therefore, KNX protocol also has security vulnerabilities.

2.2.3. Message Queuing Telemetry Transport (MQTT)

MQTT is a machine-to-machine IoT communication protocol, allows clients and servers to communicate with one another and share data. This protocol, whose working logic is very simple and fast, works with subscribe and publish methods that is incredibly lightweight. MQTT is a communication protocol designed for fast and reliable messaging between devices over the internet. This protocol is a very effective communication protocol for IoT devices with limited network resources such as low bandwidth and high latency. The MQTT protocol supports communication with a large number of IoT devices. Therefore, with the MQTT protocol, all devices can be easily managed, no matter how many devices are in the system [45]. The MQTT protocol is designed on publish and subscribe models. In our model, an MQTT broker publishes messages and devices receive these messages as subscribe.

When a device communicates a message about a specific topic to the MQTTbroker, this process is called MQTT publish. This process is used for devices to send data to other devices or MQTT broker. For example, a temperature sensor can publish its temperature data under the "sensors/temperature" topic to publish it to the MQTT broker. An MQTT subscribe operation is described as when a device subscribes to an MQTT broker to listen to messages about a particular topic. With the subscription process, devices can receive messages published on a particular subject. For example, any device in the system can subscribe to listening to the temperaturedata under the "sensors/ temperature" topic. In this way, when the temperature sensor device sends data by publishing, the other device automatically receives this data by subscription. Security is a crucial concern in the system for example. So, it is necessary to authenticate the identity of the device by sending data to enhance the security of the MQTT protocol. This ensures that the data sender is trustworthy and thus makes the protocol more secure.

2.2.4. Cloud Security

Since IoT automation is used in many areas, ranging from industrial activities to homes, security should be kept in the foreground. Cloud-based solutions, offer security measures and services related to data protection [46]. Data is transmitted by using various protocols, such as secure connections TLS and encryption methods. When relevant data is stored in the cloud, it is protected in a more secure environment compared to physical devices. In addition, cloud service providers implement security measures such as continuous updates and backups and protect users against malicious attacks. However, the user should consider every possibility and design a system to take security measures just in case.

2.2.5. Transport Layer Security (TLS)

TLS is a security protocol used to secure communications on a network connection. TLS is mainly used for communication on the Internet and is supported by HTTPS, SMTPS, FTPS, IMAPS, POP3S and many other protocols. TLS uses encryption and authentication mechanisms. These mechanisms include using digital certificates (POLICY) and authentication protocols. Additionally, devices exchange data by connecting to the internet in IoT, and therefore TLS is generally used for secure communication. TLS is also used to authenticate the identity of devices for exchanging data. In this way, TLS helps preventing unauthorized access to IoT devices. IoT devices also get updates from time to time.

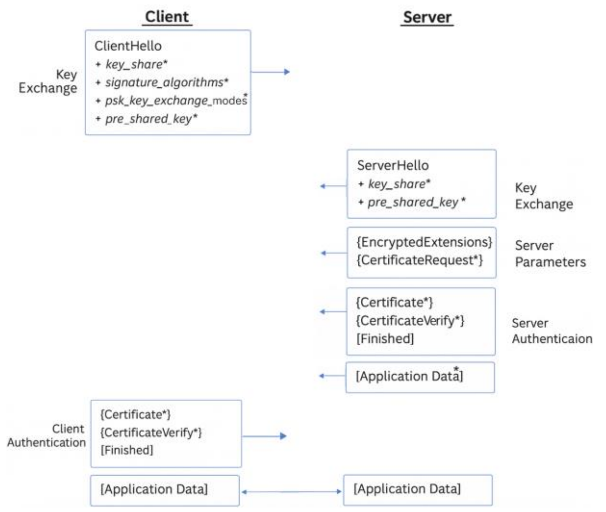

Fig. 2: TLS 1.3. Handshake Process [47].

It is important to transfer data securely during these updates as well. TLS also provides a secure data transfer during these updates. For these reasons, TLS is highly valuable for IoT devices. There are two main types of TLS: TLS 1.2 and TLS 1.3. Both are used to provide security on network connections, but TLS 1.3 has some advantages over TLS 1.2. First of all, TLS 1.2 is used especially for communications on websites and uses various security mechanisms such as encryption keys, digital certificates (POLICY) and authentication protocols. However, TLS 1.3 is a newer version and is considered as a faster, safer and more flexible protocol. TLS 1.3 is specifically designed to suit specific needs for use in devices requiring low power consumption such as mobile devices and IoT devices. The benefits of TLS 1.3 include faster connection time, better encryption strength, less latency and less CPU load. Figure 2. shows TLS 1.3. Handshake process [47].

3. Algorithm Working Logic

Thanks to the development of cutting-edge technology, IoT has attracted a lot of interest in these days. In this study, an intelligent home automation system is proposed based on IoT technologies and cloud computing. Proposed architecture includes a number of different parts, including auto-configuration and device management, auto - monitoring and control, cross-platform communication protocol, object access control, user interface, data analysis, and visualization. Figure 3. illustrates how the proposed system works. It basically shows the system algorithm that consists of user and cloud.

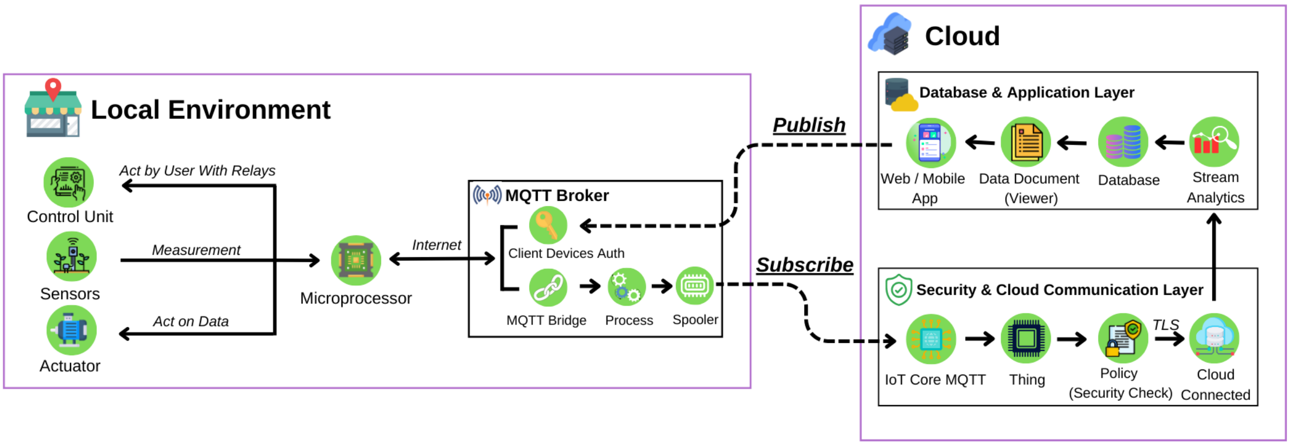

Fig. 3: Proposed System Architecture

3.1. Local Environment

The area called Local Environment refers to the place where the automation device is located, such as home. Automation devices have 3 tasks; taking measurements from sensors, activating/deactivating the devices connected to the control unit and controlling the moving elements in the house by using actuator, etc. This control unit has relays. These relays can turn on/off the device they are connected to. The sensors are receiving/listening to the data. Actuators are also a name given to motors that can be moved electrically, such as the opening and closing of a curtain or a garage door.

A microprocessor is used in the automation board for the realization of these 3 tasks. These are all connected to the microprocessor. As shown in Figure 3 with the bidirectional arrow, these devices can be switched on and off according to the user's preference. So that, it can be shown an interactive system. The microprocessor that receives the data and transfers the relevant data to the cloud. However, even if the microprocessor is connected to the internet, it is not possible to transfer data directly to the cloud. Thus, MQTT broker should be used for interactive data transfer between the cloud and the microprocessor. Likewise, it is necessary to connect to the cloud with MQTT to build efficient communication in the system. Safety is the most important parameter to this system. In this study, it is aimed to always keep safety in the foreground. MQTT brokers provide management of topics, subscriptions and clients. A broker allows clients to connect, create topics, manage subscriptions and even filter messages in some cases. MQTT brokers also provide a number of security features to ensure messaging security. These features include encryption, authentication, access control, and message logging. Encryption of MQTT traffic provides protection against third-party attacks. TLS/SSL is one of the most widely used methods for encryption of MQTT traffic.

Incoming data will come to MQTT broker. Thereby, it will be able to provide communication with the cloud. MQTT broker contains four items [48]:

1. Verifying the data coming from the devices: Under the name of verifying the data coming from the devices, for example, when we give one data from the phone, it tests whether this data comes from a correct user or not. If true, processing continues. In this way, a security measure is actually taken at the first stage.
2. MQTT bridge: It is a software component that enables communication and message exchange between two MQTT brokers. It can be considered as a phase prior to browsing the internet by establishing a bridge communication with the incoming data.
3. Processing the data: Then the data is processed. It temporarily stores all the data that comes later.
4. Sharing the data: Finally, the data is shared with the cloud. This operation is called “Publish”.

3.2. Cloud

In cloud environments, data management and storage operate utilizing the MQTT protocol. Devices, referred to as "Things," encapsulate their configuration details in JSON format to support authentication. TLS security protocols are employed to guarantee safe communications, leveraging certificates and keys for robust encryption. Users can manage and control devices such as lights and appliances remotely through mobile or web applications, transmitting commands via the MQTT protocol.

3.2.1. Security and Cloud Communication Layer

In this layer, the "Client Auth ID" stage, which shows the ID of the device in the MQTT Broker stage, has been added. MQTT Broker carries the data through the bridges, processes it, and after storing it temporarily, it shares the data through the cloud by performing “SUBSCRIBE” process. When data comes to the cloud via MQTT Broker, it first passes over MQTT in the cloud. There must be an MQTT in the cloud for detecting the data we send. The MQTT protocol will communicate only with systems (devices) that have to possess the MQTT protocol.

MQTT in the cloud read the incoming data. It then puts it into a Thing. Things are like a work environment. It is a structure that represents any device. It was created as a JSON document describing the device's properties, configurations, and other information. This document is used to verify the identity and authorization of devices. After MQTT reads the incoming data in the cloud, Thing is opened. Desired definitions can be made in Thing, making communication more effective. All owned devices are introduced in a virtual environment. The relevant data is transferred to the "thing" in the cloud.

Things are used to send data to the cloud. The cloud processes the related data. During this process, a "policy" is used to establish a secure connection with certificate and key files [49]. These files include certificate, public key and private key. Through these key files, the cloud authenticates the user and establishes a secure connection with the TLS protocol. Policy gives three files to keep communication with the cloud secure. It gives keys, certificates and a special file like certificate-related key. This file is introduced to the system. These key files are used to verify the identity of the right person, which allows the cloud server to authenticate the user and establish a secure connection. Once security is ensured, the cloud server generates a connection that cannot be accessed without permission. This link can be accessed through these three files. After verification, a connection to the cloud is provided. However, when it is typed directly, it cannot be accessed. This policy is required to access it, which is already identified in the link. This process is also called TLS. In this way, the connection is established, and it is accessed to the cloud.

TLS layer security is crucial on the Internet of Things. The server requests the client for certificates so that communication between the two parties is secure. This means that before TLS establishes a connection to the server, it has carried out a data exchange with the server, verified, ensured the layer security and opened a database. It does not open in any other way. Then communication is provided with the cloud. This part is named security and cloud communication. Then the data is processed. JavaScript Object Notation (JSON) is a lightweight data interchange format used to move and exchange data. Although JSON was originally designed for the JavaScript language, it is now supported by many programming languages [50]. It is frequently used when exchanging data between different platforms and applications. The MQTT protocol, on the other hand, is not designed to connect directly to a database. This is because there are language and code incompatibilities here. JSON format is used for communication between MQTT and Database. That is, MQTT messages are encoded as JSON and data can be retrieved decoding JSON while being saved in a database. In this way, the code incompatibility between the database and MQTT is corrected through JSON. Both protocols are bridged to each other [51].

3.2.2. Database and Application Layer

This layer is also very important. As it is depicted in Figure 3, all of these processes are in the cloud. At this stage, the data is analyzed and transferred to the database. The data stored in the database is documented and presented in a file format to be viewed.

There is a mobile/web application to manage the system. The relevant data is transferred to the mobile/web application. Thus, the user has the opportunity to view the data. In addition, if the user wants to manage the Local Environment (for example Home) remotely with the mobile/web application, user can manage the systems on the Local Environments by transmitting this request to the MQTT Broker through the "PUBLISH" process. Thanks to the MQTT protocol, interactive and secure communication is provided.

Firstly, the data is streamed to the database at the other side. The data is collected in the database, and they are ready to use. The gathered data in the database needs to be viewed and analyzed later on, for which an additional layer has been created. For example, documentation can be created at this point. In this documentation and display process, it is assigned a mobile application via an API. In the mobile application, the user can see what the incoming data is. The user is able to see the data from the application. For instance, the user wants to manage a home device manually with the app.

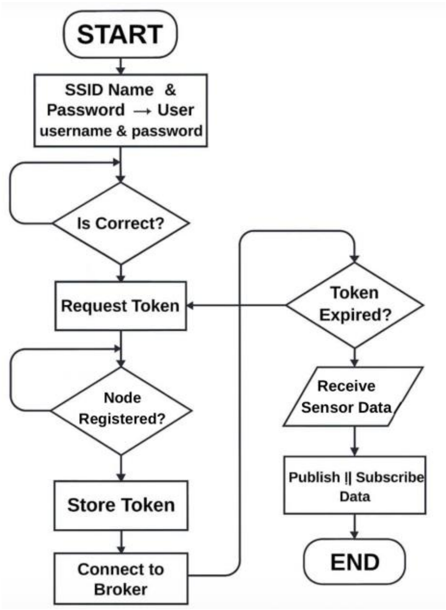

Fig. 4: Flow Chart of Proposed System

When it is given a command to do so, this command goes to the cloud. The MQTT process comes into play to access the home through the cloud. This situation is also called “subscribe”. The term "subscribe" refers to user-driven MQTT communication. The user sends the data to subscribe. This data is subsequently transferred to MQTT broker, and the user is checked to see if the correct data has actually arrived. If the data is correct and security measures have been taken, data comes to the microprocessor. From there, it goes to relays, actuators, etc. Thus, the user can manage relays, actuators, etc. This is how the system structure functions.There is such an algorithm. It is available in our web application. There are several companies that broadcasts free cloud and have a mobile application. These companies allow us to make our own codes, upload certificates to the application, providing communication between related devices. In this study, one of these platforms has been specifically chosen since it is convenient. Normally, this process can be achieved by opening an SQL server, renting a server and writing a mobile application. But we use ready-made templates (platforms) of an operating company (such as Amazon, Microsoft...etc.) to speed up the process. This study, therefore, has aimed to improve a platform, through which we can speed up the process.

In our proposed architecture, the user can be able to manage lots of tasks. Take a garage, for example, the user can open/close the garage. It allows us to control it remotely. In other words, it can be simplified as open/close/lock the doors of the house for security purposes. Furthermore, it can monitor the house remotely through internet-connected cameras located inside the house. Once it detects a movement from the camera, itcan notify the user that there is movement in the house at the moment. Various image processing applications can be developed here. The user may want to remotely turn on the air conditioners/air conditioning system (HVAC) inside the house. The user might command “turn on the heater and open the natural gas.

Thermostats’ sensors are devices that measure the temperature and humidity of the house. These are the systems that measure the incoming data and then send this data to our device to manage it. For example, the thermostat has reached 45 degrees, it may warn “run the air conditioning system”. This kind of work can be achieved in home automation. That's why it is written on smart thermostat here. Lighting systems can certainly be automated and controlled remotely on/off/managing the normal lighting in the house. Then, a technical infrastructure can be built to manage and control the home appliances such as washing machines, dishwasher, refrigerator, etc. As for energy management, there are electronic counters at the entrances of the buildings that display the electricity bill. For example, the user can read that device and may want to see the electricity bill. The user may also want to see the current drawn, how much energy is spent, etc. More can be achieved for management purposes. Further studies can also be carried out to this end. For example, the user could have a solar panel installed on the roof. Also, user wants to manage/read data from solar panel. This type of management can be realized. This is open to development.

New technology allows us to instantly monitor how much kW has been spent, how much Volts is spent on a regular basis, what is the instantaneous energy consumption. But all of this can be done by the company. But here, the user should be able to monitor the energy consumption statistically no matter where they are. It is called a communication counter which has two cables. In our proposed architecture, it can be connected one to the ESP. It can be done under the name of monitoring.

As it can be seen flowchart in Figure 4, firstly, it is necessary to transfer our incoming data to the internet world. There are some steps to be followed to gain access to this network. The data must be firstly connected to the correct WiFi address with the correct password by the device. Then, the device must log in to the portal gateway with a unique username and password in order to connect to the portal in the common network in use. If any of this information is wrong, the process returns to the begining and asks for WiFi information or portal information again.

If it has passed these stages successfully, it comes to the Request Token section. In other words, this indicates that it is ready to notify an MQTT client that a request has been completed, and a response can be received. If this request is registered in MQTT, the data can continue on its way. Or if the request times out, the loop should make the request again. The procedures function properly, especially if the Tokens communicate and know each other. All their data will be transferred to the cloud system. It is then published as Publish or Subscribe upon request of the user.

4. System Reliability Model, Database and Data Structure

The system achieves high reliability by ensuring secure data processing, storage, and continuous monitoring. Anomalies are identified through machine learning, and TLS/SSL protocols secure data transmissions. The authorization process encompasses cloud validation and user authentication. Error logging further enhances transparency and system integrity.

4.1. End-to-End Architecture

Proposed end-to-end model consists of admin control and security parts. It can be easily seen in Figure 5. After the sensors are connected to the device, the incoming data is organized. Then, these edited data are both saved in a database and transmitted to a display panel.

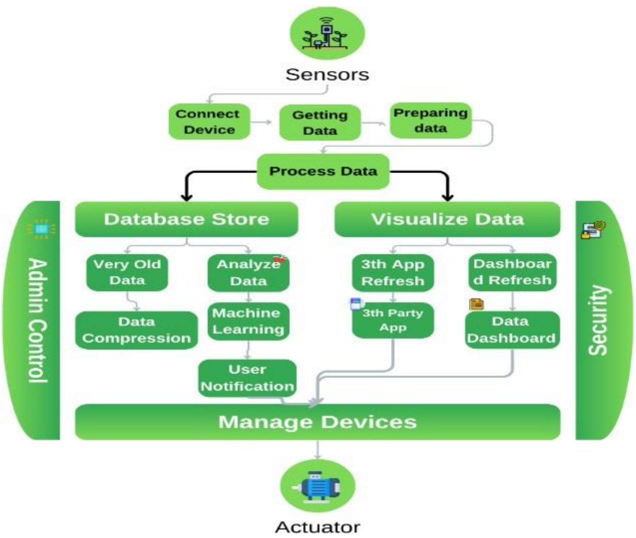

Fig. 5: System Architecture

the relevant data can be easily monitored. The data transmitted to the display panel is also updated and made available to users by third-party applications. In this process, the security level is increased by taking measures such as TLS/SSL for the security of data. In addition, the admin panel is also updated to monitor and manage the data obtained during the process [52].

4.2. Authorization

As illustrated in Figure 6., the established system consists of three items named cloud, user and controlled place. It is a very important issue regarding how the established system receives a reaction in every movement, every command given and how it will transmit this reaction, and most importantly, how it will provide security during this transmission. Therefore, the following algorithm was preferred when establishing this system;

Transmitter (user) takes detailed data of the device uses it and saves this data to the database. This data includes the status of the device, the name of the device, its address and the IMEI address. If it is a phone, the user logged in and the encrypted password, the name of the thing in the cloud, the date-time of the transaction and the sent command. There are additional characters to bring a security measure.

Client Device Auth (MQTT Broker): is the unit that contains the data of the device in the managed system (eg. home) and provides communication. This unit contains the address of the

Fig. 6: System Authorization Framework

The data recorded in the database is compared with the previous data. After the comparison is completed, the old data is compressed. New incoming data is analyzed and negative situations are quickly reported by sending instant notifications to the user with machine learning methods. The monitoring of all these processes is carried out through the admin panel and

device containing MQTT, its name, the name of the thing in the cloud, the status of the device and whether there is a request. If all these requests are pertinent, it identifies the device requesting the data and validates the data from that device.

Transmitter verifies whether all data from the transmitter match or not. If all data is accurate, it returns a data indicating that it has achieved the security validation.

-It confirms the date and time that this data came from, makes the device perform the command sent (for example, actuation), records the information that it has done, saves the date-time data of the operation and transmits them to the cloud in a database form.

-Cloud: Cloud saves all verification and command transfer processes on Transmitter and Client Device Auth. to the cloud database. If all of these operations are in place, the device that performs the operation records the date-time, and identities information of the device, the command sent, the operation performed and the result of the operation. In case of a possible conflict or no transmission, it classifies it as “Error" in the database. For example, a data type named “VAR” is added next to the command sent by the device. Putting an attachment like this instead of just sending a command increases reliability.

If this additional data type is not seen, the system will not perform the operation. It will save the detailed data of the device that sent this operation, identify where the error is and save this error to the database.

Existing IoT-based smart home and building automation systems primarily rely on protocol-level security mechanisms or isolated authentication techniques, which often fail to provide holistic protection across heterogeneous devices, cloud platforms, and user interfaces. Traditional approaches such as Zigbee, BACnet, and KNX mainly focus on functional interoperability, while security is either optional, static, or limited to network-level protection. These methods typically lack fine-grained authorization, continuous verification, centralized identity management and detailed traceability, making them vulnerable to unauthorized access, replay attacks, device spoofing, and malicious command injection. The proposed methodology addresses these limitations by introducing a multi-layered security architecture integrated into the end-to-end system design, as illustrated in the validation and authorization layers presented in Section 4.1. Unlike conventional systems, security is not treated as an add-on component but as a core design principle spanning from the local device level to the cloud infrastructure. Device identity is enforced through Client Authentication IDs and certificate-based authentication, while access control is governed by cloud-defined policies that strictly regulate publish–subscribe permissions within the MQTT broker.

Furthermore, the proposed system introduces continuous verification mechanisms at both broker and cloud levels, where each command is validated using device identity, timestamp information, and policy compliance before execution. All operations are logged and stored in the cloud database, enabling full traceability, anomaly detection, and fault classification.

Table1. Comparison between proposed framework and state-of-the-arts

Feature	**ZigBee**	**BACnet / KNX**	**MQTT (Basic TLS)**	**Proposed Framework**
Communication Model	Mesh / Star	Client-Server	Publish-Subscribe	Publish-Subscribe
End-to-End Encryption	Partial / Optional	Limited	Yes	**Yes (TLS 1.3)**
Certificate-Based Authentification	No	No	Optional	Yes (Device Certificates)
Fine-Grained Access Control	No	Limitde	Limited	Policy-Based Authorization
Continious Verification	No	No	No	**Yes (Broker + Cloud)**
Device Identify Management	Static IDs	Network-Based	Client ID	**Client Auth ID + Thing Model**
Centralized Logging & Traceability	No	Limited	Partial	Yes
Cloud Integration	Limited	Limited	Yes	**Native & Secure**
Typical Latency	Low-Medium (Short Range)	Medium	Low	**Very Low (Reduced Handshake Latency)**
Communication Reliability	Medium (Mesh Retry)	Medium (Polling-Based)	High (Broker ACK)	**Very High (Broker + Cloud ACK)**
Packet Loss Tolerance	Low	Medium	High	High
Security Handshake Latency	Low	Low	Moderate	Low
Authentication Method	Network Key	Delice-Based ID	Username / Certificate	Certificate-Based + Client Auth ID

By combining MQTT with TLS 1.3, JSON-based data integrity checks, and Thing-based virtual device representation, the proposed framework overcomes the static and fragmented security models of existing solutions, offering a scalable, resilient, and security-centric IoT automation framework.

5. IoT Application

IoT devices are often complex and do not have a direct user interface. Mobile applications for IoT devices provide many advantages. Therefore, users can easily control their devices by using a mobile application.

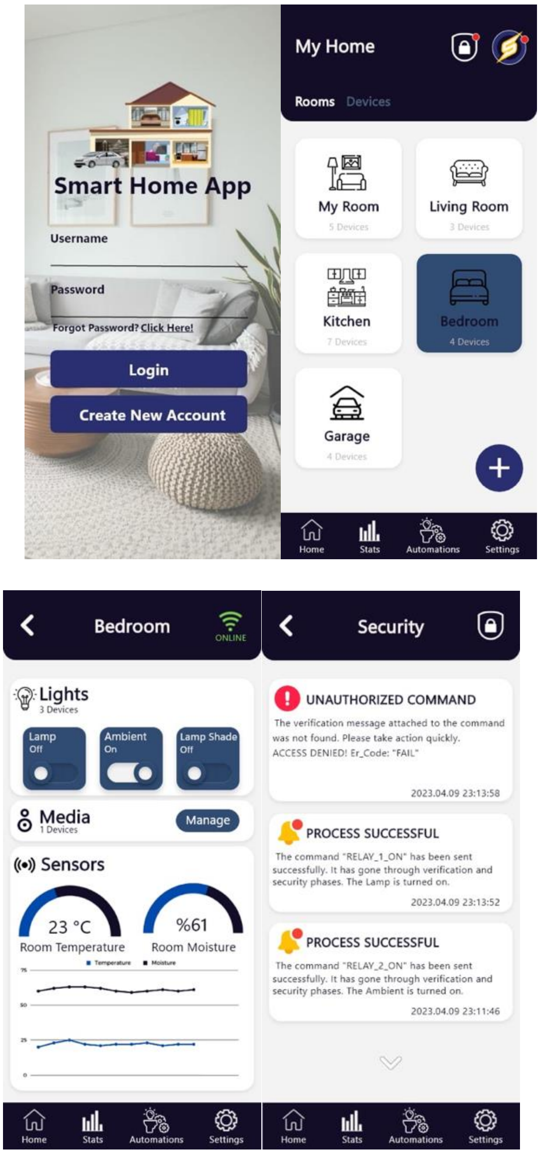

Fig. 7: System Mobile Application, (a) Login Page, (b) Home Page, (c) Bedroom Page, (d) Notification Page

In addition, when IoT devices need updating, they can be easily updated, analyzed and remotely controlled via the mobile application. Mobile apps also increase the security of IoT devices with better authentication and encryption processes and protect them from malicious use. Typically, users can access all platforms to control and maintain the security of these devices. This platform can use desktop or mobile applications. Figure 7. shows the user interface of proposed systems' mobile application. It consists of login page, home page, bedroom page and notification pages. Users can create an account in Login page. The home page provides some options for users such as living room, kitchen or garage, etc. When the user enters one of these alternatives, it can be seen as lights situation, sensor measurements, etc. Notification pages inform the user for processes such as thief entering the house, etc.

6. Conclusion

One of the key components of a home automation system is the Internet of Things. It makes life simpler and is beneficial for everyone. This study takes a stab at creating a home automation system based on the IoT. Because of their quick development, IoT networks are becoming more susceptible to cybersecurity attacks. In this study, it is introduced a designed prototype automation card system and used MQTT protocol by giving comparison with the other protocols. TLS security protocol is also explained. Furthermore, the components of smart home systems are designed to address various issues such as scalability, interoperability, device adaptability, security and privacy. Moreover, the proposed system application is user-friendly, adaptable, and beneficial for consumers and the disabled in particular. Through the use of numerous tools, it has the potential to be expanded still further. The major goals of this effort are to increase the security and intelligence of our home automation system. This study proposes a cloud-based IoT smart home automation architecture with a strong emphasis on end-to-end security and system integrity. Secure communication is achieved by integrating the MQTT protocol with TLS 1.3, providing encrypted data transmission, mutual authentication, and protection against man-in-the-middle and replay attacks. Device identity and access control are enforced through certificate-based authentication, Client Authentication IDs, and policy-defined permissions within the cloud environment, ensuring that only authorized nodes can publish or subscribe to MQTT topics. The use of Thing-based device representation, JSON-encoded messaging, and continuous verification at both broker and cloud layers enables fine-grained authorization, traceability, and fault detection. Consequently, the proposed architecture offers a resilient, secure, and scalable solution suitable for modern smart home systems and extensible to large-scale building automation infrastructures.

References

[1] D. Evans, "La próximaevolución de Internet loestácambiandotodo," Cisco Internet Business Solutions Group (IBSG), 2011.

[2] V. Jyothi, M. G. Krishna, B. Raveendranadh, and D. Rupalin, "IoT Based Smart Home System Technologies," International Journal of Engineering Research and Development, vol. 13, no. 2, pp. 31-7, 2017.

[3] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A Secure and Efficient Internet of Things Smart Home Architecture Based on Cloud Computing and Blockchain Technology," Int. J. Distrib. Sensor Networks, vol. 15, no. 4, p. 155014771984415, 2019, doi: 10.1177/1550147719844159.

[4] G. Lilis, G. Conus, N. Asadi ve M. Kayal, "Towards the next generation of intelligent building: An assessment study of current automation and future IoT based systems

with a proposal for transitional design," Sustainable Cities and Society, cilt. 28, pp. 473–481, 2017, doi: 10.1016/j.scs.2016.08.019.

[5] A. Aldahmani, B. Ouni, T. Lestable ve M. Debbah, "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, andTrends," IEEE Open Journal of VehicularTechnology, cilt 4, pp. 281-292, 2023, doi: 10.1109/OJVT.2023.3234069.

[6] S. Za, "Bina Otomasyon Sistemlerinde Entegrasyon ve BACnet," 2000.

[7] T. S. Gunawan, I. R. H. Yaldi, M. Kartiwi, N. Ismail, N. F. Za'bah, H. Mansor ve A. N. Nordin, "Prototype Design of Smart Home System Using Internet of Things," Indonesian Journal of Electrical Engineering and Computer Science, cilt. 7, sayı 1, pp. 107–115, 2017, doi:10.11591/ijeecs.v7.i1.pp107-115

[8] L. Atzori, A. Iera ve G. Morabito, "The Internet of Things: A survey," Computer Networks, cilt 54, sayı 15, pp. 2787-2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[9] S. Madakam, "Internet of Things: Smart Things," Int. J. Future Comput. Commun., vol. 4, no. 4, pp. 250–253, 2015, doi:10.7763/IJFCC.2015.V4.395.

[10] ISO, 2004. ISO 16484-2: 2004, Building Automation and Control Systems (BACS) - Part 2: Hardware, International Organization for Standardization, Swtizerland.

[11] M. Jerabandive M. M. Kodabagi, "Internet of Things Based Technology for Smart Home System: A Generic Framework," International Journal on Recent and Innovation Trends in Computing and Communication, cilt. 5, sayı. 6, pp. 1–5, 2017.

[12] B. D. Davis, J. C. Mason ve M. Anwar, "VulnerabilityStudiesand Security Postures of IoTDevices: A Smart Home Case Study," IEEE Internet of ThingsJournal, cilt 7, sayı 10, pp. 10102-10110, 2020, doi: 10.1109/JIOT.2020.2983983.

[13] T. Pattanasri, "Mandatory Data Breach Notification and Hacking the Smart Home: A Legal Response to Cybersecurity?" QUT Law Rev., vol. 18, no. 2, pp. 269–290, 2018.

[14] J. Koo, S.-R. Oh ve Y.-G. Kim, "Device Identification Interoperability in Heterogeneous IoT Platforms," Sensors, cilt. 19, sayı 6, s. 1433, 2019, doi: 10.3390/s19061433.

[15] O. Hamdy, H. Gaber, M. S. Abdalzaherve M. Elhadidy, "Identifying Exposure of Urban Area to Certain Seismic Hazard Using Machine Learning and GIS: A Case Study of Greater Cairo," Sustainability, cilt. 14, sayı 17, s. 10722, 2022, doi:10.3390/su141710722

[16] F. Hussain, R. Hussain, S. A. Hassan ve E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," IEEE Communications Surveys & Tutorials, cilt. 22, sayı. 3, pp. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.

[17] J. Jaihar, N. Lingayat, P. S. Vijaybhai, G. Venkatesh ve K. P. Upla, "Smart Home Automation Using Machine Learning Algorithms," 2020 International Conference for Emerging Technology (INCET), pp. 1–4, 2020, doi: 10.1109/INCET49848.2020.9154007.

[18] E. Likotiko, Y. Matsuda ve K. Yasumoto, "Garbage Content Estimation Using Internet of Things and Machine Learning," IEEE Access, cilt. 11, pp. 13000–13012, 2023, doi: 10.1109/ACCESS.2023.3242547.

[19] L. Salhi, T. Silverston, T. Yamazaki, and T. Miyoshi, "Early Detection System for Gas Leakage and Fire in Smart Home Using Machine Learning," in Proc. 2019 IEEE Int. Conf. Consum. Electron. (ICCE), pp. 1–6, 2019, doi: 10.1109/ICCE.2019.8661990.

[20] J. Kim, "Cloud Internet of Things for the Smart Environment of a Smart City," Yüksek LisansProjesi, Information and Decision Sciences Bölümü, California State University, San Bernardino, 2021.

[21] S. Iqbal, "AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems," SN Computer Science, vol. 3, pp. 1-12, 2022, doi: 10.1007/s42979-022-01043-x.

[22] I. Froiz-Míguez, T. M. Fernández-Caramés, P. Fraga-Lamas ve L. Castedo, "Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes," Sensors, cilt. 18, sayı 8, s. 2660, 2018, doi:10.3390/s18082660

[23] K. Gill, S.-H. Yang, F. Yao ve X. Lu, "A ZigBee-Based Home Automation System," IEEE Transactions on Consumer Electronics, cilt. 55, sayı 2, pp. 422–430, 2009, doi:10.1109/TCE.2009.5174403

[24] J. Han, H. Lee ve K.-R. Park, "Remote-controllable and energy-saving room architecture based on ZigBee communication," IEEE Transactions on Consumer Electronics, cilt. 55, sayı. 1, pp. 264–268, 2009, doi: 10.1109/TCE.2009.4814444.

[25] G. V. Vivek and M. P. Sunil, "Enabling IoT services using WIFI - ZigBee gateway for a home automation system," in Proc. 2015 IEEE Int. Conf. Res. Comput.

Intell. Commun. Networks (ICRCICN), pp. 77–80, 2015, doi:10.1109/ICRCICN.2015.7434213.

[26] OASIS, "MQTT Version 3.1.1," 2014.

[27] X. Chi, M. Zhu, J. Yang ve W. Wang, "An MQTT-basedScalable Remote Control Framework withNodeMCUand Cloud platform," 2020 5th International Conference on Mechanical, Control andComputerEngineering (ICMCCE), 2020, pp. 731-735, doi: 10.1109/ICMCCE51767.2020.00161.

[28] A. Khakimov, A. Muthanna, R. Kirichek, A. Koucheryavyve M. S. A. Muthanna, "Investigation of methods for remote control IoT-devices based on cloud platforms and different interaction protocols," 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 160–163, 2017, doi: 10.1109/EIConRus.2017.7910518.

[29] J. Kim, S.-C. Choi, J. Yun ve J.-W. Lee, "Towards the oneM2M standards for building IoT ecosystem: Analysis, implementation and lessons," Peer-to-Peer Networking and Applications, cilt. 11, sayı 1, pp. 139–151, 2018, doi: 10.1007/s12083-016-0505-9.

[30] M. V. S., R. A., Santhosh, R. A. H., K. D., V. M. P., and V. S., "Internet of Things Based Smart Energy Meter with Fault Detection Feature Using MQTT Protocol," in Proc. 2022 8th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), 2022, pp. 1592–1596, doi:10.1109/ICACCS54159.2022.9785026.

[31] B. Mishra and A. Kertesz, "The Use of MQTT in M2M and IoT Systems: A Survey," IEEE Access, vol. 8, pp. 201071–201086, 2020, doi:10.1109/ACCESS.2020.3035849.

[32] Y.-C. Tsao et al., "An Implementation and Design of a Digital Light Switch of Smart-Home Based on MQTT Broker," in Proc. 2021 IEEE 4th Int. Conf. Knowledge Innov. Invention (ICKII), pp. 92–96, 2021, doi: 10.1109/ICKII51822.2021.9574779.

[33] A. S. Abhishek, M. Bhasker ve A. S. Ponraj, "IoTBased Control Systemfor Home Automation," 2021 IEEE 2nd International Conference on Technology, Engineering, Management forSocietalImpact Using Marketing, EntrepreneurshipandTalent (TEMSMET), 2021, pp. 1-5, doi: 10.1109/TEMSMET53515.2021.9768686.

[34] S. Dash ve P. Choudekar, "Home Automationusing Smart DevicesandIoT," 2021 9th International Conference on Reliability, Infocom Technologies andOptimization (TrendsandFutureDirections) (ICRITO), pp. 1-5,2021, doi: 10.1109/ICRITO51393.2021.9596533.

[35] C. Ghosh, S. Chanda ve K. Sil, "IoT Based Smart Home Automation Using Solar Photovoltaic System and Online Time Server," 2021 5th International Conference on Green Energy and Applications (ICGEA), Singapur, pp. 114–118, 2021, doi:10.1109/ICGEA51694.2021.9487628

[36] M. Ibne Joha, Md. S. Islam ve S. Ahamed, "IoT-Based Smart Control and Protection System for Home Appliances," 2022 25th International Conference on Computer and Information Technology (ICCIT), pp. 294–299, 2022, doi: 10.1109/ICCIT57492.2022.10054941.

[37] A. K. Kaibortave S. Samal, "IoT based Voice Assistant for Home Automation," 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 165–172, 2022, doi: 10.1109/ICSSIT53264.2022.9716533.

[38] S. N. Tayus, A. K. M. Kamrul Alam Kakon, and M. Ullah, "IoT Based Web Controlled Multiple Home Automation and Monitoring with Raspberry Pi," in Proc. 2022 3rd Int. Conf. Emerging Technol. (INCET), pp. 1–4, 2022, doi: 10.1109/INCET54531.2022.9825087.

[39] V. Graveto, T. Cruz ve P. Simões, "Security of Building Automation and Control Systems: Survey and Future Research Directions," Computers & Security, cilt. 112, p. 102527, 2022, doi: 10.1016/j.cose.2021.102527

[40] "Zigbee in the Market," CSA IoT, 2025. [Online]. Available: https://csa-iot.org/all-solutions/zigbee/.

[41] H. Li, W. Zhang, W. Zhou ve B. Su, "A Novel Vulnerability Detection Method for ZigBee MAC Layer," 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing, pp. 121–124, 2014, doi: 10.1109/DASC.2014.30.

[42] W. S. Song and S. H. Hong, "A reference model of fire detection and monitoring system using BACnet," Building and Environment, vol. 42, no. 2, pp. 1000–1010, 2007, doi: 10.1016/j.buildenv.2005.10.028.

[43] S. T. Bushby, "BACnet™: A standardcommunicationinfrastructureforintelligentbuildings," Automation in Construction, cilt 6, sayı 5-6, pp. 529-540, 1997, doi: 10.1016/S0926-5805(97)00029-0.

[44] S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park ve R. Sandhu, "Attribute-Based Access Control for AWS Internet of ThingsandSecureIndustries of theFuture," IEEE Access, cilt 9, pp. 107200-107223, 2021, doi: 10.1109/ACCESS.2021.3101218.

[45] A. S. SuwardiAnsyah, M. Arifin, M. B. Alfan, M. V. Suriawan, N. H. Farhansyah, A. M. Shiddiqi, and H.

Studiawan, "MQTT Broker Performance Comparison between AWS, Microsoft Azure and Google Cloud Platform," in Proc. 2023 Int. Conf. Recent Trends Electron. Commun. (ICRTEC), pp. 1–6, 2023, doi: 10.1109/ICRTEC56977.2023.10111870.

[46] A. K. S. Sanger and R. Johari, "Survey of Security Issues in Cloud," in Proc. 2022 Int. Mobile Embedded Technol. Conf. (MECON), pp. 490–493., 2022, doi: 10.1109/MECON53876.2022.9751959.

[47] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," Aug. 18, 2018. [Online]. Available: https://tools.ietf.org/html/rfc8446#section-4.6.2.

[48] G. Wang, "The Study of IoT MQTT Publish Latency," in Proc. 2021 IEEE Int. Conf. Electro Inf. Technol. (EIT), pp. 27–31, 2021, doi:10.1109/EIT51626.2021.9491838.

[49] C. J. Fung ve B. McCormick, "An Effective Policy Sharing Mechanism for Smart Home Networks," 2020 16th International Conference on Network and Service Management (CNSM), İzmir, Türkiye, pp. 1–7, 2020, doi:10.23919/CNSM50824.2020.9269110

[50] A. A. Frozza, R. D. S. Mello ve F. D. S. D. Costa, "An Approach for Schema Extraction of JSON and Extended JSON Document Collections," 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, ABD, pp. 356–363, 2018, doi:10.1109/IRI.2018.00060

[51] S. Ahmed ve Q. Mahmood, "An authenticationbasedschemeforapplicationsusing JSON web token," 2019 22nd International Multitopic Conference (INMIC), pp. 1-6, 2019, doi: 10.1109/INMIC48123.2019.9022766.

[52] S. N. Swamy and S. R. Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)," IEEE Access, vol. 8, pp. 188082–188134, 2020, doi:10.1109/ACCESS.2020.3029847.