STM JOURNALS

International Journal of
Mobile Computing Technology

Volume 2, Issue 2, 2024
July—December
DOI (Journal): 10.37591/IJMCT

https://journals.stmjournals.com/ijmct

Research IJMCT

Efficient Message Captivating Environment in IoT Home Networks

Yatharth Agrawal*

Abstract

The Internet of Things (IoT) concept involves connecting and monitoring physical objects via the internet, generating significant interest among researchers and users due to widespread internet availability. This concept encompasses a broad spectrum of devices, including internet-connected "smart" versions of traditional appliances, novel gadgets designed for an Internet-enabled environment, and Internet-enabled sensors transforming various sectors such as manufacturing, healthcare, transportation, and living spaces. Home automation, an IoT application, has significantly simplified people's lives. The 21st century has fully embraced IoT in smart home automation, enhancing the ability to control and operate household appliances and devices remotely conveniently and comfortably. IoT-based home automation systems incorporate servers and sensors, with remote servers situated on the internet facilitating data management and processing without the need for personal computers. This study includes household systems like fire prevention systems, surveillance cameras, smart TVs, lighting systems, smart thermostats, air conditioners, doors, fans, and humidity and gas monitoring systems. Users can receive alerts through microcontrollers and sensors from any location. The implementation of IoT has streamlined the performance of home automation systems in residential, commercial, and workplace settings, delivering efficient and effective safety, security, and comfort. A home automation system utilizing VPN technology offers a more secure and robust voice-controlled system with the assistance of a microcontroller, enhancing the intelligence and usability of existing appliances. This system also includes home security functions like access control and alarm systems. When connected to the internet, household devices become key elements of the Internet of Things (IoT) ecosystem. Moreover, the overall sensors' message receiving, handling, and response system must be more efficient, and various architectures have been presented in the paper.

Keywords: Sensors, Internet of Things (IoT), microcontroller, home automation, gadgets, communication protocols, message queuing telemetry transport (MQTT), constrained application protocol (CoAP), message response time

INTRODUCTION

The rise of the Internet of Things (IoT) has permitted the formulation of an array of innovative applications, consequently improving automation and efficiency across multiple sectors. Home automation exemplifies this phenomenon, wherein IoT technology is utilized to manage various facets of domestic life, including illumination, climate regulation, security systems, and entertainment apparatus [1].

Home automation pertains to the automated regulation of household appliances [2]. Various microcontroller-based systems have been engineered to supervise and control domestic devices using distinct parameters [3]. In contemporary times, ubiquitous objects such as

***Author for Correspondence**
Yatharth Agrawal
E-mail: agrawalyatharth007@gmail.com

Student, Spring Valley Public School, Kanadiya Bypass Road, Kanadia Main Rd, Indore, Madhya Pradesh, India

Received Date: October 11, 2024
Accepted Date: October 12, 2024
Published Date: October 21, 2024

Citation: Yatharth Agrawal. Efficient Message Captivating Environment in IoT Home Networks. International Journal of Mobile Computing Technology. 2024; 2(2): 8–16p.

sensors, actuators, and appliances with the internet have facilitated millions of people with various needs [4]. The demand for automation systems has surged markedly because of their myriad advantages, which streamline human existence, and promote energy, and time conservation [5]. Domestic appliances can be operated remotely through mobile devices, laptops, or the internet [6]. The progression of sensor technology and IoT has enabled seamless interaction with the environment [7, 8]. IoT embodies a global network of information for intelligent residences, consisting of internet-connected entities (Figure 1).

Home automation systems typically comprise three primary components: hardware, software/applications, and communication protocols. Each element is crucial for creating a genuine smart home experience for the users. Careful selection of appropriate hardware and protocols, along with thorough testing, helps prevent performance issues [9]. These systems generally connect devices to a central hub or gateway [10]. Control interfaces may include wall-mounted terminals, computers, smartphone applications, or web-based interfaces that are remotely accessible via the internet [11]. Various wireless technologies that support remote data transfer via Bluetooth, control, and cellular networks have evolved to improve home intelligence at greater levels [12].

The primary focus of this study is to develop IoT-enabled devices that consume less power and are more energy-efficient and cost-effective, while simultaneously providing safety and security and reducing the Wireless Message transfer and response time [13]. In addition, sending, receiving, managing, and maintaining messages and signals using various architectures, including communication protocols, message response times, constrained application protocols (CoAPs), and message queuing telemetry transport (MQTT) [14].

LITERATURE SURVEY

This section provides an analysis of various home automation system models that integrate diverse emerging technologies. Scholars have articulated and deliberated these systems, emphasizing their characteristics, benefits, and constraints [15]. The illustration below depicts a basic block diagram of the home automation system.

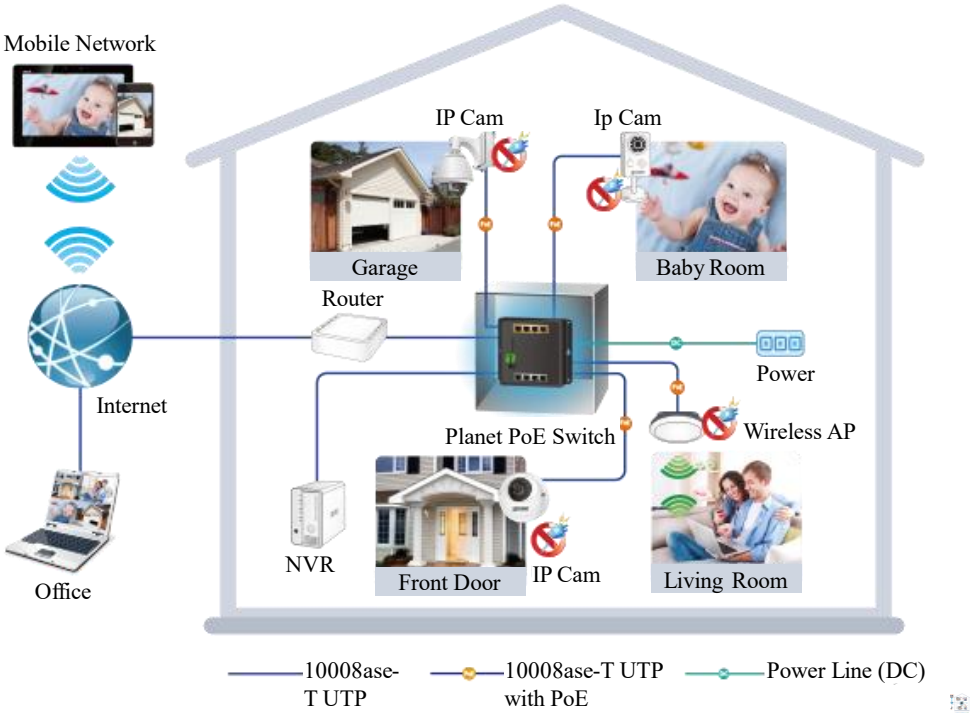

Figure 1. IoT for home network (existing).

Khan and Ahmad [16] presented a Wi-Fi-based home automation system that consists of three principal components: a web server serving as the nucleus for user control and monitoring of the home, and a hardware interface module that facilitates appropriate connections to sensors and actuators. This innovation has substantially improved the scalability and adaptability of the commercially available home automation systems. When the system runs smoothly, individuals can engage with the server's online applications through the web using a browser.

Cui and Kim [5] associates proposed a cloud-based system designed for the monitoring and regulation of home appliances. Their architecture employs a home gateway that collects metadata from domestic devices and relays it to a cloud-based data server for storage within the Hadoop Distributed File System, thereby providing monitoring functionality to remote users.

Baraka [10] introduced a home network that transmits data from household appliances and sensors to cloud-based data servers. This server systematically organizes information and delivers services by exchanging data and receiving user commands from various applications. The design demonstrates commendable modularity and reconfigurability while ensuring reduced power consumption and lower operational costs.

Lamine [7] engineered an Android-based application. They devised an interface card to facilitate effective communication between remote users, the Raspberry Pi, a web server, and home appliances. The application, which can be readily installed on Android smartphones, operates in conjunction with a web server and Raspberry Pi card to manage window shutters. The smartphone application transmits commands to the Raspberry Pi card, while an interface card updates the signals between the actuator sensors and the Raspberry Pi card.

Gabriele [6] used relays and specialized input-output drivers to interface an Arduino board that served as the controller for their GSM-enabled home appliances. To operate home appliances, an Arduino-connected GSM modem receives SMS messages generated by a smartphone application, which responds to user requests. However, this approach is expensive and has security issues.

Al-Ali [3]—The Konnex-Bus home automation system eliminates the need for distinct profiles by storing data for all actuators and sensors in a smart home which uses less energy. Vishwakarma [14] and Piyare [24] invented Zigbee technology as a home automation system, and work coordinators captured and saved performance. It uses a normal wireless Asymmetric Digital Subscriber Line (ADSL) modem router's four switch ports to create a Wi-Fi network with preconfigured Wi-Fi security settings and network SSID. After being analyzed by a virtual home algorithm and deemed safe, messages are re-encrypted and sent to the actual network devices. Zigbee communication lowers the installation intrusiveness and system expenses.

Kumar [22] presented a system that enables the internet-based operation of fundamental household appliances from any point in the world using PCs or mobile devices. The goal of this technology is to preserve both human energy and electrical energy. It consists of sensors and a Wi-Fi module server. The server can handle additional hardware interface modules and monitor a variety of sensors. The web server used was an Arduino board. The Automation System can be accessed remotely from any internet-connected PC or mobile device with a compatible web browser by utilizing the server's real IP address, or it can be accessed locally from any PC by using the server IP. As Wi-Fi is the most secure, it is used for all communication with sensors, actuators, and devices.

Jain [12] introduced algorithmic procedures and emails to construct a Raspberry Pi system. In practice, they maintained that home automation powered by Raspberry Pi is superior to alternative approaches such as DTMF-based automation, which has significant call tariff drawbacks. By using the already existing Gmail web server services, their solution improves system flexibility and efficiency by eliminating the requirements for web server design and memory space.

Baraka [10] introduced cloud-based servers to maintain all communication, interchange commands, and exchange information. Their system uses less electricity and provides strong configurability and modularity.

Vishwakarma et al. [14] suggested a system that leverages the Adafruit platform for web-based services and the Node MCU module to operate devices via Wi-Fi utilizing smartphones. It also contains voice control features for information execution and control.

Chen [17] proposed a smart system to handle garbage collectors or dustbins, as it leads to the cleanliness of the home and society.

Sheikh [18] implemented smart home automation with enhanced security features. They also discussed the limitations of the various wireless communication techniques discussed above, such as ZigBee and Wi-Fi [19].

Raza [20] colleagues presented a smartphone-based smart home system with touch-to-speech feedback for visually impaired people. The smartphone connects through a router that receives home location information and sends signals via IoT devices to activate the electronic devices [21].

This research aims to update the readers and researchers of the IoT field with the latest occurrences related to architecture/infrastructure and hardware and software behind the latest automation systems from 2019 to 2024.

PROPOSED SYSTEM

Recent technological advancements have significantly contributed to the growth of the IoT. The developments in ubiquitous computing are converging to create smart home technologies. However, the continuous introduction of new technologies raises concerns about security, privacy, and cost-effective implementation in smart home environments. To address these issues, we propose a secure, integrated, and affordable home automation system that overcomes the limitations of existing systems.

Focuses of Proposed System

- Scalability, affordability, and end-to-end security
- Implementation of a Virtual Private Network (VPN)
- Voice-controlled functionality
- Utilization of microcontrollers to enhance existing appliances
- Development of a practical, viable, and user-friendly application
- Use of best architecture for Messaging Protocol

The first important perspective is to add standards/benchmarks to hardware, software, actuators, and sensors. Otherwise, they pose the risk of excessive data generation at their end.

Over time, research has demonstrated that IoT is becoming an increasingly powerful tool. Today, humans are increasingly influenced by sensors and self-managing devices. For IoT users, privacy protection remains a primary concern that can be mitigated through smart technology. However, this also increases the possibility of hacking or system failure. Security challenges in IoT can be broadly categorized into three groups: systems, networks, and applications.

The proposed model aims to provide an integrated voice control system with enhanced security for each device connected to a smart home, ensuring a secure connection with the IoT network. OpenVPN uses RSA 2048 encryption with a certificate file, whereas Point-to-Point Tunneling Protocol (PPTP) is limited to MPPE-128 encryption using RC4 with a 128-bit key, and MS-CHAPv2 authentication using SHA-1.

A VPN or gateway can be a router, server, Firewall, or similar device with data transfer capabilities. It creates a point-to-point connection using virtual protocols, tunneling links, or encrypted data traffic.

A VPN-enabled Gateway Typically has Three Network Interfaces

1. *Wlan0:* Serves as the LAN entrance, collecting and delivering packets from local devices
2. *Eth0:* Maintains the connection between the gateway and WAN
3. *Tun0:* Created by the VPN client process

The VPN server forwards the restored packets to their original destinations, concealing the source IP and the port from the destination remote server. This protects the user's privacy against potential eavesdroppers.

The VPN security system authenticates senders to prevent unauthorized access and detects intrusions by sending direct user notifications. It employs a Public Key Infrastructure (PKI), which requires a public key (certificate) and a private key for both the server and client, as well as a Master Certificate Authority certificate and key for signing the server and client certificates.

Key Features of the VPN Security Model Include

- Server ownership of a certificate or key
- Server acceptance of connections only from clients with certificates signed by the master CA certificate

Implementing a VPN in Home Automation Involves Several Steps

1. Setting up a VPN server using a VPN appliance, server-based solution, or cloud-based service
2. Configuring the home automation system to work with the VPN, including router or Firewall settings
3. Connecting to the VPN using a remote device with VPN client software

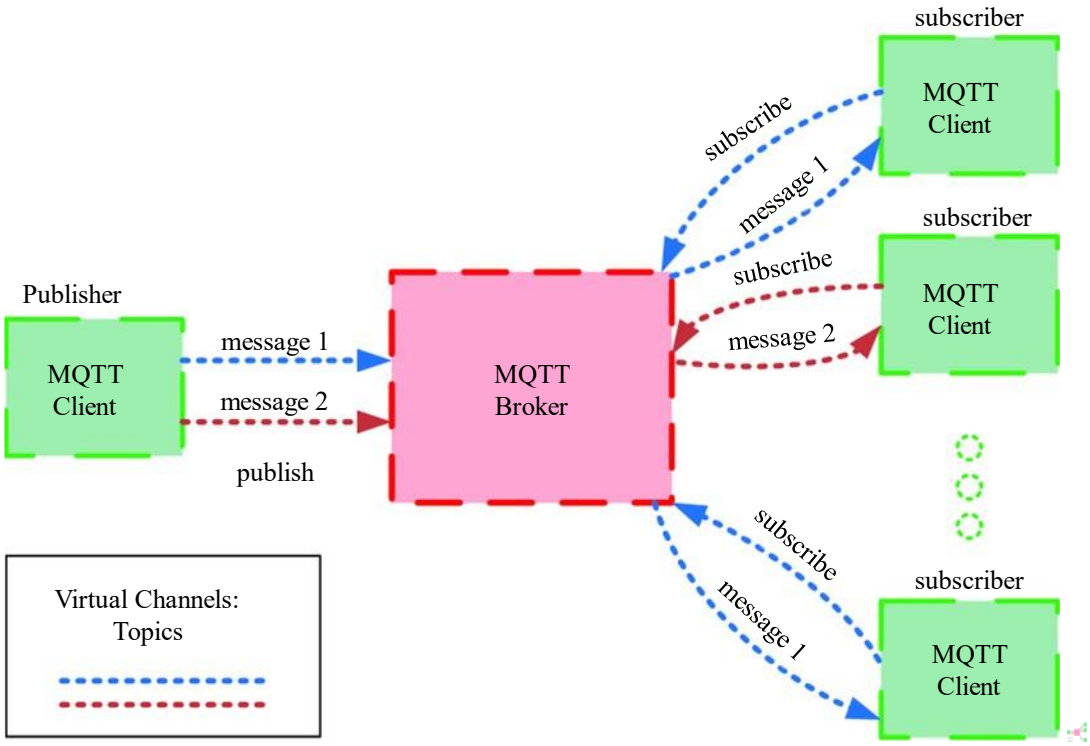

Figure 2. MQTT protocol for home network.

MQTT is a large-scale, lightweight network that can connect with various wearables, help analyze data and automate huge machinery (Figure 2). It uses a low battery and has faster communication.

The constrained application protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks on the Internet of Things (Figure 3). CoAP is designed to enable simple, constrained devices to join the IoT, even though constrained networks with low bandwidth and low availability. It is generally used for machine-to-machine (M2M) applications such as smart energy and building automation.

Essential Components for Connecting a VPN in Home Automation

1. *VPN Server:* Responsible for creating the VPN connection and encrypting traffic (e.g., OpenVPN, SoftEther VPN, and WireGuard).
2. *Home Automation System:* Comprises smart devices, controllers, and sensors for task automation.
3. *Remote Devices:* Used to remotely access home automation (e.g., smart displays, gesture control devices, smart thermostats).
4. *VPN Client Software:* Used to connect to the VPN server, supporting the required VPN protocol and encryption method Figure 4.

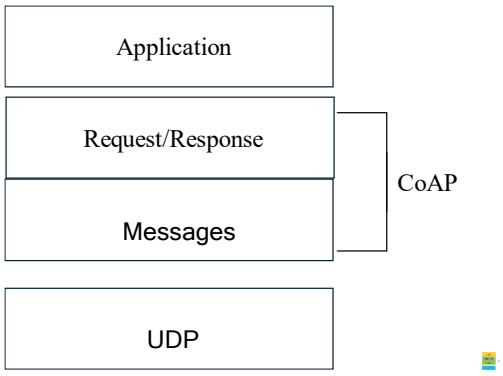

Figure 3. Constrained application protocol.

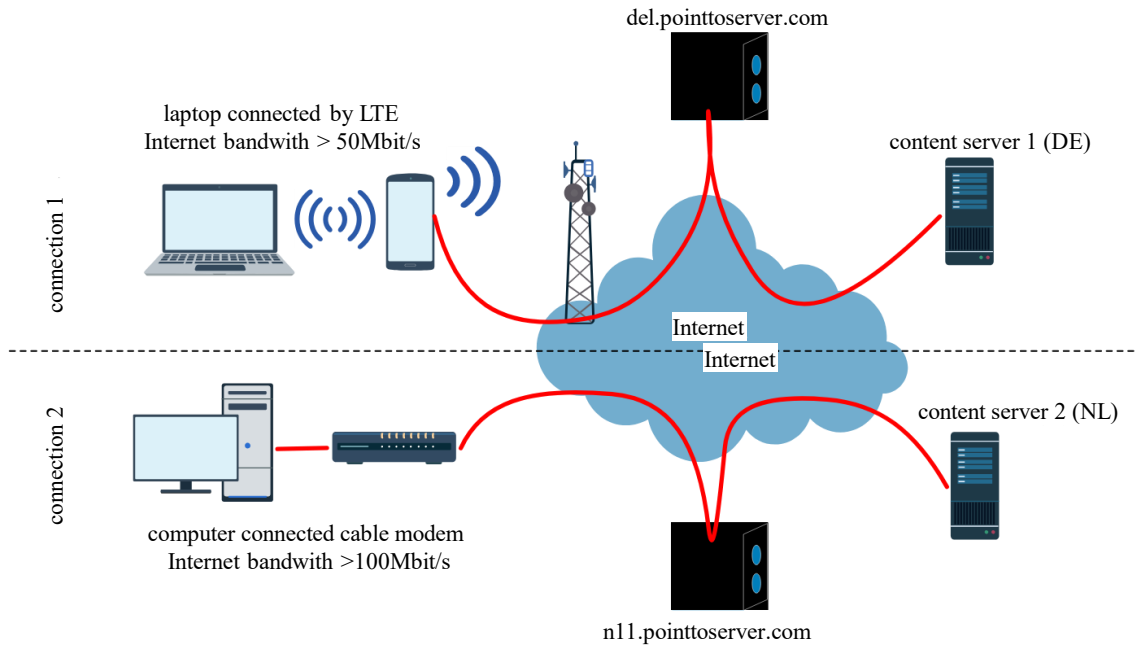

Figure 4. Virtual private network (VPN).

RESULT ANALYSIS AND FUTURE SCOPE

IoT, once considered a mere trend, has evolved into a significant technological advancement with promising future potential. In 2017, approximately 8.4 billion IoT devices were connected globally, increasing to 9.2 billion in 2018. Projections suggest that by 2020, this number could reach 20.8 billion, with IoT devices expected to generate trillions in value across various industries in the coming years [17–27].

The IoT is poised to bring about significant changes in both professional and personal spheres. Many IoT-based innovations are already in use and the progression of technology is irreversible [28]. The level of control and efficiency offered by the IoT is unprecedented, making it difficult for any industry to disregard or reject it. Messaging protocols such as MQTT and Constrained Application Protocol (CoAP) have their advantages and disadvantages; however, Message Queuing Telemetry Transport (MQTT) is better in the longer run owing to its architecture [29].

Currently, some IoT devices are directly accessible via the internet, whereas others are concealed within local networks and protected by firewalls and address-translating routers. Numerous researchers have proposed IoT technologies for this purpose. However, several challenges still need to be addressed [30]. Resolving these issues is crucial for the advancement of technology and should be the focus of future research. Future applications of IoT technology may include home automation, smart cities, intelligent transportation systems, and e-health solutions. A wide array of devices capable of sensing and responding to environmental activities are being developed and implemented.

Application

IoT is a concept that extends beyond the realm of computer science and finds applications in diverse sectors, such as agriculture, healthcare, lifestyle, manufacturing, retail, transportation, energy, logistics, and environmental monitoring. The versatility of this technology allows it to be implemented across numerous industries to enhance various processes and systems. One of the most practical and widely adopted applications of IoT is home automation, which has been integrated seamlessly into daily life, offering significant benefits in routine activities.

Applications of Home Automation Encompasses

HVAC Management

Heating and cooling expenses typically account for 50% of annual energy costs, making efficient HVAC control increasingly beneficial. The Nest Learning Thermostat, a leading product in this field, adapts to users' temperature preferences over time, eliminates manual programming, and offers smartphone control.

Intelligent Lighting

Energy-efficient lighting systems utilize motion and environmental sensors to regulate illumination. Key technologies in this domain include LED lights and network-connected lighting solutions.

Advanced Garden Systems

These systems employ IoT devices with soil moisture sensors to monitor the ground hydration levels. Water is dispensed through pipes when the moisture falls below a set threshold. Data were collected and analyzed on servers or cloud platforms to optimize the watering schedules.

Security Monitoring

IoT-enabled home security products allow for remote surveillance and management. These systems oversee home monitoring and regulate access through smart locks.

Intelligent Appliances

Smart appliances simplify the management and provide remote status updates. These consist of three main components.

1. *Controller:* Manages device scheduling and integration

2. *Designer:* Enables creation of controller configurations and user interfaces

This study presents an IoT-based model for secure, cost-effective home automation across multiple platforms. The implementation addressed the following challenges.

1. Integrating various technologies into a secure, user-friendly system
2. Overcoming privacy concerns and affordability issues

The proposed system initiates processes based on user requirements. The experimental setup effectively controls various home appliances. The design incorporates IoT and VPN concepts, enhancing security and affordability, while reducing wiring and simplifying installation. It also decreases household power consumption.

Future research should focus on developing security protocols that incorporate data-compression technologies based on the proposed considerations.

CONCLUSION

Although home automation is reaching the nook and corner of India, it will take a lot of effort to make IoT human-friendly and approachable. No doubt there is a risk of security and unintentional errors in the system, coming years will see a lot of growth related to research and development, Indian population usage patterns, and allied information. Technologies such as Wi-Fi, Bluetooth, VPN, and sensors and actuators are self-sufficient, and research has to be conducted to make them more user-friendly.

REFERENCES

1. El-Hajj M, Fadlallah A, Chamoun M, Serhrouchni A. A survey of internet of Things (IoT) authentication schemes. Sensors. 2019;19(5):1141. DOI: 10.3390/s19051141.
2. Kelly SDT, Suryadevara NK, Mukhopadhyay SC. Towards the implementation of IoT for environmental condition monitoring in homes. IEEE Sensors Journal. 2013;13:3846-3853. DOI: 10.1109/JSEN.2013.2263379.
3. Al-Ali AR, Al-Rousan M. Java-based home automation system. IEEE Transactions on Consumer Electronics. 2004;50:498-504. DOI: 10.1109/TCE.2004.1309414.
4. ElShafee A, Hamed KA. Design and implementation of a WIFI based home automation system. Int J Comput Inf Eng. 2012;6:1074-1080.
5. Cui Y, Kim M, Gu Y, Jung JJ, Lee H. Home appliance management system for monitoring digitized devices using cloud computing technology in ubiquitous sensor network environment. Int J Distrib Sensor Networks. 2014;10:174097. DOI: 10.1155/2014/174097.
6. Gabriele T, Pantoli L, Stornelli V, Chiulli D, Muttillo M. Smart power management system for home appliances and wellness based on wireless sensors network and mobile technology. In: 2015 XVIII AISEM Annual Conference. 2015:1-4. DOI: 10.1109/AISEM.2015.7066808.
7. Lamine H, Abid H. Remote control of a domestic equipment from an Android application based on Raspberry Pi card. In: 2014 15th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA). 2014:903-908. DOI: 10.1109/STA.2014. 7086757.
8. Jivani MN. GSM-based home automation system using app-inventor for Android mobile phones. Int J Adv Res Electr Electron Instrum Eng. 2014;3.
9. Gebhardt J, Massoth M, Weber S, Wiens T. Ubiquitous smart home control on a raspberry pi embedded system. UBICOMM. 2014;172-177.
10. Baraka K, Ghobril M, Malek S, Kanj R, Kayssi A. Low-Cost Arduino/Android-Based Energy-Efficient Home Automation System with Smart Task Scheduling. In: 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks. 2013:296-301. DOI: 10.1109/CICSYN.2013.47.
11. Koyuncu B. PC remote control of appliances by using telephone lines. IEEE Transactions on Consumer Electronics. 1995;41:201-209. DOI: 10.1109/30.370328.

12. Jain S, Vaibhav A, Goyal L. Raspberry Pi based interactive home automation system through E-mail. 2014 International Conference on Reliability Optimization and Information Technology (ICROIT). 2014:277-280. DOI: 10.1109/ICROIT.2014.6798330.
13. Coskun I, Ardam H. A remote controller for home and office appliances by telephone. IEEE Transactions on Consumer Electronics. 1998;44:1291-1297. DOI: 10.1109/30.735829.
14. Vishwakarma SK, Upadhyaya P, Kumari B, Mishra AK. Smart Energy Efficient Home Automation System Using IoT. In: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). 2019:1-4. DOI: 10.1109/IoT-SIU.2019.8777607.
15. Manojkumar P, Suresh M, Ayub Ahmed AA, et al. A novel home automation distributed server management system using Internet of things. Int J Ambient Energy. 2022;43:5478-5483. DOI: 10.1080/01430750.2021.1953590.
16. Khan MA, Ahmad I, Nordin AN, et al. Smart android based home automation system using internet of things (IoT). Sustainability. 2022;14:10717. DOI: 10.3390/su141710717.
17. Chen WE, Wang YH, Huang PC, Huang YY, Tsai MY. A Smart IoT System for Waste Management. 2018 1st International Cognitive Cities Conference (IC3). 2018:202-203. DOI: 10.1109/IC3.2018.00-24.
18. Sheikh RU, Kale PA, Sarfaraj S, Sukhdeve S, Sherekar K, Faruqui S. A review paper on IoT-based smart security and home automation. Int J Sci Res Sci Technol. 2021;8(3):700–705. DOI: 10.32628/IJSRST2183159.
19. Nurse JRC, Atamli A, Martin A. Towards a usable framework for modelling security and privacy risks in the smart home. In: Tryfonas T, editor. Human Aspects of Information Security, Privacy, and Trust (HAS 2016). Lecture Notes in Computer Science. Cham: Springer; 2016;9750. DOI: 10.1007/978-3-319-39381-0_23.
20. Raza S, Misra P, He Z, Voigt T. Building the Internet of things with Bluetooth smart. Ad Hoc Netw. 2017;57:19-31. DOI: 10.1016/j.adhoc.2016.08.012.
21. Desai D, Upadhyay H. Security and privacy consideration for internet of things in smart home environments. Int J Eng Res Dev. 2014;10:73-83.
22. Kumar PM, Sandhya N. Bluetooth based wireless home automation system using FPGA. J Theor Appl Inf Technol. 2015;77(3): 2015;77(3):411–420.
23. Wang M, Zhang G, Zhang C, Zhang J, Li C. An IoT-based appliance control system for smart homes. 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP). 2013:744-747. DOI: 10.1109/ICICIP.2013.6568171.
24. Piyare R, Tazil M. Bluetooth based home automation system using cell phone. 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE). 2011:192-195. DOI: 10.1109/ISCE.2011.5973811.
25. Shokri Gazafroudi A, Soares J, Fotouhi Ghazvini MA, Pinto T, Vale Z, Corchado JM. Stochastic interval-based optimal offering model for residential energy management systems by household owners. Int J Electr Power Energy Syst. 2019;105:201-219. DOI: 10.1016/j.ijepes.2018.08.019.
26. Djumanazarov O, Väänänen A, Haataja K, Toivanen P. An Overview of IoT-Based Architecture Model for Smart Home Systems. In: Abraham A, Gandhi N, Hanne T, Hong TP, Nogueira Rios T, Ding W, editors. Intelligent Systems Design and Applications. Singapore: Springer Int Publ; 2022. pp. 696-706. DOI: 10.1007/978-3-030-96308-8_65.
27. Overmars A, Venkatraman S. Towards a secure and scalable IoT infrastructure: A pilot deployment for a smart water monitoring system. Technol. 2020;8:50. DOI: 10.3390/technologies8040050.
28. Qiu W, Saleem K, Pham M, Halpern M, Beresford-Smith B, Overmars A, Dassanayake KB, Thoms G. Robust multipath links for wireless sensor networks in irrigation applications. In: 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP). 2007:95-100. DOI: 10.1109/ISSNIP.2007.4496826.
29. Yar H, Imran AS, Khan ZA, Sajjad M, Kastrati Z. Towards smart home automation using IoT-enabled edge-computing paradigm. Sensors. 2021;21(14):4932. DOI: 10.3390/s21144932, PubMed: 34300671.
30. Taiwo O, Ezugwu AE. Internet of things-based intelligent smart home control system. Sec Commun Networks. 2021;2021:1-17. DOI: 10.1155/2021/9928254.

