IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 May 2023, accepted 27 May 2023, date of publication 1 June 2023, date of current version 20 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3282095

RESEARCH ARTICLE

Design and Implementation of a Pilot Model for IoT Smart Home Networks

AMIN S. IBRAHIM[1], AHMED M. ABBAS[2], ASHRAF MOHAMED ALI HASSAN[3], WAEL M. F. ABDEL-REHIM[4,5], AHMED EMAM[5,6], AND SAEED MOHSEN[5,7]

[1]Electronics and Communications Department, Thebes Higher Institute for Engineering, Cairo 11434, Egypt
[2]Nuclear Research Center, Egyptian Atomic Energy Authority, Qalubia, Cairo 11787, Egypt
[3]Department of Electronics and Communications Engineering, October High Institute for Engineering and Technology, 6th of October 12596, Egypt
[4]Department of Computer Science, Faculty of Computers and Information, Suez University, Suez 43512, Egypt
[5]Department of Artificial Intelligence Engineering, Faculty of Computer Science and Engineering, King Salman International University (KSIU), South Sinai 46511, Egypt
[6]Computer Science and Mathematics Department, Faculty of Science, Menoufia University, Menoufia 13829, Egypt
[7]Department of Electronics and Communications Engineering, Al-Madinah Higher Institute for Engineering and Technology, Giza 12947, Egypt

Corresponding author: Ahmed M. Abbas (ahmed.abbas@eaea.org.eg)

ABSTRACT Internet of Things (IoT) technology is a complementary part of our style of life. IoT technology coexists with existing cellular communication for developing 5G. Both academic researchers and industrial householders pay attention to the benefits of IoT technology. However, the rapid growth of IoT networks suffers from some limitations, such as heavy traffic load, traffic congestion,…*etc*. In this paper, a parallel distributed smart home architecture is proposed to solve human-being problems and achieve welfare in society. The proposed network has a light traffic load and low traffic congestion to avoid a single-point failure. The architecture of the proposed smart home network involves connectivity, security, registration, protocols, and scenarios to update registration. Also, the paper presents a framework of state diagrams, processes, and algorithms for IoT smart home networks. This framework includes a design and implementation of a pilot model of IoT smart home domains to meet human beneficiaries. The model consists of six practical smart home network domains in both normal and urgent modes to proof of the concept. The pilot model is programmed based on three major aspects: objectives, processes with algorithms, and state diagrams. The novelty of the paper lies in the capability to implement a smart home architecture pilot model using simple development kits. The design and implementation of the practical IoT smart home networks are tested and measured using a CoolTerm sniffer tool. The results of measurement prove that the proposed model achieves light traffic profiles and low average data rates.

INDEX TERMS IoT, smart home, networks, pilot model, IoT protocols, traffic profile.

I. INTRODUCTION

Internet of Things (IoT) is one of many technologies established for emerging wireless cellular communication network, such as 5G and 6G [1], [2], [3], [4]. IoT technology is ''everything talks with others in an intelligent & automated manner to gain human beneficiary''. IoT devices may be physical electrical devices or virtually through the website on the internet. The IoT exploits the interaction of things within the surrounding environment to collect information, process it, make a decision ''actuating'', and send data to other things using existing or evolving communication technologies. In addition, the IoT would be used as a component in the operational technologies of nuclear power plants and radiation monitoring networks as a complement component of the smart city toward achieving a green environment [5], [6]. In 5G technology, it is predicted that IoT technology can offer numerous beneficiaries to satisfy the rapid growth of citizen demands and services in efficient methods, low cost, energy saving, green communication, secure, and optimized ways. IoT technology covers a variety of applications in all society fields, such as security [7], logistics [8], asset tracking [9], and monitoring [10], smart metering [11], smart homes [12], retail & vending [13], and E-health [14].

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

The smart home is one of several IoT use cases that is not limited to connecting things (e.g., sensors, actuators, cameras, home appliances) with each other, but it is extended to offer amazing new solutions in our live homes, meeting connecting people's needs. Moreover, it can remotely monitor and control the overall system. Therefore, IoT technology-based smart homes simplifies the daily tasks of humans, seamlessly make the home a safe environment & more secure and provide greater peace of mind in the house.

IoT-based smart home has a variety of available smart appliances in homes. For instance, smart thermostats can be automatically adopted to make the weather of the house appropriate to the inhabitants, light bulbs can be controlled to the content of TV play, and garden sprinklers can work in an efficient way in coordination with the weather forecast, smoke and gas alarms, washing machine dishwashers, coffee makers, garage door, window shades, and of course refrigerators.

Usually, smart home things are connected to the short or very short range of existing wireless communication technologies to internally guarantee reliable connectivity among them in the wireless Local Area Network (WLAN) or even through long cellular communication networks. However, the diversity of IoT devices ''home appliances, sensors, actuators'' at any place with increasing numbers of connectivities among them anywhere in the IoT smart home causes a new wave of complicated and the huge amount of traffic data, specifically over the traditional and centralized networks with the limited capabilities to handle and support the heavy traffic load [15], [16], [17], [18], [19], [20], [21].

This paper presents an IoT smart home network design that achieves light traffic profiles, low average data rates, and mitigates network drop due to single-point failure, and has ease of scalability. The paper proposes parallel, distinct, and distributed IoT smart home networks with a simple and low-cost development kit. The hierarchy architecture is adopted instead of the centralized smart home networks in the existing works [15], [16], [17], [18], [19], [20], [21] to solve many IoT smart home issues, such as single point failure, heavy traffic load, and traffic congestion. The proposed system architecture has a parent node ''cloud'' that is connected to many separated route nodes ''parallel, distinct, and distributed networks'' in the sensor field. Each routing node is expanded onto many leaf nodes ''IoT smart devices''. Each parallel, distinct, and distributed network has a group of smart IoT devices, attached to one low-cost ''microcontroller ESP82266 Node'' as a coordinator for efficiently organizing tasks, communication, and relations among them. The controller on the same network can communicate with the IoT broker ''gateway'' and the user interface point ''Mobile app or web server'' via the internet. The behaviour of the proposed IoT smart home networks considers security, scalability, registration, and interoperability. In this paper, the parent node of the proposed smart home networks could be expanded into M number of route nodes ''parallel, distinct, and distributed networks''. The route node ''controller'' in a such network could be also expanded by N number of leaf nodes ''IoT devices'' based on its capabilities ''input-output terminals''. This type of network can interface and be interoperable with other IoT heterogeneous networks and cellular networks via the Internet. The proposed smart home networks are supported by three main servers in the smart home management system to develop security, registration, and update registration.

The contributions of the paper are mainly in two points:

- The capability to realize a smart home architecture pilot model using the simplest development kits i.e. ESP8266;
- Accordingly, the pilot model enables researchers and developers in the future to utilize this pilot as the base for continuous development according to future predictions and demands.

The paper is organized as follows: Section II presents the related works. The proposed smart home model including a generic architecture for IoT applications and a typical smart home model is explained in Section III. Section IV formulates and designs the six main smart home domains. The implemented smart home pilot is presented in Section V. Section VI describes the experimental results of the pilot model measurements. Finally, Section VII shows the conclusion of the paper.

II. RELATED WORKS

In the literature, several designs and implementations of IoT smart home architectures have been presented [15], [16], [17], [18], [19], [20], [21].

Chaudhuri et al. [15] designed and implemented an IoT framework for home automation and monitoring. They controlled the home appliances with the human being. Their paper prototyped several smart home projects: Turning ON/OFF lights, motion sensing, smoke sensing, and temperature detection. However, their work is a limited number of source nodes (sensors/actuators), and thus the IoT smart home system couldn't be extended to provide scalability. Their proposed system depended upon human interaction and didn't reflect the smart or automation concept in their system.

Jabbar, et al. [16] designed and fabricated a smart home prototype based on an automation system using an Arduino controller and an Android smartphone. Several sensors, Arduino, ESP8266 Wi-Fi, actuators, and home appliances were installed to develop the proposed smart home system. However, their work adopted the centralized approach. In this work, an Arduino was a controller for all system components. The centralized manner caused a single-point failure and doesn't meet the IoT concept. In addition, a single Arduino had limited Input/output terminals, which made the system can't achieve scalability. Finally, it didn't develop parallel distributed ''heterogeneous'' networks.

In [17], Hoque et al. proposed a framework to build a low-cost smart home security system. The design included a Camera, a magnetic reed switch, an Arduino, a Raspberry Pi, and an Android application via the Internet. However, their work didn't tackle other scenarios or applications in the smart city. Although Wi-Fi technology is cheap and exists

in most smart home systems, it can't be used for communication in the smart security system. The authors exploited two main controller units ''Arduino and Raspberry Pi'' for the communication between the magnetic reed switch and the internet-based RF signals, which encounters interference. Thus, this smart security system was expensive compared to other smart home systems.

Tayan et al. [18] proposed a home automation system based on IoT technology and focused on safety monitoring, home-security monitoring and energy monitoring and control. Each domain had its associated controller and isolated components. Scalability, heterogeneity, and modularity are considered in their design. However, in the security monitoring module, an ultrasonic sensor detects objects at a very narrow distance and didn't cover a long-range distance. The communication technology used in their module was Bluetooth which only covere a short-distance region. The wireless connectivity was not supported in both the energy monitoring and the safety monitoring modules. The sensors were communicated with the internet using an Ethernet shield. In case of any failure or faults in the wired connections, all components in the smart home automation system are disconnected. Finally, the system may be subject to a single-point failure due to Master Arduino that was centralized around the smart home automation system.

In [19], Davies et al. formulated, architected, and installed the Rapid Application Development (RAD) in the smart home system based on IoT technology to increase the robustness and to solve the problem of time development. However, the smart home system was simulated and did not practically prototype and the number of sources (appliances, sensors) was not considered in the execution time result to judge the robustness of their system.

Baranilingesan et al. [20] designed and implemented a simplified and centralized smart home automation with two main scenarios: manual and automatic operations. However, their work didn't cover several use cases and human demands in the IoT smart home system. It was limited to monitoring and controlling a low number of source nodes and electrical devices using the smartphone application.

In [21], Sisavath, et al. proposed a full IoT smart home integrated with Gateway and mobile application. The authors architected, designed, and implemented the IoT smart home system using advanced communication technology and software to collect and display the temperature and humidity sensor only on the mobile application. The main drawback of this work that the IoT system had a limited number of sensors was used to generate diverse types of data traffic on the cloud.

All previous works did not completely escape the shackles of traditional automation concepts, that monitor the physical parameters in the sensory field ''physical layer'' side using the source nodes (sensors, appliances, cameras,...*etc*) and then control or actuate the home appliances at the same environment through the web server or mobile application in the front end side ''application layer''. The previous methods have only one communication channel using the centralized controller unit ''Arduino/Rasberry Pi'' from the sensory field on one side onto the cloud on the other side. This problem may encounter from a single-point failure. Consequently, this failure will lead to traffic congestion and a heavy traffic load on the central unit. Specifically, when it accepts or receives data from a massive number of source nodes.

The limited capabilities of power, processors, and memory in the central controller didn't allow the traditional subsystem to handle the high traffic load and sent it onto the cloud. Thus, the existing systems can't deploy over large areas and don't provide the scalability concept. This problem restricts these systems from being interoperable with other heterogeneous networks. The coexisting between the traditional home automation system based on IoT and other networks with different technologies leads to an increase in the traffic load and generates a new wave of a complicated traffic type, which is difficult to process and analyze on the cloud entity.

Most of the existing works relied on the central controller unit with limited input/output terminals to interface and handle real smart home systems, including massive IoT devices (sensors, actuators, and home appliances). This limitation restricts the scalability concept.

Finally, the previous works discussed the registration using an IP address on the mobile application to enter the smart home automation system. However, they didn't tackle the security system. They didn't propose a framework to prevent unauthorized users to access the IoT smart home system.

III. THE PROPOSED IOT SMART HOME ARCHITECTURE

The proposed IoT smart home system solves many limitations in other previous smart home automation networks such as; heavy traffic load and traffic congestion, limited capabilities of the controller unit (limited source nodes), scalability, and single point failure.

The proposal is composed of parallel distributed networks, each with its associated source nodes ''Thing enablers'', communication network, and main controller ''Intelligent Device''. Inside the network, the source nodes communicate with each other at a certain zone in the form of scenarios. The controller unit for each distinct network is connected to the IoT broker (gateway) and the web browser/mobile app through the internet. The whole proposal is described in Figure 1.

The source nodes in the same network can generate light data traffic via Wi-Fi technology. The data traffic in one network is different from others based on the source nodes' types. The light data traffic on each parallel distributed network is aggregated on the IoT broker and the cloud of the proposed smart home system. The expected heavy traffic load on the cloud is distributed and divided into different light traffic loads, which were generated over distinct networks in the sensor field. Compared to other previous smart home automation systems that have one centralized and limited controller unit that can't provide the connectivity of diverse source nodes and may not handle the expected and generated heavy traffic over these source nodes. Accordingly, the

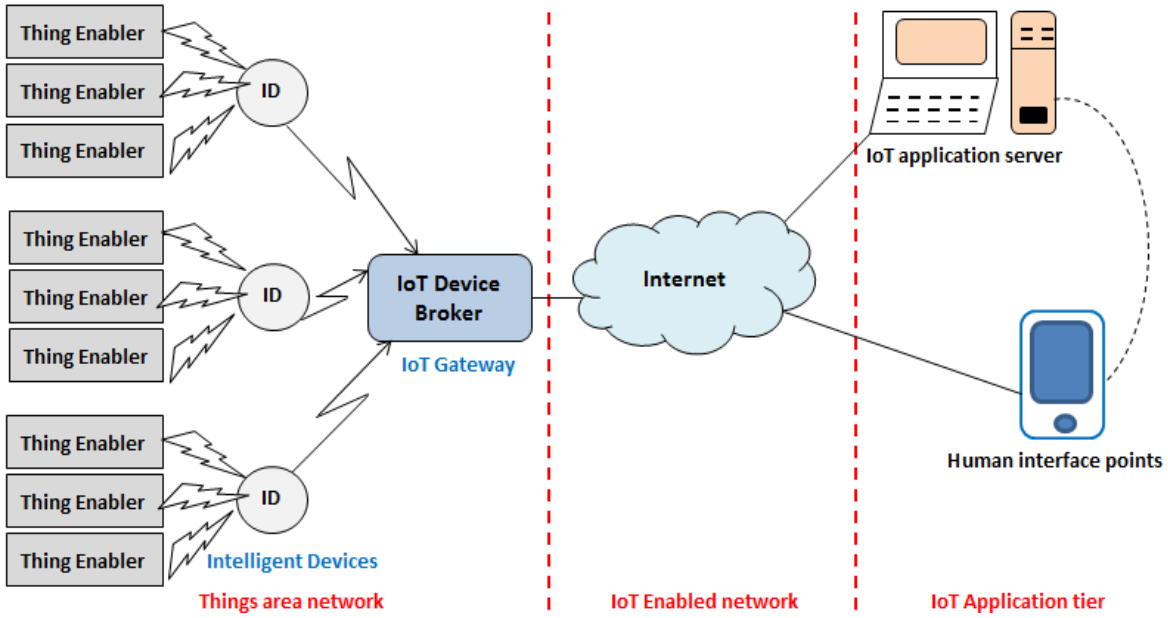

FIGURE 1. Proposed generic IoT network architecture.

proposed heterogeneous networks can avoid the problem of traffic congestion and the expected heavy traffic load.

It is supported by several controller units to solve the problem of the limited capability at a unique centralized controller unit. As shown in Figure 1, the proposal has several heterogeneous networks and controller units that are connected to the IoT broker unit. The proposed architecture enables the installer to add a massive number of source nodes at the same controller in such a network and other extra heterogeneous networks on the same IoT broker unit. Consequently, the proposed system can provide interoperability.

The proposed heterogeneous networks can be easily deployed and extended over large geographical areas as shown in Figure 2 such as smart community, smart campus,...*etc*. Accordingly, the scalability can be increased.

In case of one controller of network X at a certain zone has fatigue, the source nodes that attached to the failure controller is only stop working. The remainder networks of the other zones are working properly and don't affect by the failed network. In this paper, the proposed smart home networks enable the user on the other side to detect the fatigue network. The proposal allows a user to monitor the connectivity and the operation of each distinct network inside the IoT smart home system through queries. Regular request and response messages are sent from each installed controller into the cloud on the other side and vice versa. If the acknowledge message wasn't sent by one controller unit, the user recognize that some fatigue in this network. Thus, the proposed IoT smart home doesn't have a single-point failure problem.

In this paper, the proposed IoT smart home system provides registration and security rather than other existing smart home automation systems. As seen in Figure 2, the management smart home system involves Things Naming Server (TNS), and Authentication, Authorized, and Accounting (AAA) server that can monitor and detect any anomaly data of the unauthorized users that try to access the proposed IoT smart home system.

The proposal includes the following:

- IoT smart home architecture that develops parallel distributed networks.
- IoT smart home management framework, including several protocols for connectivity, registration, security, and update registration.
- IoT smart home network has six main domains to prove the concept.
- Design and implementation of the six practical scenarios of each domain over a real pilot model smart home zones, including process, algorithm, and state diagram.
- Monitoring the traffic profile and the average data rate in the measurement results.

A. PROPOSED GENERIC ARCHITECTURE

Figure 1 shows the main components of a generic IoT network architecture as follows:

- **Things Enablers:** The electronic devices located at one end of the IoT architecture network, called things network. They interact with the physical environment for measuring and sensing purposes. The things enablers may be sensors or devices. They use the short and very short range of existing wireless technologies (e.g., Wi-Fi, ZigBee, RFID, and Bluetooth) to send their sensed data into intelligent devices in the sensor field. Wi-Fi and ZigBee nodes are the most key enablement for developing the connectivity among the elements composed of the things domain.

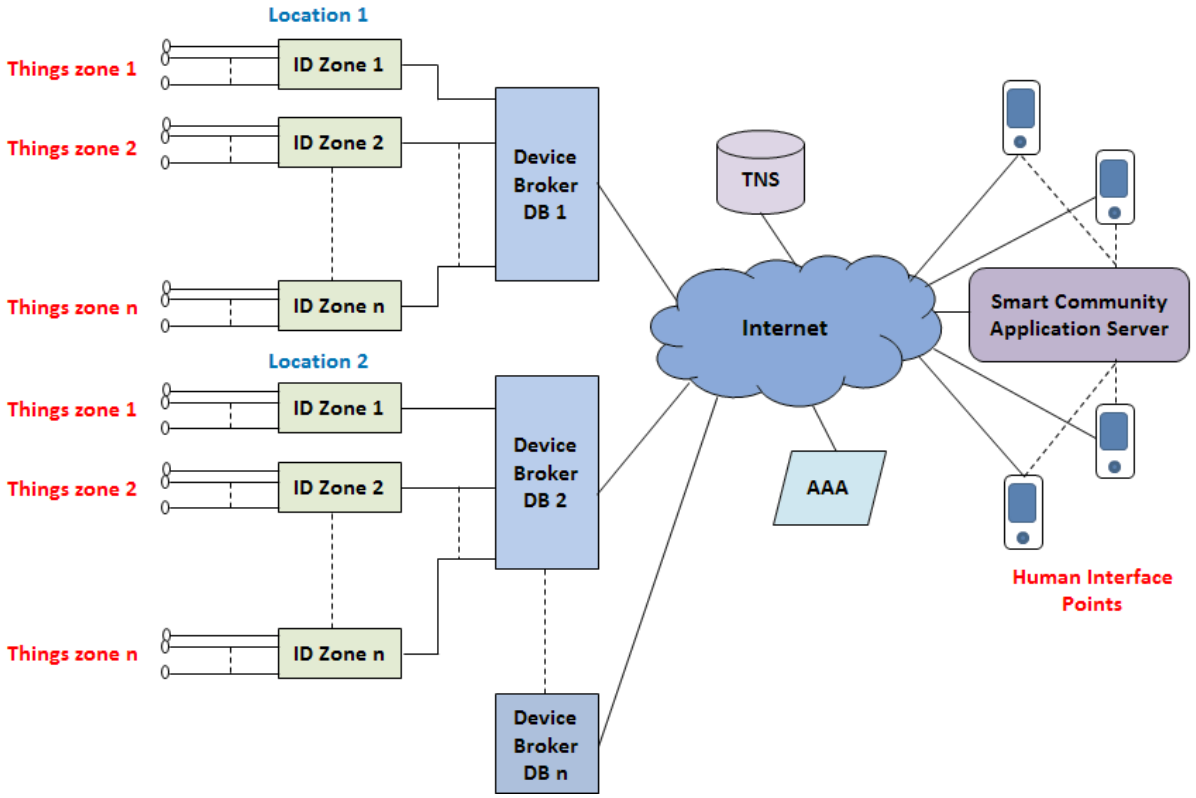

FIGURE 2. Proposed smart home management hierarchy.

- **Intelligent Device (ID):** It is used to collect and coordinate data from a group of things enablers at a specified place of the sensor field. Then, it can send and manage these data into an IoT device broker.
- **IoT Device Broker:** It is namely, IoT gateway which receives the sensed data from several IDs in the sensory field. It then integrates between two or more heterogeneous networks, such as the things area network and the IoT enabled networks. For example, an IoT device broker may be a router or ZigBee gateway.
- **IoT Application Server:** It can be hardware/software entities (e.g., data centers, computers, databases in the cloud, *etc*.). They provide data storage, big data processing, and data analytics to manage the collected data incoming from things and take accurate decisions or actions suitable for the actuation process. Thing speak is an example of an IoT platform for monitoring and actuating different unstructured big data of things/devices.
- **Human Interface Point:** This can be a mobile app operating on a smartphone or tablet or a web service browsed from a laptop. It is connected virtually to the IoT application server through internet media.
- **IoT Enabled Network:** This network uses long-range wireless communication technologies, including backhaul and core network, to interconnect the collected sensed data from IDs onto the IoT application server through the internet. IoT-enabled networks have existing and evolving networks from 2G and 3G onto Low Power Wide Area networks (LPWA) along with 3G, LTE, and LTE-A.

B. PROPOSED IoT SMART HOME MANAGEMENT SCENARIOS

Figure 2 explains the proposed IoT smart home management architecture hierarchy for diverse community locations with different profiles and functions, e.g., home, company, restaurant, club, and business building. The main issue of this hierarchy is to design a standard agreement of IoT smart home management to achieve integration and harmony among different smart home location characteristics.

As previously illustrated in the smart home system, each hierarchy location consists of a set of zones. Each has numerous things associated with a specified intelligent device, namely ID Zone or Beacon. The things zone can be categorized as associated family, complementary, and non-complementary things. The communication among these things is provided by ID Zone, which contains things IPs mapping table, including all IP destination addresses of things zone. Connecting two different ID zones is necessary to communicate different zones. All these components are located in the sensory field network. Each ID zone of a certain location can connect to the internet using one Device Broker (DB) gateway, which interfaces between the things low range network and wide range communication network or internet.

After an internet connection, the IoT smart home management system's clouding system includes three main servers: (TNS) server, (AAA) server, and the smart home application server. TNS server is a database of things information, carrying the things names of the overall IoT smart home management system and corresponding IP addresses in terms of their equivalent zones. The TNS server provides ID zone by the name of each thing. AAA server is responsible for registration, authentication, and update registry (reconfiguration) of all things of IoT smart home system. It authenticates and authorizes each thing of the system for access control policy. It provides an encryption process for data integrity protection using Advanced Encryption Standard with a 128-bit symmetric key (AES-128) security algorithm and empowers ID Zones to create addresses for all things zone. The smart home application server is used for data management to generate statistical analysis, helping it to take a suitable decision and actuation of things or human interface point. For example, a smart home application server manages things data of the human safety domain from such zone to send fire or smoke alarm messages into the human interface point (e.g., mobile phone) or even activate sound and light indicators things.

The paper proposes scenarios leading to a full description of the IoT smart home management system and explains the policies governing the interconnection among system elements. The most proposed IoT smart home system protocols are subject to Constrained Application Protocol (CoAP), which is applied to IoT communication. It is a web/document transfer protocol like HTTP protocol. It is supported by UDP protocol (e.g., connectionless datagram) with small packets and lower overheads or headers rather than HTTP, runs over TCP flow and guarantees reliable connection [22]. CoAP protocol employs a request/response model. The CoAP protocol is a client-server network, where clients (things) request information from the server (DB), and the server sends a response as in HTTP to increase some level of assurance in the connectionless UDP transport. In addition, it makes addressing client/server networks attached to UDP connection easier. The proposed IoT smart system protocols can be described as follows:

1) THING REGISTER ON IOT SMART HOME NETWORK

Firstly, the thing of the certain zone should be registered and secured in IoT smart home management system to keep the system's privacy, provide data integrity, and avoid any external intruder or hacker on it. Before the registration process, the hashing algorithm converts k thing (thing X input number) into k1 hash value. Secure Hash Algorithm (SHA-1) is the most common hashing algorithm. It is designed to be a collision- resistance, meaning it is difficult to find the same hash string value created for different data.

Thing X requests registration (e.g., Thing ID) through a message carrying its hash value onto the AAA server. The server also produces an equivalent hash value from its K thing using the SHA-1 algorithm. If the hash matches, it notifies that the k thing values match due to the collision-resistance property. Otherwise, the server mitigates any intruder things from accessing the system. Next, the server uses AES-128 encryption security to produce K2-key encryption from its hash value and generate a random number. Then, it exploits K2-key to encrypt Thing ID before sending it into Thing X.

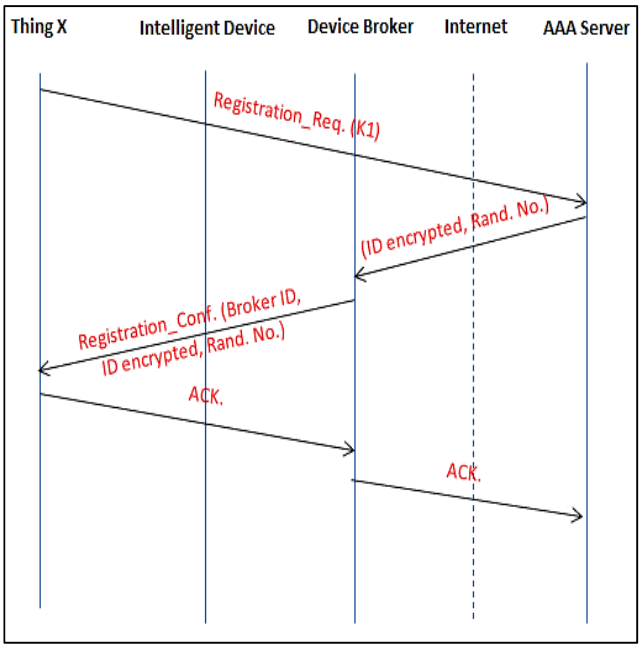

FIGURE 3. Things registration protocol on IoT smart home system.

AAA server confirms registration by sending a random number and encrypted ID into DB suitable for thing X. In this way, the AAA server enables DB to directly interact with its Thing X. Next, DB can send ID encrypted, random number, and its ID broker to Thing X. Where, the random number is valid to decrypt the ID encrypted of thing X. The ID broker is used from Thing X to acknowledge registration into DB, which releases the complete registration process by sending an ACK. Then inform the AAA server that Thing X recognizes its ID and DB for connectivity and transmission with equivalent neighbor things in IoT smart home management system. The whole scenario is discussed in Figure 3.

2) SECURITY PROTOCOL FOR AUTHENTICATION AND ENCRYPTION ALGORITHM

After the registration scenario, thing X of a certain Intelligent Device requires authentication through the AAA server. Thing X requests a connection, carrying its ID encrypted into the AAA server, which checks if this identifier is previously registered on it or not. AAA server sends a connection response message with an activated ID encrypted into the ID device, bypassing its identifier into thing X to confirm that thing X is authenticated. At this moment, Thing X is defined as an ID device that can connect easily.

Thing X again requests information about opening a virtual session, which permits thing X to establish a connection in the next scenarios of the IoT smart home management system.

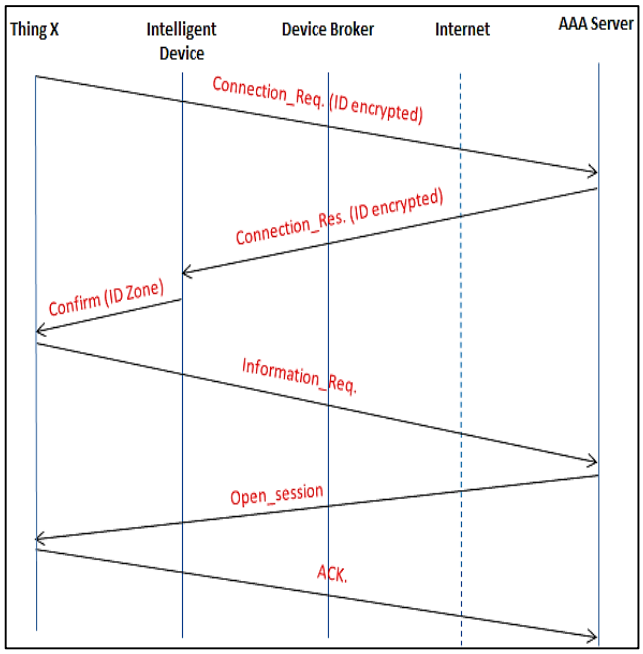

FIGURE 4. Authentication & authorization scenario of IoT smart home management system.

AAA server makes authority to an authenticated thing X to open a session to it for performing connection and exchanging data processes in the proposed approach. Finally, thing X acknowledges opening the session to the server successfully. The whole scenario paragraph is shown in Figure 4.

After the establishment of the data session, the data or information should be encrypted before being sent through the created session between the Thing X and any Thing or the cloud in the IoT smart home networks. In case of the data exchange between two Things at different zones, the data is encrypted by the ID device 1 which is to the Thing X as a source. While, the other ID device 2 of Thing Y as a receiver has an essential role in decrypting the incoming encrypted data from the source. In case of the data exchange between two Things in the same zone, one ID device can perform both encryption and decryption processes. Data exchanges are encrypted and decrypted using a highly secure cryptographic tool, called AES-128 bit key length algorithm [23].

In the AES-128 bit algorithm, the data to be sent before it ciphered ''Plain text'' of 128 bits size is ciphered with a private key of the same size through 10 rounds. The first nine rounds involve four stages: SubBytes, ShifRows, MixCoulmns, and Add Round Key. While, the tenth round has the same stages excluding the MixCoulmns stage. The AES-128 bits algorithm adds the security key for each round ''Add Round key K'' [23].

In the SubBytes function, each byte in the plaintext is replaced or mapped by another byte from the lookup table using matrix of 16×16 byte values called S-box. Each byte in the plaintext was mapped by the equivalent byte in the S-box that has the same coordinates. This matrix aims to avoid any redundancy or duplication in the plaintext bytes.

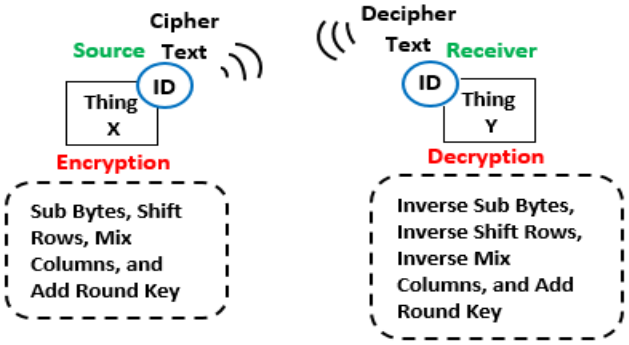

FIGURE 5. Ciphering and deciphering of data exchange between two Things.

The next step is the Shif Rows stage which shifts the raws of the plaintext matrix to the left in a circular manner. The first raw in the plain text matrix is not shifted. The second raw is shifted one byte to the left. The third row is shifted 2 bytes to the left. The last or the fourth row in the plain text is shifted 3 bytes to the left.

The Mix Column transformation stage is a matrix multiplication process. Each column in the matrix is treated individually as a polynomial over the GF(2^8) and multiplied modulo $X^4 + 1$ with the fixed polynomial of $a(X) = \{03\}X^3 + \{01\}X^2 + \{01\}X^1 + \{02\}X^0$ to produce a new byte value that is a function of all four bytes in the column. The plaintext matrix is XOR with the private Key to produce the cypher text in the Add round Key stage.

The cypher text is sent from the ID device of the source Thing onto the ID device of the receiver Thing. The ID device receiver decrypts the cypher text using AES 128 bits. The decryption is the inverse process of the encryption method. the decryption process has 10 rounds, each round consists of the four main stages: Inverse Sub Bytes, Inverse Shift Rows, Inverse Mix Columns, and Add Round Key, respectively. The tenth round has the same stages excepts Inverse Mix Columns. Finally, the ID device receiver sends the decrypted data to the receiver Thing. Figure 5 clarifies graphically the role of the source and receiver.

3) CONNECTION BETWEEN TWO THINGS IN THE SAME ZONE

Figure 6 shows the handshaking between things in the same IoT smart home system zone. Essentially, addresses of the IoT devices in the same zone are easily recognizable due to their connection to the main controller (physical ID device). Therefore, there is no need to request IPs of things from ID devices. The connection between two things passes through three main stages: connection setup, data transfer, and connection release.

The connection will be established when Thing X requests a connection from neighbor Thing Y at the same Zone to check if it is freely available, busy, or even out of service. If Thing Y is available, it is converted from idle mode into the wake-up mode for operation. Thing Y responds to the

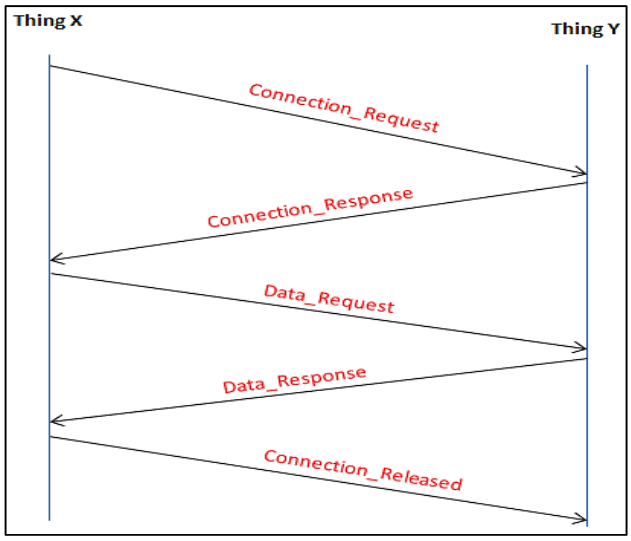

FIGURE 6. Message sequence chart of things connection in the same zone.

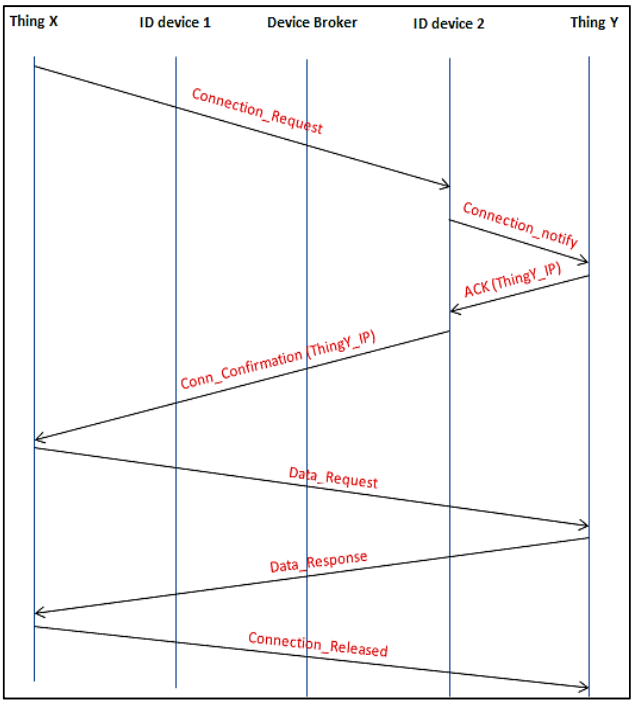

FIGURE 7. Things connection protocol at different zones of IoT smart home system.

connection setup process via sending an acknowledgment to Thing X. After connection setup, data will be exchanged between two things at the same zone. Thing X requests data from Thing Y. While Thing Y responds with a connection to Thing X. After handshaking, the connection is released by Thing X as well as, Thing Y returns to its idle state.

4) CONNECTION BETWEEN TWO THINGS IN DIFFERENT ZONES

The IP address has an important role in the communication between two things (e.g., X and Y) at different ID devices (e.g. zones 1 and 2), as depicted in Figure 7. Thing X needs the thing destination address of Thing Y to interconnect with Thing Y. It sends a connection request to its ID device. However, ID device 1 hasn't this IP due to thing Y being at zone 2 and its address is founded at ID device 2. Based on the DB, ID device 1 knows the address of the corresponding ID device 2, and vice versa. So, Thing X requests a connection (e.g., Thing Y_IP) from ID device 2 along with ID device 1 and DB. ID device 2 sends a connection notification to Thing Y to test its availability. When thing Y is available, it accepts the handshaking with Thing X. Thing Y transmits an acknowledgment message with its IP address into ID device 2. Then, thing X receives a connection confirmation message, having Thing Y_IP from ID device two passing through DB and ID device 1, respectively. Both Data request and Data response messages can be used to transfer the information between both things. Thing X releases the connection after the data transfer scenario between the two things is completed successfully.

5) CONNECTION BETWEEN THINGS AT DIFFERENT LOCATIONS

As explained in Figure 7, the connection scenario between two things at different locations of the IoT smart home management system is similar to the scenario between things at different zones of the same location. However, it differs in the connection methodology between two different ID devices (zones) at different locations. Therefore, only DB has an important role in the connection methodology in this scenario.

As shown in Figure 8, the connection between two DBs through the internet makes the telemetry interconnection between two ID devices at a different location in IoT smart home management system. Virtually, both DB1 and DB2 are responsible for message routing from/to things in the level of things field domain. They talk together through the internet to arrive at and access a suitable ID device (e.g., ID device 2) having the IP address of Thing Y. Whereas DB2 selects among different routes of many associated ID devices to find a required IP address of Thing Y. Then, DB2 sends the response into DB1 with Thing Y IP, which is transferred into ID device 1 and then Thing X. The data connection between two things exists, and the disconnection will be achieved after the data exchanging process is finished.

6) UPDATE REGISTRATION ON IOT SMART HOME NETWORK

Figure 9 describes the update registration scenario of a current thing X, falling (e.g., out of service) for a long time to be configured with previously designed things in IoT smart home management system. First, thing X requests a connection message onto DB with its K1 hash value. Then, DB fetches if the ID of thing X is changed or not. Finally, if Thing ID is valid, DB confirms the successful registration into Thing

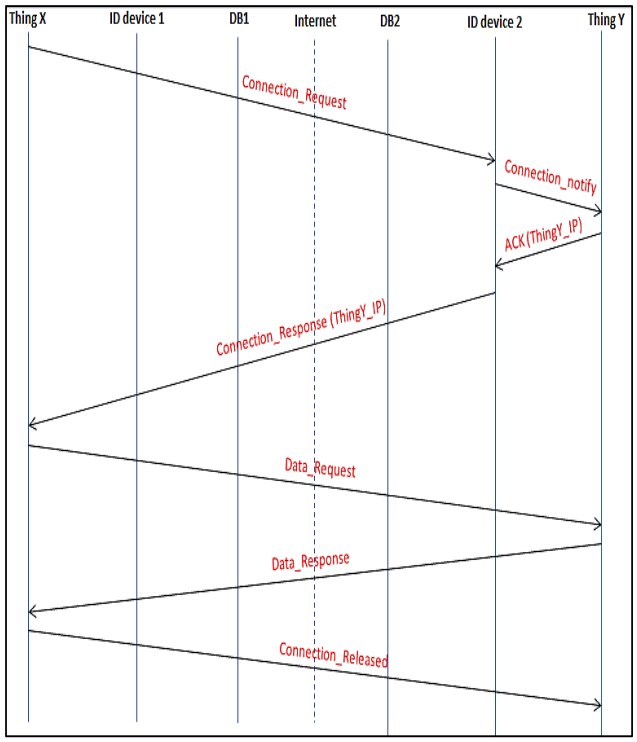

FIGURE 8. Connection scenario between two things at different locations of IoT smart home system.

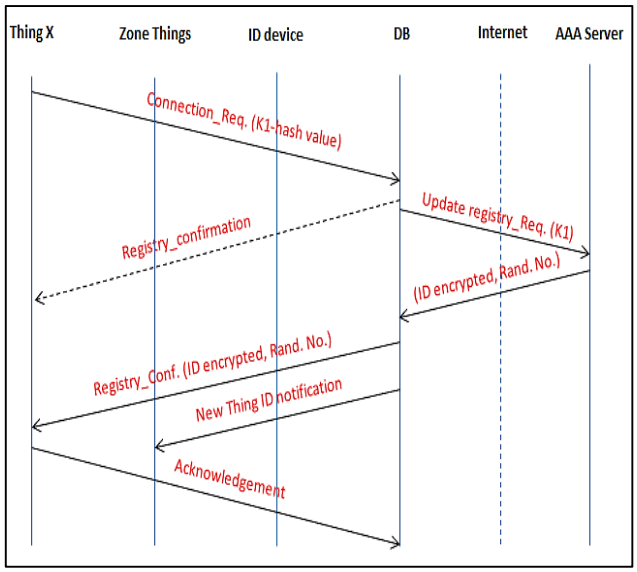

FIGURE 9. Message sequence chart of update registry scenario.

X. Otherwise, as depicted in the above registration protocol, DB sends a new registration request (e.g., update registry) onto the AAA server with a K1 hash value. Surely, the AAA server creates its equivalent hash value, checks if hash values matches, and generates a new random number. It also uses K2-key, which results from both random number and server hash values to encrypt a new Thing ID produced by it. AAA server sends a random number and new ID encrypted into thing X along with DB. Thing X decrypts ID encrypted using a random number of the server. It acknowledges that the new or updated registration protocol has been released. DB notifies all things of the zone that a new Thing ID is configured and added to this zone.

7) MQTT PROTOCOL FOR IOT SMART HOME MANAGEMENT SYSTEM

This scenario provides Message Queuing Telemetry Transport (MQTT), a published/subscribe protocol more suited for IoT smart home systems. As shown in Figure 10, the MQTT network architecture consists of device brokers as a server, subscriber things, and publisher things based on TCP connection. This protocol led to QoS, persistence, and secure communication in the IoT system. The MQTT protocol scenario has six main regions: setup TCP/IP session, subscription to a topic, data topic publishing, keep connection continuity, unsubscribing a topic, and disconnection.

The subscribers (e.g., screen, display, PCs, and mobiles) request information (topic) from other things like temperature sensors distributed at home zones. Subscribers connect to DB using CONN control signal to open TCP/IP session with DB. They subscribe with a selected topic (e.g., temperature/living room/home) to the publisher device broker by SUBSCRIBE message. The device broker itself requests an explanation and description for this topic using a TNS server, which translates it into things IPs. A connection between two or more DBs is required to grant important things talk telemetry with others over the internet in IoT smart home management. At this moment, DB exploits things IPs to request information on the subscribed topic (e.g., living room temperature) from them. Things/publishers publish data topics into DB of MQTT, which publishes data topics by PUBLISH control signal into subscribers. PING control signals are necessary to keep alive of MQTT connection for an agreed time duration between DB and subscribers. Finally, subscriber things eliminate the topic session based on UNSUBSCRIBE and DISCONN control signals, respectively. This protocol deals with QoS1level, which supports acknowledged service mode. The subscribers expect to receive multiple copies of the data topic due to QoS 1 mechanism, which retries to send the data topic again if subscribers do not receive the ACK packet [24].

C. THE PROPOSED IoT SMART HOME ARCHITECTURE DOMAINS

Figure 11 shows the proposed smart home architecture as a part of the IoT smart home management system [25], which is composed of six main domains, enabled to communicate over low range network within the home boundaries for human beneficiaries.

1) PHYSICAL SECURITY DOMAIN

The main task of the physical security system is to detect intruders, identify the incoming people types onto the home, and monitor the overall home using its security things group.

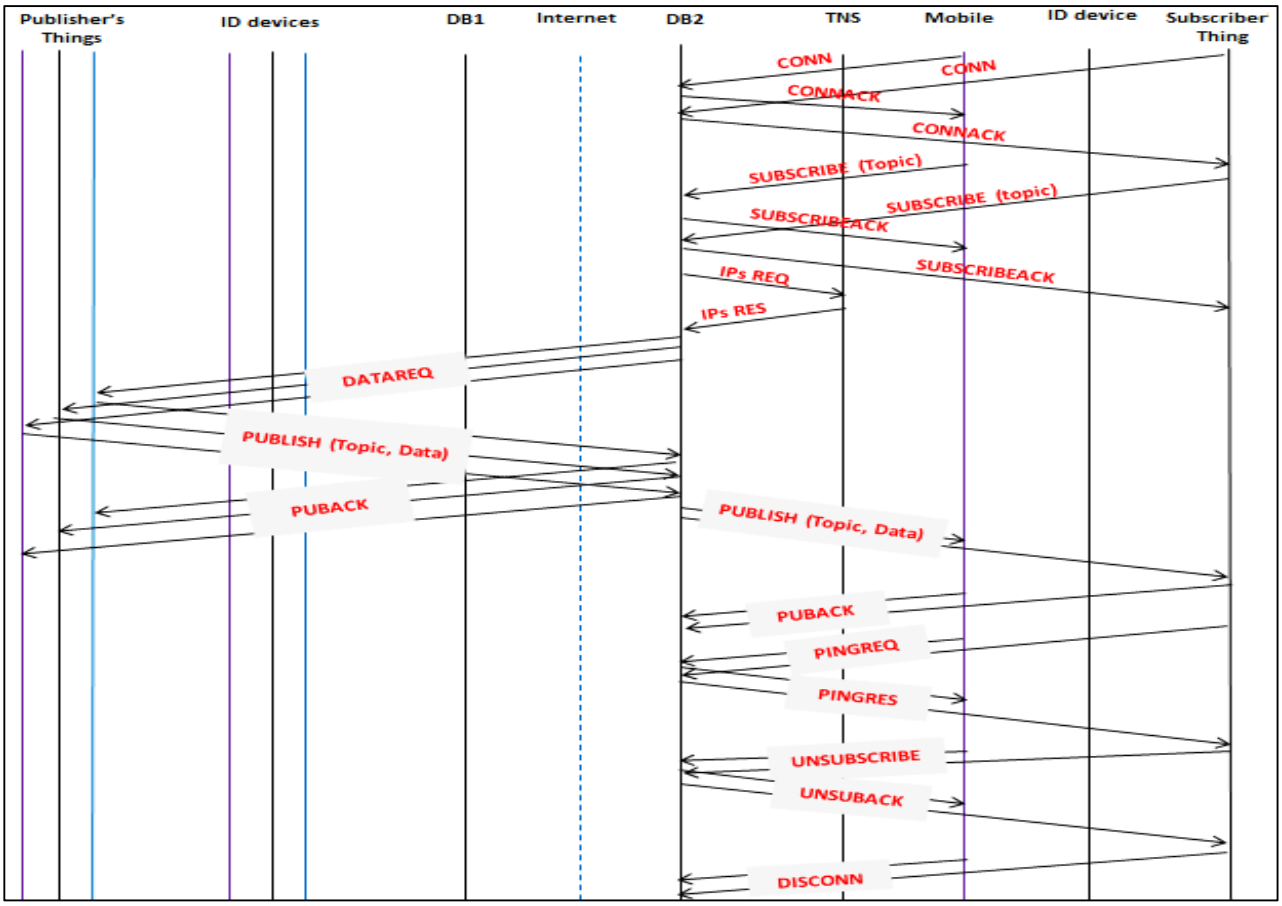

FIGURE 10. Control Packets of MQTT protocols.

The physical security domain can be typed into two main modes: intrusion mode and safe mode.

In intrusion mode, once any intruder attempts to attack the home's door and window, which are protected by both magnetic door switch and glass breaker, respectively. They activate motion detection and surveillance camera in the physical security domain. Motion detection detects any unexpected motion inside the home. It can identify if this object is a human or domestic pet. Once the intruder motion is detected, the system makes the electricity of the light bulb turned ON in the room, leading to self-automatic home defense. The surveillance camera is set in trigger mode to capture the human picture and record the important events at this moment for a duration of time. Sometimes, it can be adjusted to monitor the process for the overall home continuously at the expense of power consumption. So, the camera can identify if the detected object is an intruder or any of the household members.

When the intruder is detected, the security system sends an alarm message and an intruder photo onto the human interface point (e.g., householder mobile phone) through the internet with the help of an IoT gateway toward calling and requesting the police. In addition, it can actuate a control signal into other things in this domain, such as light or Siren alarms based on human demand.

In safe security mode, with the homeowner's presence, the householders themselves edit a private password onto the intelligent access device of the security system to access the home door. Intelligent access device attached to face recognition, which is a smart technology to permit or prevent a human from accessing the home via door locker. It guarantees that the detected object is not an intruder and then deactivates the things enablers of the intrusion security domain to save power consumption. With the householder's absence, the intelligent access device easily recognizes the housekeeper out of the home to open the house door using the door locker to execute her missions in-home at a specified time. After exceeding the time, it locks the home door and doesn't permit the housekeeper to go out. It also notifies householders about daily incoming and outgoing humans over the internet.

On the other hand, the physical security domain can integrate with the device management domain via a motion detector for controlling the home's electrical and electronic appliances.

2) HUMAN SAFETY DOMAIN

The human safety domain of the IoT smart home is concerned with serving and holding human safety at home. It also detects the data about fire, smoke, gas leakage, and toxic gases for human healthcare using the things enablers distributed at

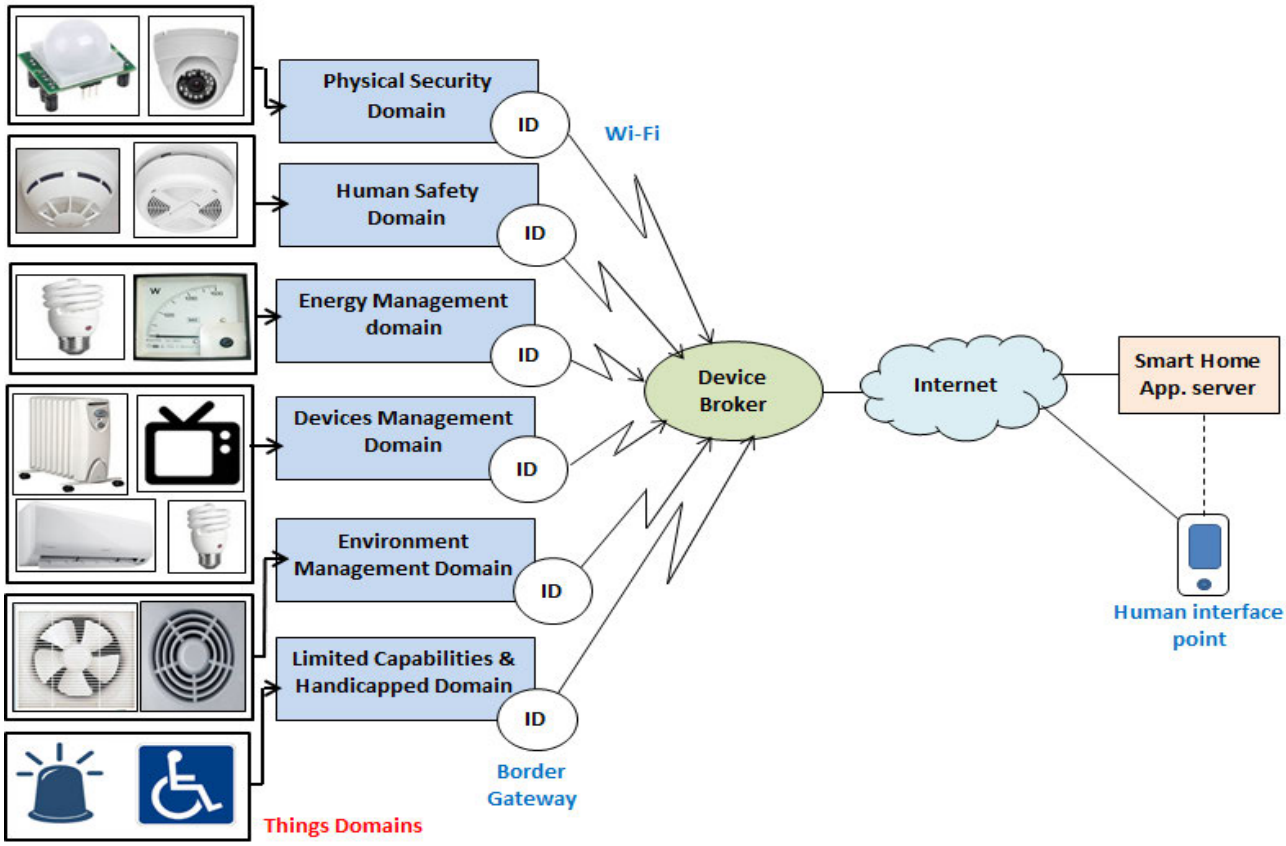

FIGURE 11. The proposed IoT smart home architecture domains [25].

home. The data is processed and analyzed to take a suitable decision for the human beneficiary, i.e., emergency message to householder interface points. The physical safety domain can be described as fire detection, smoke detection, gas leakage detection, and Toxic gas detection.

Fire detection is designed to monitor and detect the presence of fire or flame when the consumer is out of the home. It activates the fire suppression system, but deactivates a fuel line (e.g., propane and natural gas). When the fire is detected, the fire alarm is translated into several actions for home safety. Such as immediately cutting off the electricity from all electrical appliances connected to it, locking in-home doors, sending a caution message to the mobile device of the owner's home using the internet, suppressing the fire using water sprinklers, and activating the siren alarm and light indicator to call the attention of people out of the home.

Smoke detection is similar to fire detection in terms of the methodology of detection. However, it is not only sensitive to smoke gas, but also combustible gas. Smoke detection detects the smoke gas and then converts it into an alarm message to help householders avoid health troubles caused by smoking. It uses statistical analysis and medical knowledge to detect the safe limit of smoking in a closed home. If the smoke readings exceed the threshold level of safety, the smoke detection sends a warning message to a user and notifies him that he must stop smoking and that his health is in danger.

A gas leakage detection alarm is necessary to meet the increasing demand for home energy. It is designed to detect a gas leak, attempt to save energy resources (e.g., natural gas) at home, and avoid possible accidents and the riskiness caused by: Fire due to gas leaks, especially from cooking gas-fired appliances such as ovens, stoves as well as, suffocation due to gas leak in heating gas fired appliances like boilers, domestic water heaters. In this system, if the gas sensor at home detects a natural gas leak, the gas leakage detection triggers an alarm in three different faces: both light & siren alarms are activated, owner of the home receives a ''Gas Leakage'' message on his human interface points (mobile phone, Pc, lab top,...*etc.*), opening the ventilation, and operating the exhaust fan or hood to push gas leak out of the home through a window or home door.

Researches show that low-level carbon monoxide poisoning may cause depression, confusion, and memory loss. Therefore, a toxic gas detection alarm system is a must specifically for places (e.g., homes, buildings, companies, and factories) containing fuel-burning devices (gas stoves), gas heaters, and nice & warm fireplaces to trouble with ventilation or just airtight closed windows. It detects the dangerous Poisson CO_2 gas radiation in the surrounding air. It is designed to save human lives and the asphyxiation caused by it. The system is programmed to send an alert message to the subscriber about the level of CO_2 gas concentration

coming from the family home and industry or car, turn on the ventilation system, and even open the windows.

3) ENERGY MANAGEMENT DOMAIN

The energy management domain of the proposed smart home is used to control and manage the electricity of home appliances & light bulbs based on several issues such as fire alarm issues in the human safety domain, wattmeter issues, and motion detection issues in the physical security domain, and smart light issue. Integrating the above issues is needed to save energy, low power consumption, and considerably reduce CO2 emissions.

The human safety domain, specifically the fire alarm, is one of the key enablement for contribution to the energy management domain. In this paper, this emergency issue should be kept in mind to avoid any mistakes or problems caused by activating the home appliances with a fire that broke out. Thus, the home appliances and light bulbs' electricity are controlled to be OFF in the energy management system when a fire is detected.

The current sensor of the wattmeter is considered the best candidate to measure and monitor the electricity of the home appliances. It is considered one of many solutions developed the energy saving. The energy management system exploits a wattmeter to classify the loads into low, medium, and high according to their applied currents. So, it can identify the allowable threshold current of each appliance or load. If the current applied on certain appliances exceeds the detected threshold level, the system immediately turns off the electricity. It can also inform the consumer what he consumes.

In contrast to the classic lighting control used in the home, the light bulbs can be controlled by a smarter and more efficient issue called smart light. On a sunshine day, the luminance or brightness falls on the light detection of the smart light issue, which turns off the electricity of light bulbs when the measured lux exceeds the threshold level. The electricity of light is automatically switched ON in darkness (sunrise day) when a small lux of light is detected under the condition of motion detection issue of the physical security domain, which detects the human motion inside the allowable motion detection range. The motion detection issue also develops the activation and operating of some home appliances based on household demand. Otherwise, once the user is out of motion detection range, the electrical and electronic appliances, including light bulbs, are switched OFF.

The light dimmer system of the energy management domain can control the intensity of the light bulbs and fluctuate at alternating times to be compatible with other lighter appliances (e.g., TV play, laptops, smartphones,...*etc*.) and create the right atmosphere based on householder demands.

4) DEVICES MANAGEMENT DOMAIN

The devices management domain can control the home devices and appliances based on the IoT smart home concept, which empowers the connectivity among them over IoT-enabled networks. Whether direct accessing control inside the home or home away to coordinate the usage of home appliances energy, make the consumer life easier & comfort, and outperform anticipating of the people needs accurately and consistently. It is a better solution for smart home applications than the classical home automation system, providing the remote controller for controlling home appliances. In addition, it still deals with human mistakes. The manual controller unit can be damaged easily in addition to humans' bad use or disability to operate it smartly.

A smart thermostat used in Heating, Ventilating, and Air Conditioning (HVAC), uses wireless temperature & humidity monitoring in the environment management domain. It adjusts the temperature of the house, the office, or on a trip by periodically sending the report of weather status onto a smart thermostat, enabled by Wi-Fi technology. The temperature readings from the environment management domain make the smart thermostat taking suitable decisions preheating or cooling your home remotely. Accordingly, heater, air condition devices and fans are adapted to a suitable temperature at home. Wi-Fi smart thermostat is setting back the instantaneous change of temperature room status at home compared to a classical thermostat module. The householder can receive an alert email when the temperature room of the home is too low or too high, especially when a user is out of home for a long time. Another story in the device management domain is smart waking up. Once an alarm clock works to wake up the homeowner, it immediately connects to the heater for water adaptation for the user to take his shower. A clock makes order into the door locker of the car garage. It contacts into the car to configure it to be ready for operation. All these connections among these things are necessary to achieve comfortable daily life.

5) ENVIRONMENT MANAGEMENT DOMAIN

The interesting field of the smart home is the environment management domain, which makes the user feel comfortable and like to do this. The main idea of the environment management domain is to display the useful home physical environment in real-time. Such as temperature & humidity, air pollution, and sound pollution.

This domain exploits wirelessly temperature & humidity thing enabler to measure & monitor both temperature and humidity, which give important information about the weather status of the indoor or outdoor home.

World Health Organization (WHO) states that "poor Indoor Air Quality (IAQ) is being found to be a cause of childhood asthma and mental illness, or that air pollution is the single largest environmental health risk." So, a good IAQ tester helps us make our home healthier [26]. This system is installed to overcome the growing pollution, control the air pollution, and enhance healthy living. As part of the environment management domain, the air pollution monitoring system or IAQ system uses its air quality to monitor the air quality and the harmful gases (e.g., CO and CO2) compounding in the surrounding air. Such as, some Volatile

Organic Compounds (VOCs) cause eye irritation, headache, kidney disasters, difficulty breathing, shortness of breath, skin damage, nervous disasters, depression, …., *etc*.

In contrast, monitoring and detecting the dust particles in the air causing air pollution is considered one of the important methodologies for air pollution detection. In addition, pressure, oxygen, and carbon dioxide parameters should be monitored and displayed on screens, PCs, or mobiles to follow up, manage, and solve the in-home environment issues.

The domain displays the results and activates the ventilation or fans according to the concentration air quality level.

Least, but not last, the sound monitoring system is proposed in this paper to detect sound pollution in the indoor environment area. Such electrical appliances that have sound nature during their working should be monitored in an efficient way to make sure if these appliances are still running probably or not. Furthermore, it can remotely help the householder to detect if any of the house rooms are noisy or quiet to check the behavior of kids to cry babies at home. If the noise field is detected, this domain allows subscribers to know about and monitor this issue over the internet via their mobile phones.

6) LIMITED CAPABILITIES AND HANDICAPPED DOMAIN

In the past, the help of limited capabilities and handicapped people was limited and bounded by a manual control module attached with wireless communication and ON/OFF commands to control domestic devices such as fridge, TV, washing, cooking, and cleaning machines, as well as electronic devices such as motors, water pumps to push water onto house planet, and window. The controller has laser-engraved backlit buttons designed for the special needs of elderly users and a Braille interface for limited vision persons. So, with the limited capabilities, people make more efforts to learn the Braille method and train the manual controller use, which is opposite to the concept of easy & comfortable living. Some people with limited capabilities can't be able to use this controller unit, specifically those with a disability of hand or hand paralysis. Accordingly, disabled people need a smart and efficient system like the IoT smart home, enabling them to overcome the lack of their capabilities and handicaps toward executing missions or interesting works and habits in our lives.

Surely, the motion detection of the security domain of the proposed IoT smart home can help elderly and disabled persons automatically to control or switch ON the electricity of light bulbs and home appliances at the place of the presence of the elderly.

The limited capabilities and handicapped domain of IoT smart home improvements empower the wheelchair or limited vision stick of special needs to avoid obstacles and make their movements easy and simple. The range finder sensor develops the stick to detect any obstacles which face limited vision persons and opposes their ways. It was developed by wireless technology to connect to other things in the proposed smart home system through the internet. Smart home Appl. server sends sound alarm or sound message to the limited vision persons to tell him that "Obstacle in your way."

The integration among the previous things domains of IoT smart home is more suited for the elderly and limited capabilities instead of using the classical controller unit or even the electrical wheelchair specified for special capabilities missions. Controlling light bulbs and home appliances is one of many IoT smart home benefits for disabled persons and the elderly without dependency on another person or nurse, needing a chair, and moving from the bed into these appliances. These domains are powered by sound and light indicators as alarm actuators for limited vision and hard of hearing persons, respectively. All the text warning messages and controller commands of the mobile App. are translated into recorded messages, which are outcomes through the mobile phone speaker of disabled persons.

IV. Io T SMART HOME DESIGN

This section describes the design of the six main scenarios "domains" in the IoT smart home networks of Figure 11, which consists of four main stages: ID device, set of Things (sensors), device broker, and the Web server and Human Interface point.

A. ID DEVICE

The intelligent device of the IoT smart home system has three main functions. Firstly, it acts as a connection point of a sensor (e.g., things). It is responsible for connection among things included in it. Therefore, it is considered a controller or the brain of all sensors connected to it. ID device controls and manages all tasks and missions of the sensors at IoT smart home systems. Such as controlling the sensors group of the security domain to extract useful information (e.g., picture of an object in different zones at home) needed for the human beneficiary. Finally, an ID device can be designed as a network interface point, which coordinates the communication among things and DB gateway in IoT smart home system. Therefore, its capabilities are exploited to monitor and collect things data and remotely forward it to the device broker.

ID device consists of four main components: power supply (e.g., battery or energy harvester), processor (e.g., MCU) for smart coordinating and managing the sensed data, and wireless communication node (e.g., Wi-Fi, ZigBee, and low energy Bluetooth BLE), which is one of the key enablement for communication in IoT smart home system.

ID device classifies things into three basic types to detect the connection methodology easily according to the system design demands. First, it allows the connection among associated family and complementary things. It mitigates the connection among the non-complementary things.

Such as the security domain of the smart home system, PIR motion detection sends command signals to other associated PIR families to make the same detection function at different parts of the same zone. For example, the PIR motion sensor performs its mission after waiting for a connection from the complementary door locker thing while an intruder comes

home. The camera thing needs data about the object from the complementary PIR motion thing to capture a photo of it and then identify whether intruder or a householder. Simply, thing X can't operate in the IoT smart home system without a complementary things connection. Surely, the PIR motion thing can't connect to the non-complementary things like smoke detector thing of the human safety domain because there is no relation between them.

B. THINGS

Things are characterized as sensors for physical parameters interaction. The paper pilot will establish and install things group of four main domains, compound IoT smart home system as:

1) PHYSICAL SECURITY THINGS

Things of the physical security domain consist of safe things mode and intrusion things mode. All things of both security modes can be attached to the ID device physically.

In safe mode, the domain contains a door locker and intelligent access device.

Door Locker acts as an actuator that controls the opening and closing of the home door with the help of a control relay. Essentially, it waits for a response from the ID device for operation based on the results of the access security device of the security system.

Intelligent access device can represent an RFID reader with its tag. It follows a short radio range technology that enables the communication between the device and its tag for near field communication (NFC). The RFID device is a very short-range wireless communication technology for developing IoT applications. For example, when a subscriber passes through the front of the home door, the intelligent access RFID device reads the control command from the user's tags. Then, it immediately sends a response signal to the ID device to decide what to do [27].

The intrusion mode has three different things: A magnetic door switch, a Glass breaker sensor, a PIR motion detector, and Camera surveillance.

Magnetic door switch is an electronic tool that aims to verify the registration of householders. It is used for alarming doors in a secure home when an intruder or unauthenticated user opens the closed contact between their terminals. It contains two main parts, the magnet and switch, with two wires connected to a suitable power supply. Magnet part mounts on a door or window. At the same time, the switch lies on the frame. In the normal case, at a closed door, the magnet and switch are in close contact with each other. In contrast, when the door is opened by an intruder, the distance between magnetic sensor parts increases.

Glass Breaker sensor is mounted on the home window for detecting glass breaks. Both acoustic and shock detection techniques enable glass breaker sensors to detect the sound and vibration of the breaking glass, respectively [28].

PIR Motion Detector Passive Infrared (PIR) motion detector is an electronic device that is used to detect the presence of human movement. It uses its pyro electric or PIR to detect the IR wavelength (9-10Micro-meters) of the thermal energy emitted from the human begins when he is close to the sensor. It triggers this detection as input into the ID device. The PIR motion sensor is more suited for intruder's motion detection until 7m range than other motion detector sensors, i.e., ultrasonic sensor, IR sensor, and laser diode and photoresistor. In fact, PIR finds a problem in distinguishing between pets and humans. The PIR sensor can be calibrated by setting a higher sensitivity threshold or directing its lens to the room floor. Nowadays, the advanced PIR motion sensor is released to recognize the human from any other being. The digital output of the PIR sensor generates a high voltage (logic 1) if the intruder motion is detected. In contrast, it doesn't a generate low voltage (logic 0) onto the ID device when no intruder exists [29].

Camera as surveillance is mounted on the different zones at home (e.g., rooms) to trigger video recording & displaying and monitoring the motion detection of the physical security domain. Before camera operation, it should be defined and setup on the ID device by software programming. The camera makes the security domain more commercial, reality, and reliable, but at the expense of cost and power consumption.

The magnetic door switch and glass breaker sensor recognize that something is trying to break the door and window to enter the house. It connects to the PIR motion detector through an ID device to notify it that some object is in the home. Motion detection detects the object-type information and sends it to camera surveillance along with an ID device. Surely, the camera captures the object or intruder photo and forwards it into the ID device, which turns the light bulbs ON as one of the intrusion defense solutions. While in safe mode, the ID device sends a control signal into the control relay, connected to the door locks to access the home or not.

2) HUMAN SAFETY THINGS

Smoke gas, fire, neutral gas, and toxic CO gas sensors describe the things group of the human safety domain of IoT smart home systems.

Smoke Gas Sensor is concerned with measuring and detecting smoke. Its output voltage readings are changed according to the variation of the sensed smoke gas quantity. The smoke sensor output value is directly proportional to the quantity of smoke. The greater the smoke quantity exposed, the higher its output voltage and vice versa. The degree of smoke sensor sensitivity can be adjusted via a built-in potentiometer.

Fire Sensor has an IR detector to monitor the flame or the fire with a 60° detection angle, and detection distance ranges from 20Cm to 100Cm. The sensitivity and accuracy of the flame sensor are often higher than a smoke or heat detector. However, it hasn't a direct notification or confirmation to deal with control systems.

Natural Gas Sensor is mainly applied to gas leakage detection alarm system at home, industry, office, company, *etc*. The gas sensor is sensitive to natural gas or Liquefied Natural Gas (LNG), Propane, Butane, Methane, and Liquefied Petroleum Gas (LPG). However, it is not sensitive to clean air. Thus, the gas leakage detection system is not affected by the presence of air concentration in measuring these gases. The sensitive element of the neutral gas sensor is made from the Tin Dioxide (SnO_2) layer, called the sensitive resistance element that is changed or converted with the variation of the concentration gas. The more sensitivity to small changes in the gas concentration makes it a good pilot for detecting gas leaks down to 100 ppm. The sensor is affected by the surrounding temperature and humidity [30], [31].

The natural gas sensor supports both analog and digital output modes. The digital output mode is more suited to detect the gas leak. It triggers an alarm system if the gas leaks or if not using High or Low. The analog output mode measures the volume of natural gas leakage, which ranges from 0-1000 with a specific ppm unit. In clear air, the sensor detects the gas volume between 40-100ppm. In comparison, the measuring gas value exceeds 800ppm in gas leak status.

ID device collaborates and monitors the things group data (e.g., smoke, fire, and LNP) to keep and maintain human safety at home. In case unsafe home, it pushes a siren alarm and disconnects the electricity from light bulbs.

3) ENERGY MANAGEMENT THINGS

The nature of this domain requires a current sensor, control relay, and Digital light sensor as a part of a pilot to develop the functionality of the energy management domain, such as controlling the electricity of home appliances.

AC current sensor measures the real currents applied to the electrical and electronics things in IoT smart home system. It should be characterized and designed to accommodate all types of home appliances and things in the system. Such as, AC current sensor has a maximum current range up to 30A and high accuracy. The current sensor output per volt is converted into the current value with the help of the ID device.

Control Relay acts as the actuating process mainly used to isolate the electricity from the electrical and electronic home appliances and vice versa. Therefore, it is one of the key enablement of the energy management domain. Usually, the schematic circuit diagram of a relay consists of five main pins: Normally Open (NO) pin, Normally Closed (NC) pin, common pin, and two pins of the relay coil. Generally, both supply voltage and ground pins are connected to the ID device. For example, if the light switches ON, the common pin is connected to the NC pin. In contrast, the light is switched off or isolated to the electricity when the common pin is connected to the NO pin.

Advanced digital light sensor precisely measures luminance in diverse lighting conditions compared to low-cost CdS cells. It can detect exact wide light ranges (0.1 - 40,000 Lux) on the fly. It uses its digital ambient light sensor chip, called light to digital converter from Texas optoelectronics, to convert the incident light to a digital output signal. The light meter contains both infrared and full spectrum diodes, which enable the sensor to detect separately sense infrared and full-spectrum or human-visible light [32].

Control relay developed by ID device and wattmeter to control the electricity connection and save the energy consumption of electrical and electronic home appliances. It is designed with an ID device between electrical home appliances and electricity. The wattmeter can be represented as a current sensor, which detects the current of the home loads for monitoring the energy consumption in the IoT smart home system. AC current sensor sends the load current into the ID device, which stores it to know what home appliances are consumed. Based on the energy consumption measurements of home things, the ID device can energize the relay to be converted from NO into NC and vice versa. Digital light sensor interfaces to ID devices to detect the light illumination over a complete day. The quantity of light intensity is an important issue for controlling the home light bulbs. ID device uses a control relay to turn the light bulbs on when the light intensity is high and vice versa.

4) ENVIRONMENT MANAGEMENT THINGS

Air quality, temperature, humidity, and sound sensors are things that describe the environment management domain in IoT smart home systems.

The main gas detected in the *air quality sensor* is carbon monoxide, alcohol, acetone, thinner, formaldehyde, and other slightly toxic gases. It is designed for IAQ testing. It is characterized by low power consumption, long life, high stability, and high sensitivity. It applies to many applications, such as refreshing air modules in air conditioners and Air purifiers [33]. Air quality sensors can't describe target gases' concentrations quantitatively. Howver, it's still good enough to be used to describe qualitative air quality. Its analog output readings ranged from 0 to about 65000. The low output readings (0-3199) represent the low pollution or fresh air. In contrast, the high output values (11200 and up) describe very high pollution [34].

Temperature & Humidity Sensor is considered the good choice for more temperature readings ($-40°C$ to $125°C$) with high accuracy ($\pm 0.5°C$) and 0%-100% humidity readings with 2-5% accuracy. Simply, the digital temperature and humidity module interface to the ID device to inform the user about the surrounding air status at home and helps air condition to improve the increase of temperature & humidity degrees. The sensor checks and confirms the operation status of the air condition device.

Microphone Sound Sensor is digitally used to detect the sound intensity of the environment or sound pollution in a closed building, company, or home. It has a high sensitivity of sound strength, which is adjusted by the potentiometer. ID device integrates among environment management domain things for monitoring the pollution level at home. For

TABLE 1. Experiment lab things distribution over the home zones.

Location/nodes	KITCHEN	BEDROOM	LIVING	RECEPTION	GARAGE
Smoke-node	---	---	X	X	---
PIR-node	---	X	X	X	---
Power controller-node	X	X	X	X	X
Fire-node	X	---	---	---	---
Gas leakage-node	X	---	---	---	---
Light detector-node	---	X	X	X	---
CO gas-node	---	---	---	---	X
Temperature & Humidity-node	---	X	X	X	---

TABLE 2. Lab model things connections at different home zones.

Pilot zones	KITCHEN		BEDROOM	LIVING		RECEPTION		GARAGE
Thing-nodes Sender/Receiver	LNG gas detector	Power Controller	Power Controller	Smoke	Power Controller	Smoke	Power Controller	Power Controller
Smoke-node	Yes	---	Yes	---	Yes	---	Yes	---
PIR-node	---	---	Yes	---	Yes	---	Yes	---
Fire-node	---	---	Yes	Yes	---	---	Yes	---
Gas leakage-node	---	Yes	---	---	---	---	---	---
Light detector-node	---	---	Yes	---	Yes	---	Yes	---
CO gas-node	---	---	---	---	---	---		Yes
Temperature & Humidity-node	---	---	Yes	---	Yes	---	Yes	---

instance, sound pollution and air pollution. It displays the home temperature and humidity measurements for weather news recovery as a service demanded by the homeowner. ID device connects to a sound detector to identify if the home environment is quiet or noisy.

C. DEVICE BROKER

A broker is a gateway that interfaces between the things network on one side and the internet and web sever networks on the other side. It enables the things in the sensory field domain to communicate with the smart home application servers through the internet.

D. WEB SERVER AND HUMAN INTERFACE POINT

Both types of data (e.g., event-driven data and payload exchange) are aggregated into the cloud, which is responsible for processing and monitoring the incoming data from smart home buildings.

The human interface point is a collection of all emergency cases and rescues triggered by individuals or various buildings in the smart home system. It is used to monitor and actuate all urgent & risky cases involved in the surrounding environment of the system buildings. For instance, air pollution, fire detection, and gas leakage detection at buildings.

The Web server handles the smart home data. Then, the statistical analysis is generated to give the possibility of the human interface point to monitor the status of the house remotely. Accordingly, it can be achieved the highest safety rates in smart home buildings.

V. THE IMPLEMENTED IOT SMART HOME PILOT MODEL

This paper implements a part of the proposed smart home system as a pilot model to prove the concept and test the above-proposed scenarios. The experiment pilot landscape can be modeled into five distinct zones: kitchen, Bedroom, reception, Living, and garage. Table 1 lists the Places of the lab things of the pilot domains, being at different home zones.

The connection methodology of the proposed system design scenario subjects to the distributions of the things, labeled nodes overall home infrastructure as in Table 2. The nodes are grouped into heterogeneous networks or scenarios, connected individually through a protocol governing the scenario objective. These groups are typed according to the nature of contents (nodes) and their tasks. Node is a simple element of the scenario. It contains a wireless node (e.g., Wi-Fi) for connectivity among other nodes and sensors for monitoring and observing environmental data at home. Node is established by the ESP8266 MCU NODE module and sensors. The ESP8266 module was designed to interface or deal with sensors within monitored data using GPIO pins. ESP8266 module is divided into controller units and Wi-Fi parts. The protocol scenario functionality is implemented using the control unit, which can be programmed using Lua programming or Arduino IDE. On the other side, the Wi-Fi part of ESP8266 is responsible for talking with other nodes in the same scenario [35].

The communication among Thing-nodes of system design scenarios follows a reliable TCP/IP connection under the connectivity of the Wi-Fi router. TCP connection has three consecutive connection statuses: connection setup, data transmission, and connection release. In TCP/IP connection setup, both sender/client and receiver/server thing-nodes are connected using different known IP addresses and ports in the wireless router domain. The sender node should use client.connect (IP, port#) function to open a session with the peer server node. The handshaking of the data transmission process between peer Thing-nodes will be activated by two major functions, *client.print(data)* and *client.readStringUntil('\r')*. Each Thing-node can send data into another Thing-node (receiver/server) included in the scenario using the first function and waits ACK MSG via the second function, and vice versa. The data to be sent is called message format <MSG code, Thing-node#, Thing-node value>, and is constructed from three indices; MSG control code, Thing-node number, and Thing-node sensor value. MSG control code describes the reason or status of the communication between two Thing-nodes as in Table 3. Usually, the scheduling scenarios will be developed by PUT

TABLE 3. Description of MSG code index as part of message format.

Message code	NAME	STATUS
0	PUT ON	Node requires data from another node
1	PUT OFF	**Node needs stop sending data from another node**
2	ACK	Acknowledgement as replay to node
3	Set ON	Node sends message to set ON siren alarm or appliances attached to other node
4	Set OFF	Node sends message to set OFF siren alarm or appliances attached to other node

TABLE 4. Description of IoT smart home system scenarios [37].

Scenario No.	SCENARIO NODES	OPERATION MODE	DESCRIPTION
1	Gas leakage, smoke, and power controller	Emergency or normal mode	Emergency control upon natural gas leakage
2	Light detector, PIR motion sensor, and power controller	Emergency and normal mode	Energy management. i.e. ON/OFF electricity of home bulbs
3	Fire, smoke, and power controller	Emergency or normal mode	Emergency control upon natural Fire detection
4	Carbon monoxide CO and power controller	Emergency mode	Pollution reduction upon CO gas detection
5	Temperature & Humidity and power controller	Emergency mode	Air conditioning control
6	PIR motion sensor and power controller	Emergency mode	Increase or adjust light upon human presence

ON and PUT OFF MSG codes. At the same time, Set-ON and Set OFF MSG codes are applicable for emergency scenarios. Thing-node can be identified by the second index of the message format, called the Thing-node number. The last index of message format represents the sensed data value of the sensor attached with Thing-node. Finally, the TCP/IP session is disconnected by *client.stop()* function from Thing-node sender.

Table 4 describes the proposed six scenarios, yielding a smart home system design [36]. These scenarios are operated under normal and or emergency modes. These scenarios are placed at home zones as in Table 5. The numbers included in the Table, represent the scenario number. Some scenarios can be implemented in the same home zone, like scenarios 2 and 5 scenarios, and also, they are repeated in different home zones as scenarios 2 and 5. While Scenario 4 is only suited to the home garage. On the other side, scenarios 1 and 3 should be placed in different zones. i.e., scenario 1 tracks kitchen and reception zones.

Finally, the IoT smart home lab model consists of six main scenarios. Any scenario is composed of an ESP8266 Node attached to a group of connected IoT sensors and actuators using Wi-Fi technology. The six main scenarios "networks"

TABLE 5. Mapping of six scenarios nodes over smart home landscape.

Location/ nodes	KITCHEN	BEDROOM	LIVING	RECEPTION	GARAGE
Smoke-node	---	---	3	1	---
PIR-node	---	2 6	2	2	---
Power controller-node	1 3	2 5 6	2 5 3	1 2 5	4
Fire-node	3	---	---	---	---
Gas leakage-node	1	---	---	---	---
Light detector-node	---	2	2	2	---
CO gas-node	---	---	---	---	4
Temperature & Humidity-node	---	5	5	5	---

in the pilot model are programmed using ARDUINO C. Each scenario has its objective, process and algorithm, and the state diagram is as follows:

A. EMERGENCY CONTROL UPON GAS LEAKAGE

1) OBJECTIVES

The scenario aims to control power upon gas leakage, close follow up the smoke with gas leakage environment (if any), activate the alarm of zone 2 upon smoke according to gas leakage, and finally activate the alarm of zone 1 upon gas leakage without smoke. This scenario can operate in normal or emergency mode.

2) PROCESS WITH ALGORITHM

As seen in Figure 12, the generic block diagram states the current process stages of this scenario, which are composed of three kinds of Things-nodes, i.e., Gas leakage, smoke, and Power controller thing-nodes. In this Figure, explaination of the cooperation among these things to score the scenario goals. Gas leakage actuates alarm at area 1(kitchen) when gas leakage is detected. It sends data to the power controller to power OFF the electricity of light and appliances in the same zone. At the same moment, the smoke thing-node monitors the smoke in area 2 (reception). Although smoke is located in the second area, it talks into the LNG gas leakage thing-node to continuously follow the gas leakage at the first area plus notifying area 2 that natural gas is leaked at area 1 and running alarm. Smoke attracts attention for smoke being at area 2 through siren alarm activation and turns ON the electricity of the light bulb.

The paper is concerned with studying three of the six system scenarios mentioned above. These scenarios can be analyzed and described in terms of objective, process & algorithm, and scenario state diagram for the following scenarios:

3) STATE DIAGRAM

As shown in Figure 13, the state diagram describes the overall procedures protocol of scenario A. Each thing-node of this scenario includes a set of states, such as Sense, Send,

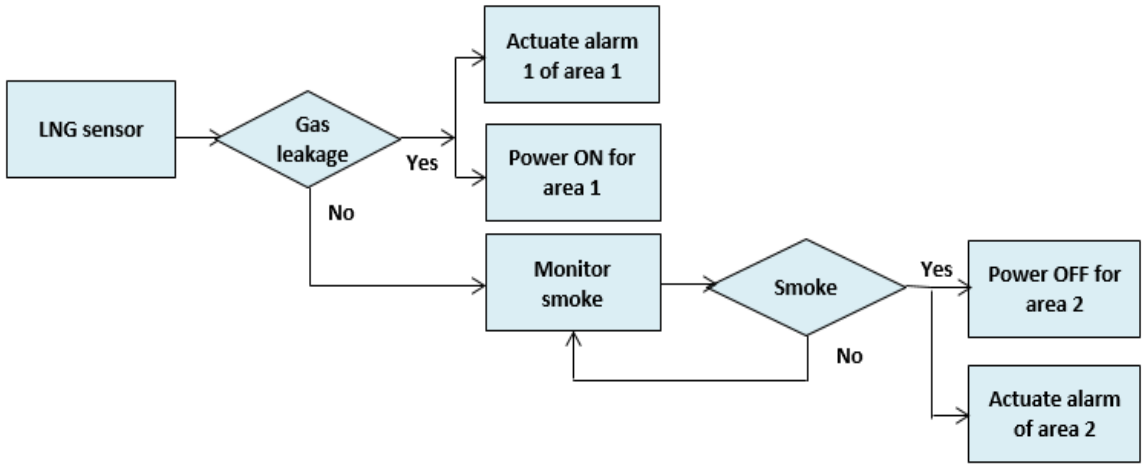

FIGURE 12. Process and algorithm of emergency control upon gas leakage scenario.

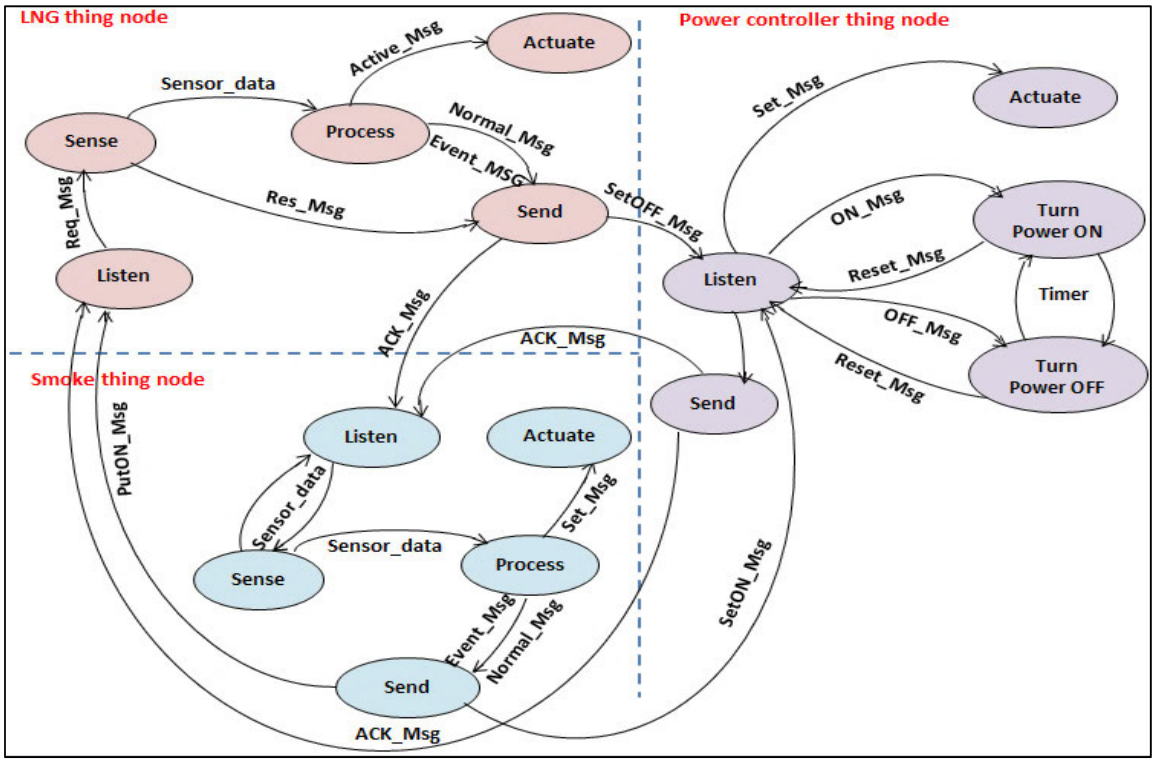

FIGURE 13. Finite state machine of scenario A.

Listen, process, and Actuate. A transition does from one state to another inside thing-node or in the scenario level via messages.

Listen and Send process states represent the communication among Thing-nodes over scenario A. In an emergency case, a Set-OFF message is sent from Send-state of LNG thing-node to Listen-state of power controller-thing-node to turn OFF the power, in addition, to operating alarm in the same zone. Send-state of Smoke sends a Set-ON message into the Listen-state of the power controller to turn ON the light via Turn-On-state or even activate alarm through Actuate-state. In normal operation mode, only communication occurs between LNG-node and smoke-node. Smoke-node exploits its Send-state, requesting gas data from the Listen-state of LNG-node by PUT-ON message. On the other side, LNG sends back ACK message, carrying LNG gas data resulting in smoke.

The initial state of the thing-node, called the Sense-state, monitors the incoming information sensed from the sensor. For example, the sense-state of LNG-node and smoke-node is

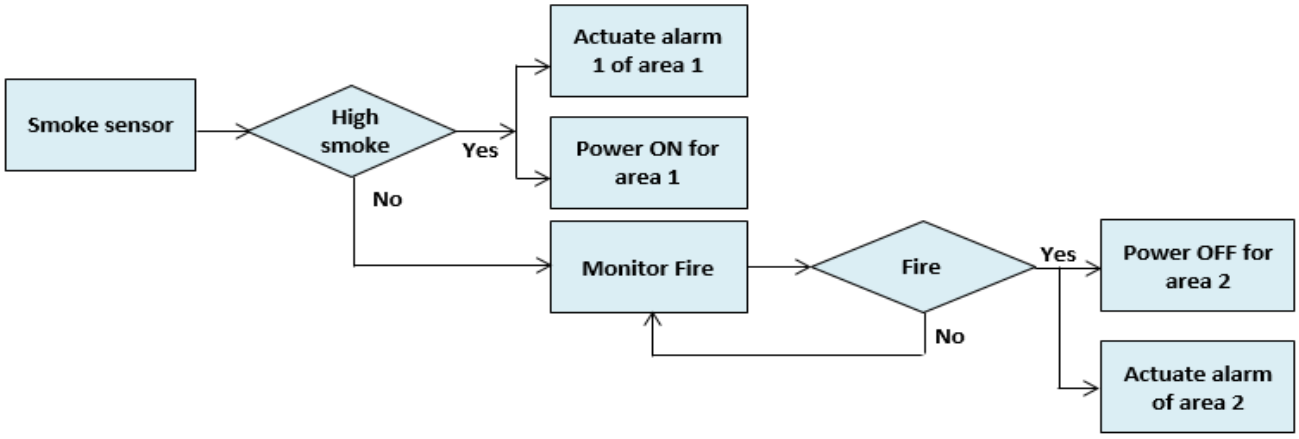

FIGURE 14. Block diagram of the process scenario.

used to continuously detect gas and smoke data, respectively. Actuate state, called the sink-state, is used to actuate alarm based on action taken from the Process-state in the same node of a certain area. It describes the real outcomes produced from the node.

The Process-state is a coordinator state to manage and control the procedures of thing-node in the scenario. Based on thing-nodes interaction with the surrounding environment, it detects whether the sensed data (e.g., gas leakage or smoke) exceeds the threshold level or not. Therefore, Process-state can easily map between emergency and normal scenario modes. It uses Event and/or Normal messages to detect what type of data messages will be sent at Send-state. Each node can control the operation of the Actuate-state using Activate message.

B. EMERGENCY CONTROL UPON FIRE DETECTION

1) OBJECTIVES

This type of scenario relies on urgent data incoming from smoke and fire sensor nodes to control emergencies and serves the factors of home safety. The power controller responds to these data, actuates alarms, and operates other useful home appliances able to prevent fire and smoke. For instance, sprinklers, fans, and air ventilation.

2) PROCESS AND ALGORITHM

Figure 14 presents the generic block diagram of this scenario. The smoke node is located in zone 1 at home(e.g., living room). If the smoking area exceeds the threshold level, the power controller node in the same area performs alarming and set ON light bulbs. The protocol scenario monitors the fire on the other side of the kitchen. It also monitors the smoke status through the connectivity between the fire and smoke node. Fire sends request data into smoke, which acknowledges its data into it. In case of fire is triggered in the kitchen, all kitchen appliances are OFF state, the siren alarm is activated, and the power controller node sets up water sprinklers.

3) STATE DIGARM

The state diagram of the scenario describes the detailed functionality procedures of this scenario and explains the ideology of communication among scenario nodes, as in Figure 15. The execution steps of the protocol procedures as the same as in scenario A. these procedures can be summarized as the following states: actuate, process, send, listen, and sense states. The sense-state is performed by smoke and fire nodes in different zones. For example, in normal mode, the fire node needs data about smoke status in another zone. Thus, the fire is in send-state and waits for the response from the smoke node through listen state. On the other hand, smoke exploits the listen-state to receive data from fire and then uses send-state to transmit its data into the fire node. In interrupt mode, the process-state detects the mode type of scenario. It is useful for fire and smoke nodes and to decide what will be done if the critical smoke and fire data has happened. It manages the ordering of overall states in this protocol. In this case, the Process-state push and aligns send state for both nodes toward the power controller node. Both nodes wait for acknowledgment from the power controller node using listen-state. Process-state also enables both nodes to actuate an alarm. Based on the incoming critical data, the power controller node actuates a siren alarm or even controls home appliances in its location. Such as making power ON/OFF appliances or bulbs according to scenario objectives using ON-state and OFF-state, respectively. It exploits its Send-state to acknowledge that critical data are sent and recognized successfully.

C. ENERGY MANAGEMENT UPON HUMAN PRESENCE

1) OBJECTIVES

This scenario is looking to control the power of home appliances upon human presence, close to monitoring the light intensity level to manage power electricity in the same zone and save energy consumption. It is designed to operate in normal and emergency modes.

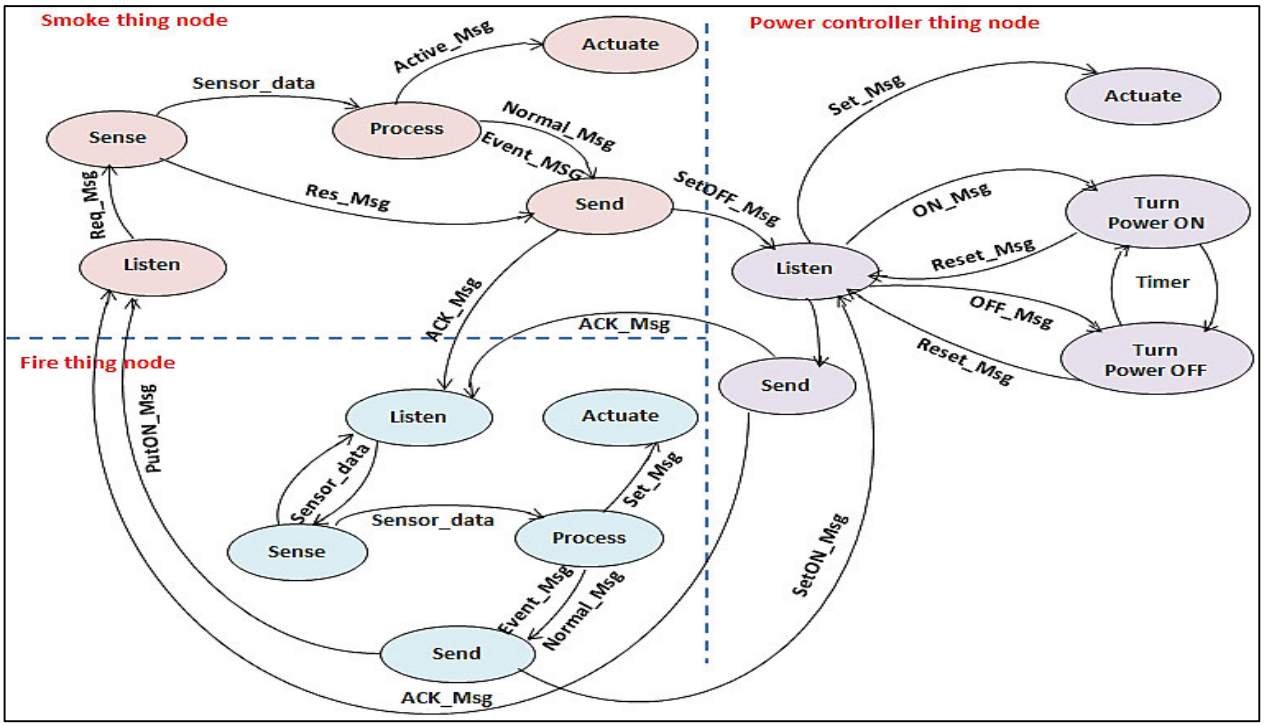

FIGURE 15. State diagram of scenario B.

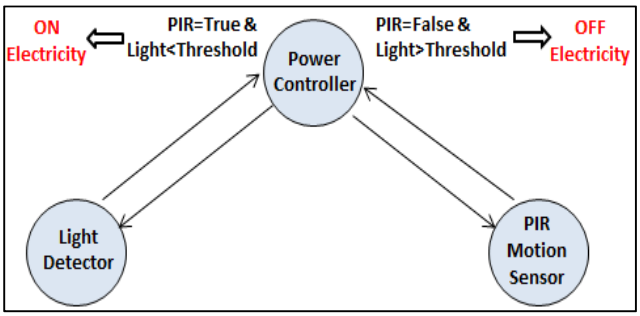

FIGURE 16. Thing-nodes of Energy management scenario.

2) PROCESS AND ALGORITHM

The scenario includes a power controller, light intensity detector, and PIR motion sensor thing-nodes, as in Figure 16. There is no connection between PIR and light detector thing-nodes. However, each of them will be established to the push power controller to be turned ON/OFF electricity of light in the same zone. As seen in Figure 17, the Power controller thing-node takes its decision based on historical information from both PIR and light detector. In other words, continuous monitoring for light intensity level, while PIR triggered data based on motion event. A light bulb is turned ON when motion is detected from the PIR node and a low light intensity level. In contrast, OFF electricity happens if there is no human presence with a high level of light intensity.

3) STATE DIAGRAM

Figure 18 explains the detailed procedures of scenario functionality in normal and emergency operation modes. The scenario protocol starts from the light detector node, which monitors the level of light intensity at zone X. It sends the sensed data continuously, whether in normal or emergency mode, into the power controller node. At the same time, the PIR motion node monitors the absence or presence of human motion. If the motion is detected, namely emergency mode, the Process-state triggers Send-state to transmit SETON_MSG data into the power controller node. The power Controller node receives both the level of light intensity and the motion data via Listen state. As well, as data sent is reached its process-state, it sends back ACK immediately into other nodes. This state compares the incoming data and the threshold reference data to decide if any of the two conditions are achieved as in Figure 16 to make the suitable state of light bulbs "Turn On/ turn OFF states." After that, the state of bulbs changes from ON to OFF and vice versa. After that, the PIR and light intensity nodes receive ACK messages and rebuild the scenario protocol loop again by Restart message.

D. POLLUTION REDUCTION UPON CO GAS DETECTION

1) OBJECTIVES

The main object of the scenario is to increase fresh air purity at home and avoid the pollution and CO gas suffocation resulting from automobile exhaust in the garage by controlling air ventilation.

2) PROCESS AND ALGORITHM

Usually, this type of scenario protocol is suited only for emergency mode, as in air conditioning control and adjusting

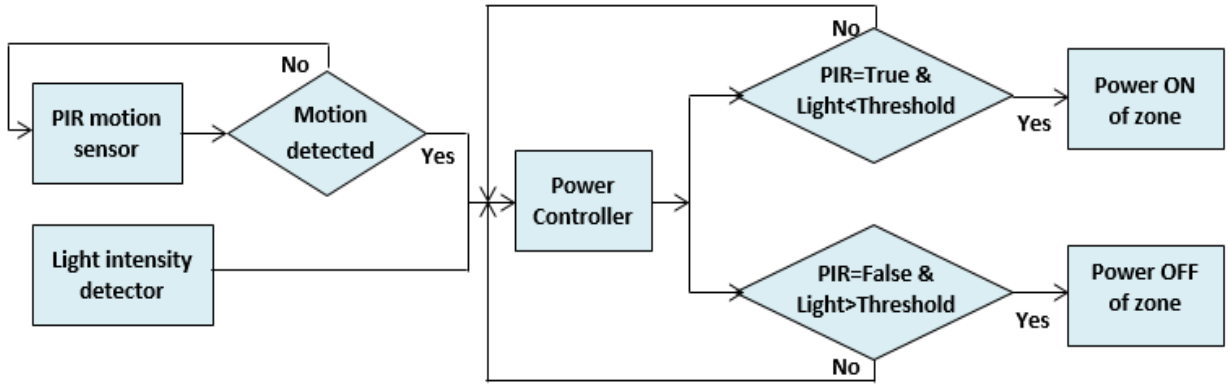

FIGURE 17. Block diagram of energy management scenario protocol.

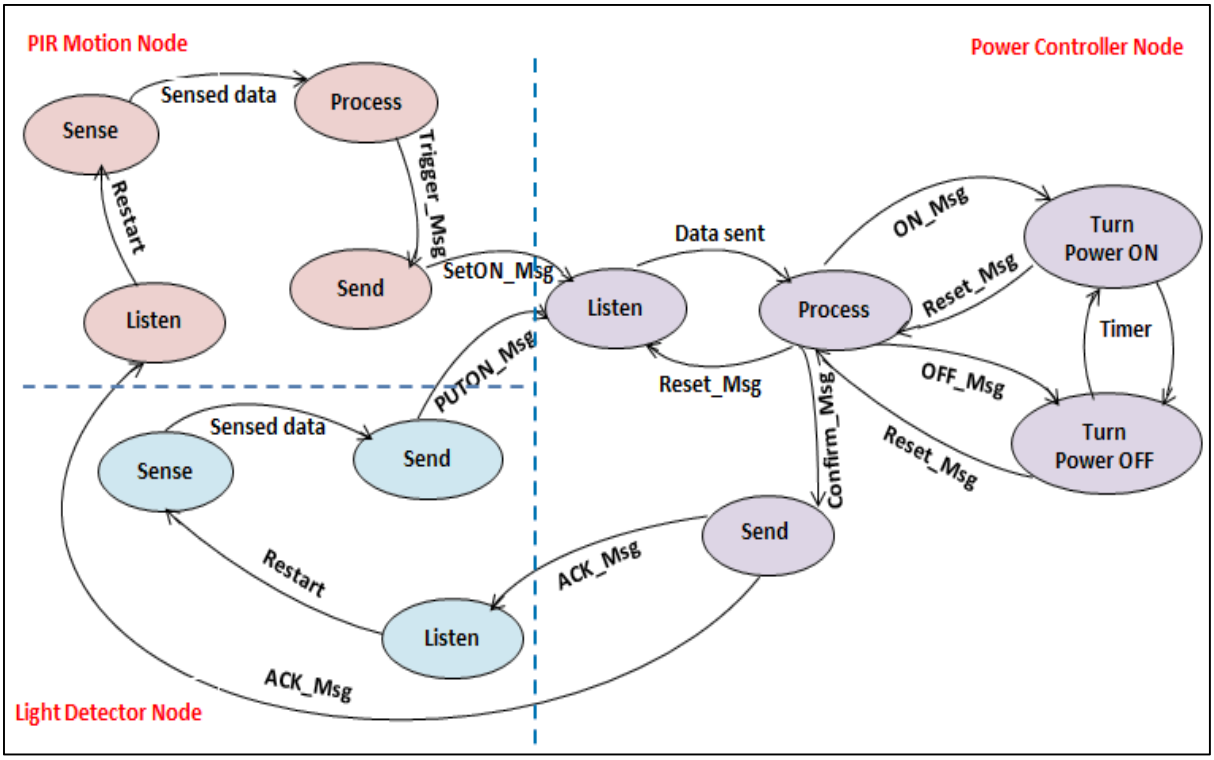

FIGURE 18. Energy management upon human presence state machine.

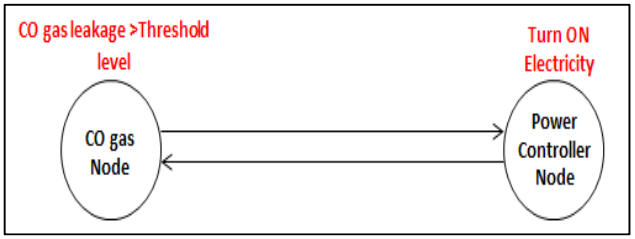

FIGURE 19. Connectivity condition between nodes of pollution reduction upon CO leakage scenario.

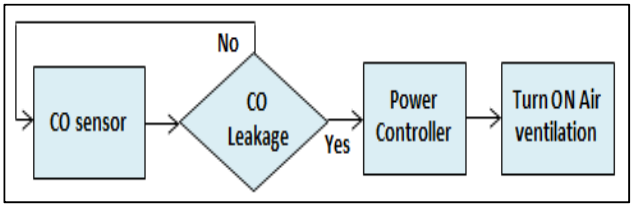

FIGURE 20. Block diagram of pollution reduction upon CO gas leakage.

light intensity upon human presence scenarios. The scenario composes of a CO gas node and power controller node, as in Figures 19 and 20. CO gas node detects air pollution, especially CO gas. At the same time, the power controller node controls air ventilation and fans in the home garage.

3) STATE DIAGRAM

The process-state of the CO gas node acts as a coordinator that detects if the CO leakage exceeds the threshold save

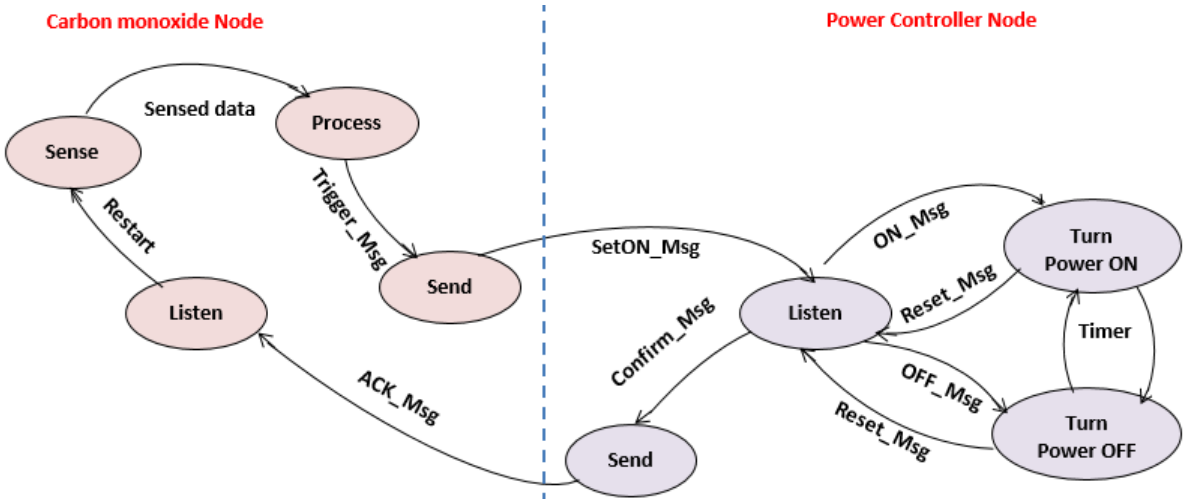

FIGURE 21. BState diagram of pollution reduction upon CO gas detection scenario.

level of gas or not to manage the sending and receiving data between the CO node and the power controller node. Under the emergency condition, Send-state of the CO node sends SetON_Msg data into Listen state of power controller node, which yields to turning ON the electricity of air ventilation and fans and sending back the ACK message into the CO node. If the connection is released, the state of electricity changes from ON to OFF after an elapsed time of the disconnection. Finally, the power controller node stays waiting for the new connection in Listen state, while the CO gas node is restarted into the Sense-state. All paragraph is depicted in Figure 21.

E. AIR CONDITIONING CONTROL

1) OBJECTIVES

Simply, an Aircondition appliance can be controlled upon the historical readings of the temperature and humidity parameters at a certain location at home. This scenario is activated only for emergency mode.

2) PROCESS AND ALGORITHM

The scenario algorithm comprises the temperature & humidity node and power controller node. A temperature & humidity sensor node is established to show the weather status in the homeroom. The power controller node can adopt the air condition appliance according to the temperature and humidity room. It avoids the extreme, very hot weather caused by the surrounding environment area at home. The adaptation process of the scenario is seen in Figure 22.

3) STATE DIAGRAM

The state diagram of this scenario in Figure 23 begins to continuously monitor the temperature and humidity room through Sense-state at home. Process-state was designed to recognize high temperature in emergency case using known threshold from temperature &humidity-node into Listen-state

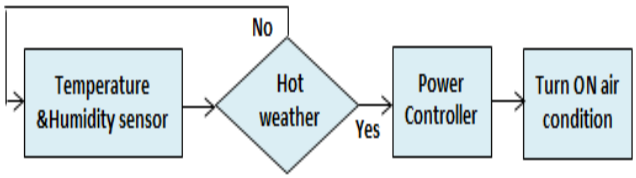

FIGURE 22. Generic algorithm of airconditioning control scenario.

of the air-conditioning device, attached to power controller-node. Thus TurnON-state is activated by the power controller node to run the home appliance. Then, acknowledgment data is sent back from the Send-state of the power controller node into the Listen-state of the temperature & humidity node. If the temperature & humidity node stops sending its data into the power controller, the power controller node turns off the air conditioner after a short time.

F. INCREASING LIGHT UPON HUMAN PRESENCE

1) OBJECTIVE

This scenario has two operation modes: safe mode and intrusion mode. In safe mode, the light intensity level is quite adopted to be increased when the human presence in the household is detected. On the other hand, extremely in intrusion mode, detecting intrusion presence at home yields to set light dimmer for home bulbs and actuate a siren alarm.

2) PROCESS AND ALGORITHM

The scenario algorithm was built to develop the two main modes. PIR motion-node is used to detect the motion of humans at home, whether household or intrusion. Power controller-node actuates siren alarm and turns ON light bulbs home in intrusion mode. While in safe mode, the power controller increases the light intensity level of bulbs. The mapping between two modes is based on the distribution of scenario nodes at home. Moreover, if the PIR node is

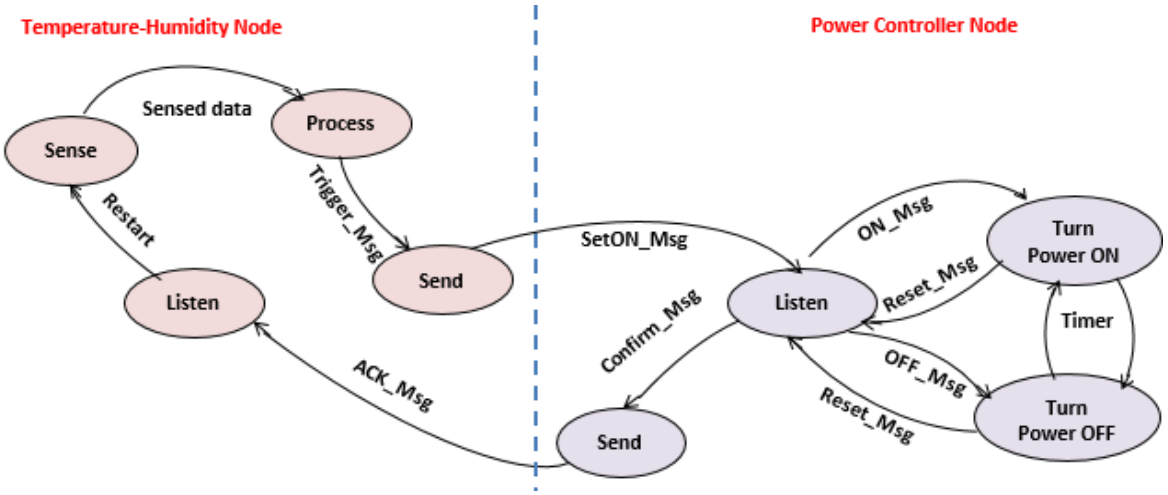

FIGURE 23. State diagram of airconditioning control scenario.

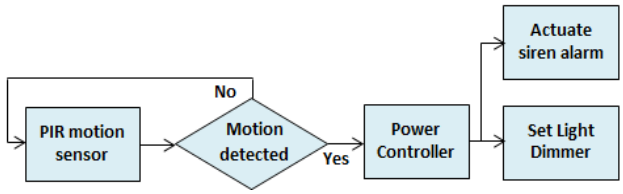

FIGURE 24. Scenario algorithm of both safe and intrusion modes.

located at the nearest home door and the power controller lies in the same Reception room, this scenario nodes are suitable for intrusion mode. While, if the same scenario nodes are applicable for safe mode if they are distributed in the bedroom. Both process modes of this scenario are seen in Figure 24.

3) STATE DIAGRAM

Initially, in both modes, the PIR node makes continuous monitoring of human motion at home. If a motion is detected, Process-state triggers a message into Send-state to transmit to the power controller that such human presence is detected. The power controller node performs two main tasks in different mode scenarios. First, it actuates the alarm of the Actuate-state in intrusion mode. In contrast, it tunes and adjusts, increasing the light intensity of the bulb in the Light Tuning-state in safe mode. In the case of power, the controller node stops receiving data in Listen-state, and the power controller node transits from the Light Tuning-state into the Turn ON/OFF-state after a given time. The whole section is seen in Figure 25.

VI. EXPERIMENTAL RESULTS

The proposed six smart home scenarios are implemented in the pilot model to measure both the traffic profile and the average data rate on each source node, over such a scenario, and on the cloud. Each scenario consists of two or three source-node traffic profiles. The first three scenarios are implemented in both normal mode and emergency mode. While the last three scenarios are implemented only in emergency mode.

The traffic profile is the number of bytes of data sent from each thing node in a certain scenario over the duration of time. Consequently, the average data rate is the average number of bytes sent per unit of time (bytes/sec.). The results of measurements are sniffed using the Cool Term program for a duration time of 60 sec. from the second 18 to the second 78.

A. NORMAL TRAFFIC PROFILE

The normal traffic profile of the six scenarios networks could be classified into intra-network traffic or intra-scenario traffic and inter-network traffic. The intra-scenario traffic is the total data traffic generated from two or three source nodes in the entire scenario. For instance, the LNG-node data from scenario 1 into scenario 3. While, inter-scenario traffic is the total traffic aggregated from all six main scenarios on the cloud through the Internet.

Figure 26 describes an individual traffic profile for each source node inside the first three main home scenarios in the normal mode. The individual traffic profile for each source node in the normal mode is ranged from about 15∼25 bytes " 0.11∼0.19 Kbits.

Figure 27 shows the traffic profile and the average traffic profile of the six main scenarios at home. As seen in Figure 27, the intra-scenario traffic is the sum of the data traffic in bytes that is transmitted from one or many source nodes inside one scenario T_n. It can be calculated from Equation (1). The traffic on each scenario records about 40bytes "0.31 Kbits" at one minute with an average data rate of about 20bytes/sec. or "0.15 Kbps".

$$T_n = \sum_{i=1}^{m} T_i \tag{1}$$

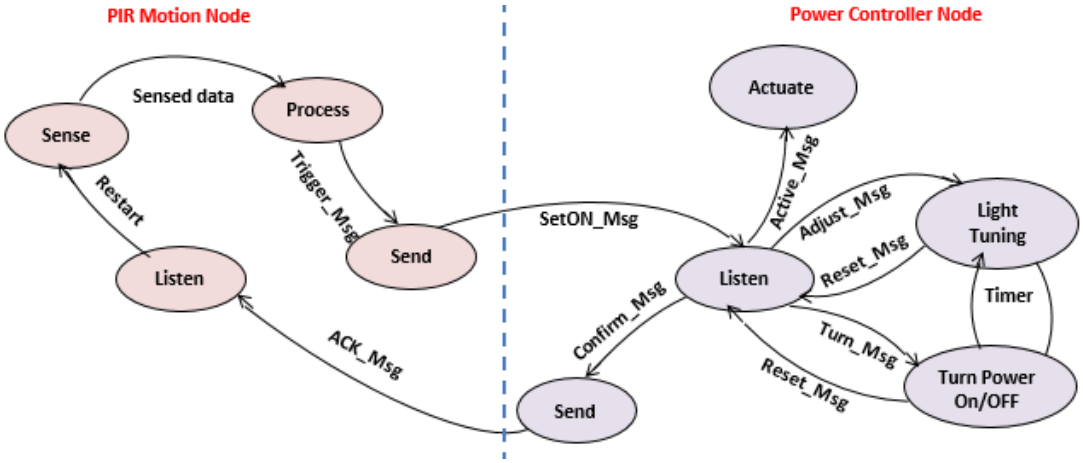

FIGURE 25. State diagram of scenario F.

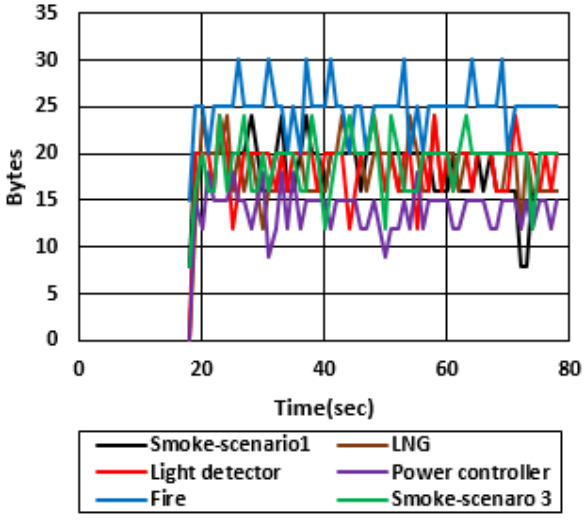

FIGURE 26. Source-nodes traffic profiles in normal mode.

where n represents the number of the scenario, and m is the number of source nodes in the scenario network. The source-node traffic profile can be represented as T_i for $i = 1,2, \ldots\ldots m$ finite number of source nodes in the scenario. Thus, the home traffic profile is the total sum of the traffic profile of local area networks of home scenarios in normal mode, as depicted in Equation (2).

$$\sum_{j=1}^{n}\sum_{i=1}^{m} T_{i,j} \tag{2}$$

where $T_{i,j}$ refers to the traffic profile of the source node i at the scenario network j. Figure 28 shows the traffic profile and the average traffic rate of the inter-network traffic on the cloud. It appears to be approximately deterministic with a small variation of 120 bytes peak value "0.93 Kbits" over the periodic time from 18-78 seconds with a constant average data rate of 160 bytes/sec. "0.16 Kbps".

It is concluded that the inter-network traffic on the cloud isn't generated through one "ESP8266 Node" controller unit in the proposed smart home networks, but it is incoming from six controller units of the six main scenarios. The overall traffic on the cloud of 0.93 Kbits is accumulated from the first three scenarios in Figure 28, each with 0.31 Kbits. Thus, any one controller in the proposed networks can carry one-third of the inter-network traffic on the cloud, compared to the unique, centralized, and limited controller unit that can carry the full traffic load on the cloud in traditional smart home automation [15], [16], [17], [18], [19], [20], [21]. Accordingly, the proposed smart home networks can avoid any expected heavy traffic and minimize traffic congestion. For a massive number of scenarios in the same smart home network and several smart home networks inside the IoT smart community or IoT smart city of several buildings and flours, the expected data traffic is heavy and can exhibit traffic congestion. In this case, the existing centralized home automation networks aren't suitable for this type of network.

B. EMEREGENCY TRAFFIC PROFILE

This emergency traffic is concerned with event-driven data triggered from one or many different networks included in the smart home system due to emergency cases at homes. For instance, data generated from source nodes is associated with interrupt modes such as smoke, LNG, fire, CO, temperature&humidity, and PIR motion source nodes. Figure 29 shows the individual traffic profile for the source nodes in emergency mode. Some source nodes have a low traffic profile as the traffic profile of about 5 bytes "0.04 Kbits" in the smoke sensor of scenario 2. While some source nodes have a high traffic load such as the traffic profile of 25 bytes "0.16 Kbits" in the temperature and humidity sensor of scenario 5.

Let's assume that all urgent cases of six scenarios networks in the home result in the same instance. Thus, the expected emergency traffic profile can be measured as the total sum of

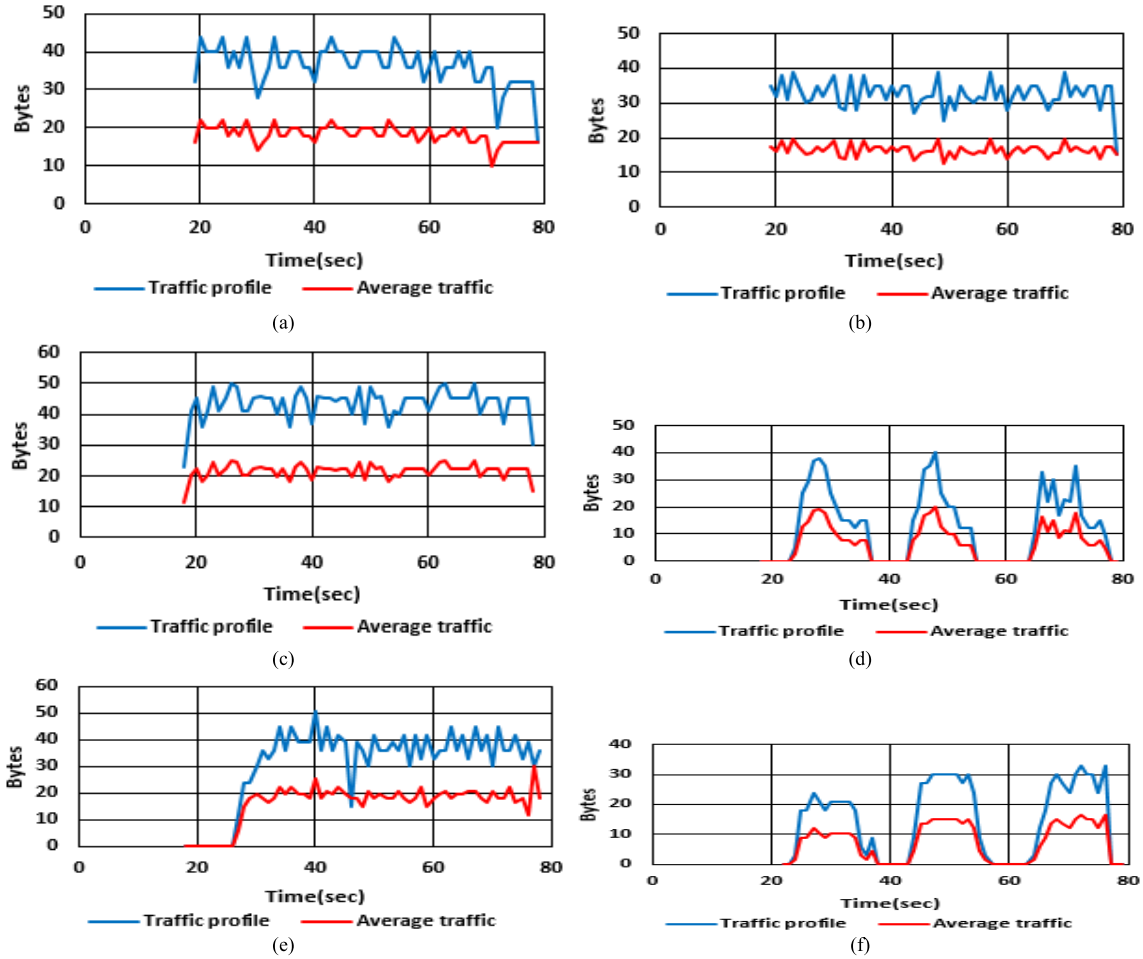

FIGURE 27. Traffic profiles of the six main scenarios: (a) Scenario 1, (b) Scenario 2, (c) Scenario 3, (d) Scenario 4, (e) Scenario 5, (f) Scenario 6.

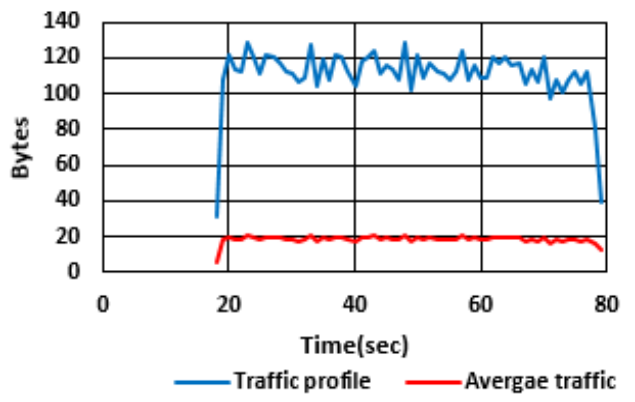

FIGURE 28. Overall traffic profile "inter-network traffic" on the cloud.

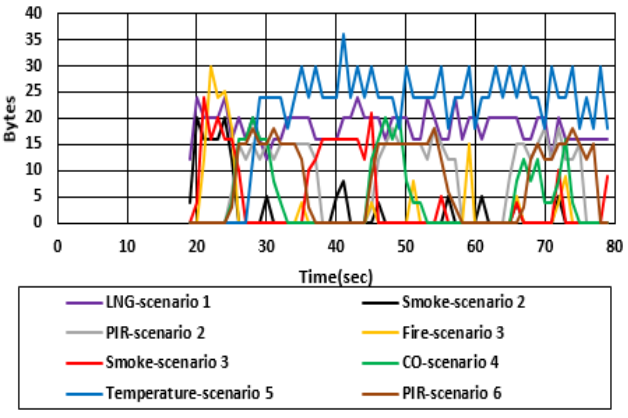

FIGURE 29. Source-nodes traffic profiles in emergency mode.

all urgent scenario cases at a short duration. In the proposed pilot, source-nodes profiles of emergency mode are triggered temporarily three times at distinct time slots for the duration of 5-10 sec., 25-30 sec., and 45-50 sec. times. As shown in Figure 30, it is observed that the emergency traffic profile has a significant variation of bytes along with time with an peak value of about 120 bytes or 0.94 Kbits. While the average traffic rate records about 5 bytes/sec. or 0.04K bps.

C. CLOUD TRAFFIC PROFILE

The home status scenario experiment is executed in this paper to describe and monitor data about the home status.

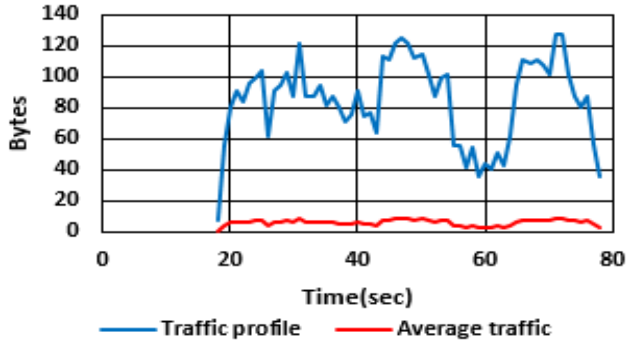

FIGURE 30. Emergency traffic profile and its average data rate-three consequence times at one minute.

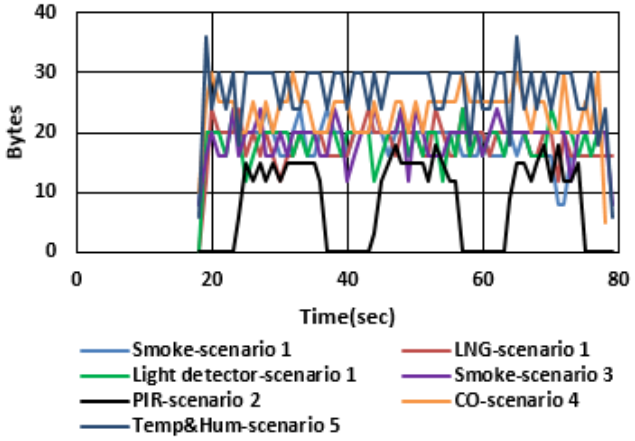

FIGURE 31. Individual traffic profiles of the seven source nodes in the status home scenario.

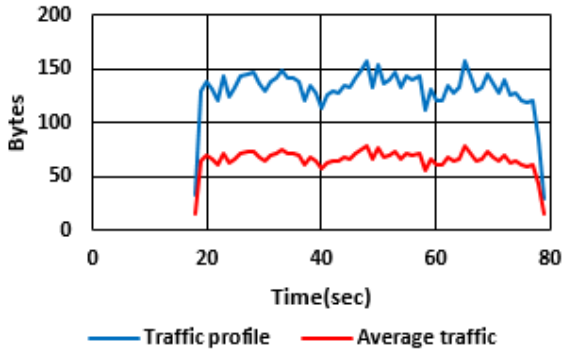

FIGURE 32. Status Home traffic profile- aggregated traffic on cloud.

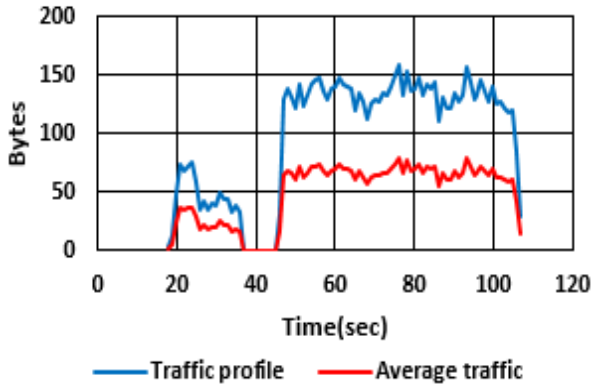

FIGURE 33. Event driven traffic profile with some of sensors in the Home Status traffic profile on the cloud.

It consists of 7-source nodes (LNG-sensor scenario 1, Smoke-sensor scenario 1, light detector-scenario 2, PIR-scenario 2, smoke-scenario 3, CO-scenario 4, temperature & humidity-scenario 5) connected directly with the cloud using the internet. Figure 31 shows the individual traffic profile of the seven source nodes without aggregation in the status home scenario. Each sensor can only generate a light traffic profile from 10-30 bytes over 60 seconds.

Home status scenario can carry information about the level of welfare, availability of home safety factors, maintaining energy, and achieving a green smart home friendly to society. Based on monitoring of smoke and LNG data in normal mode, the expectation of fire occurrence can be easily expected and gives statistical values about the smoking people in this field and green environment area. The light detector and PIR motion data are required to detect the power management level at home. The light detector data can only detect the intensity of sunlight at home and its effects on human health. The incoming data from the CO-sensor is a necessary calculation to detect the home air pollution percentage. Measuring the temperature and humidity of buildings gives a clear image of the weather status. The home status data are sent periodically to the cloud. Assume that all data types of the 7-sensors are sent at the same instance as in Figure 32. The status home traffic profile on the cloud is the total sum of the individual traffic profiles of the 7-sensors in the Status Home scenario. It records about 150 bytes or 1.2 Kbits with an average data rate of 75 bytes/sec. or 0.6 Kbps.

It is noted that the Home Status traffic profile on the cloud is accumulated from 7-source nodes using five controller units of scenarios (1-5). Each source node has 10-30 bytes or 0.08 Kbits-0.23 Kbits. Thus, the aggregated traffic profile of 1.2Kbits is not carried by one centralized controller installed in the previous smart home automation [15], [16], [17], [18], [19], [20], [21], but this traffic value is distributed over more than one controller unit and then reduces the expected heavy traffic load on the cloud if the proposed parallel distributed networks extended for several buildings in the smart city.

Another experiment is monitored in case of both event-driven data and home status data are sent over the cloud with different instants as shown in Figure 33, called a non-aggregated cloud traffic profile. The event-driven data are suddenly captured as a short pulse from the individual traffic profiles of all emergency source nodes in Figure 29 at 18-36 seconds. After that, the accumulated traffic profile of the status home data in Figure 32 are sniffed for the duration of 46-107 seconds (approximately occupied one minute).

VII. CONCLUSION

This paper begins to study IoT technology and the behaviour of IoT devices. The paper proposes a full description of

End-to-End advanced smart home system architecture as a part of IoT uses cases. Rather than existing works, the paper presents a set of protocols, processes, and algorithms required to guarantee a reliable IoT smart home system. Accordingly, a smart home pilot model is installed from an existing and allowable infrastructure in our daily life as Wi-Fi, sensors, light bulbs, home appliances, and a reliable and low-cost ESP8266 controller. Six main smart home scenarios are formulated and successfully tested to reflect the true meaning of comfort and luxury for consumers inside their homes. Furthermore, the smart home architecture is designed to empower things (e.g., home appliances) to gain enough intelligence to interact with a human beneficiary, which is called IoT. The results of the experimental pilot are not only for implementing IoT smart home system design, but also performing an optimum system scenario design with simple and low-cost development kits with less traffic generated.

The experimental results are sniffed using the CoolTerm program to prove the concept. It is verified that the experimental results of the proposed IoT smart home scenarios are validated with the light traffic patterns and minimum average traffic rate on each simple and low-cost controller unit installed in the proposed models, compared to the centralized controller unit in the previous works that carry all traffic loads on its cloud and results heavy traffic pattern, specifically if they are extended onto several smart home networks, combines IoT smart city. However, the implemented pilot model has only six scenarios and the heavy traffic load has not happened in this case. In future work, we look to extend the proposed smart home networks onto IoT smart cities and exploit the Artificial Intelligence (AI) technology with the proposed IoT smart home framework for emerging 6G.

REFERENCES

[1] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6G Internet of Things: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, Jan. 2022.

[2] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020.

[3] P. Upadhyaya, S. Dutt, Ruchi, and S. Upadhyaya, "6G communication: Next generation technology for IoT applications," in *Proc. 1st Int. Conf. Adv. Comput. Future Commun. Technol. (ICACFCT)*, Dec. 2021, pp. 23–26.

[4] W. Ejaz, A. Anpalagan, M. A. Imran, M. Jo, M. Naeem, S. B. Qaisar, and W. Wang, "Internet of Things (IoT) in 5G wireless communications," *IEEE Access*, vol. 4, pp. 10310–10314, 2016.

[5] L. G. Manzano, H. Boukabache, S. Danzeca, N. Heracleous, F. Murtas, D. Perrin, V. Pirc, A. R. Alfaro, A. Zimmaro, and M. Silari, "An IoT LoRaWAN network for environmental radiation monitoring," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–12, 2021.

[6] N. Sharma and D. Panwar, "Green IoT: Advancements and sustainability with environment by 2050," in *Proc. 8th Int. Conf. Rel., INFOCOM Technol. Optim. Trends Future Directions (ICRITO)*, Jun. 2020, pp. 1127–1132.

[7] M. A. M. Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of Things security: A survey," in *Proc. Int. Conf. Adv. Sci. Eng. (ICOASE)*, Oct. 2018, pp. 162–166.

[8] R. Bashir, B. Gaur, and A. Salil, "Logistics and IoT based survival strategies to facilitate supply chain engineering during pandemic," in *Proc. Int. Conf. Comput. Intell. Knowl. Economy (ICCIKE)*, Mar. 2021, pp. 1–7.

[9] R. Khalid and W. Ejaz, "Internet of Things-based on-demand rental asset tracking and monitoring system," in *Proc. 5th Int. Conf. Inf. Comput. Technol. (ICICT)*, Mar. 2022, pp. 84–89.

[10] B. C. Kavitha and R. Vallikannu, "IoT based intelligent industry monitoring system," in *Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Mar. 2019, pp. 63–65.

[11] Md. M. Haque, Z. H. Choudhury, and F. M. Alamgir, "IoT based smart energy metering system for power consumers," in *Proc. 2nd Int. Conf. Innov. Eng. Technol. (ICIET)*, Dec. 2019, pp. 1–6.

[12] J. Li and Y. Lin, "IoT home automation—Smart homes and Internet of Things," in *Proc. 3rd Int. Academic Exchange Conf. Sci. Technol. Innov. (IAECST)*, 2021, pp. 294–298.

[13] J. Xu, Z. Hu, Z. Zou, J. Zou, X. Hu, L. Liu, and L. Zheng, "Design of smart unstaffed retail shop based on IoT and artificial intelligence," *IEEE Access*, vol. 8, pp. 147728–147737, 2020.

[14] M. J. Hossain, M. A. Bari, and M. M. Khan, "Development of an IoT based health monitoring system for e-health," *2022 IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, vol. 2022, pp. 0031–0037.

[15] T. Chaudhuri, V. Nyamati, and K. Jayavel, "Design and implementation of IoT framework for home automation and monitoring," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC), 2nd Int. Conf.*, Aug. 2018, pp. 5–11.

[16] W. A. Jabbar, M. H. Alsibai, N. S. S. Amran, and S. K. Mahayadin, "Design and implementation of IoT-based automation system for smart home," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Rome, Italy, Jun. 2018, pp. 1–6.

[17] M. A. Hoque and C. Davidson, "Design and implementation of an IoT-based smart home security system," *Int. J. Networked Distrib. Comput.*, vol. 7, no. 2, pp. 85–92, 2019.

[18] O. Tayan, M. Alalawi, A. Alahmadi, and A. Albinsari, "Design and implementation of a multi-function home automation system based on Internet of Things (IoT)," *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 2, p. 75, 2019.

[19] E. I. Davies and V. I. E. Anireh, "Design and implementation of smart home system using Internet of Things," *J. Digital Innov. Contemp Res. Eng. Tech.*, vol. 7, no. 1, pp. 33–42, 2019.

[20] I. Baranilingesan, V. Kathirodhayan, and P. Hariharan, "Design and implementation of an IoT based home automation framework," in *Proc. Int. Conf. Intell. Technol. Secur. Privacy Wireless Commun. (ITSPWC)*, 2022, pp. 1–9.

[21] C. Sisavatha and L. Yu, "Design and implementation of security system for smart home based on IoT technology," *Proc. Comput. Sci.*, vol. 83, pp. 4–13, Jan. 2021.

[22] M. Iglesias-Urkia, A. Orive, and A. Urbieta, "Analysis of CoAP implementations for industrial Internet of Things: A survey," *Proc. Comput. Sci.*, vol. 109, pp. 188–195, Jan. 2017.

[23] S. Devi and H. D. Kotha, "AES encryption and decryption standards," in *Proc. Int. Conf. Comput. Vis. Mach. Learn.*, vol. 1228, 2019, pp. 1–10.

[24] E. Luzuriaga, J. C. Cano, C. Calafate, P. Manzoni, M. Perez, and P. Boronat, "Handling mobility in IoT applications using the MQTT protocol," in *Proc. Internet Technol. Appl. (ITA)*, 2015, pp. 245–250.

[25] A. S. Ibrahim, K. Y. Youssef, and M. Abouelatta, "Traffic aggregation techniques for optimizing IoT networks," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 6, no. 1, pp. 509–518, Jan. 2021.

[26] *Energy Smart Home Performance*. Accessed: Jul. 8, 2022. [Online]. Available: http://energysmartohio.com/uncategorized/which-indoor-air-quality-monitors-are-best-and-why/

[27] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *Proc. 2nd Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Apr. 2012, pp. 1282–1285.

[28] *Safety*. Accessed: Jul. 20, 2022. [Online]. Available: https://www.safety.com/glass-break-sensors/#gref

[29] H. Verma, M. Jain, K. Goel, A. Vikram, and G. Verma, "Smart home system based on Internet of Things," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2016, pp. 2073–2075.

[30] L. Fraiwan, K. Lweesy, A. Bani-Salma, and N. Mani, "A wireless home safety gas leakage detection system," in *Proc. 1st Middle East Conf. Biomed. Eng.*, Feb. 2011, pp. 11–14.

[31] *Parallax*. Accessed: Jul. 28, 2022. [Online]. Available: https://www.parallax.com/downloads/mq-5-lpg-gas-sensor-datasheet

[32] *CDN-Adafruit*. Accessed: Aug. 5, 2022. [Online]. Available: https://cdn-shop.adafruit.com/datasheets/TSL2561.pdf

[33] *Air Quality Sensor*. Accessed: Aug. 8, 2022. [Online]. Available: https://www.seeedstudio.com/Grove-Air-quality-sensor-v1.3-p-2439.html
[34] *SmartGarden3*. Accessed: Aug. 20, 2022. [Online]. Available: http://store.switchdoc.com/air-quality-extender-pack-for-ourweather-raspberry-pi-arduino-esp8266-grove-headers/
[35] M. Schwartz, *ESP8266 Internet of Things Cookbook*, 1st ed. China: Packet, 2017.
[36] B. Sarwar, I. S. Bajwa, N. Jamil, S. Ramzan, and N. Sarwar, "An intelligent fire warning application using IoT and an adaptive neuro-fuzzy inference system," *Sensors*, vol. 19, no. 14, p. 3150, Jul. 2019.
[37] A. S. Ibrahim, K. Y. Youssef, H. Kamel, and M. Abouelatta, "Traffic modelling of smart city Internet of Things architecture," *IET Commun.*, vol. 14, no. 8, pp. 1275–1284, May 2020.

AMIN S. IBRAHIM received the B.Sc. degree in electronics and communication engineering from the Thebes Higher Institute, in 2006, and the M.Sc. degree in electronics and communication engineering and the Ph.D. degree from Ain Shams University (ASU), in 2013 and 2021, respectively. He was a Demonstrator with the Thebes Higher Institute for Engineering, from 2007 to 2013, where he was also a Teaching Assistant and a Teacher, in 2022. He is currently a Lecturer with the Thebes Higher Institute and Geiza Higher Institute for Engineering. He has published eight papers in conferences and international journals. His research interests include traffic modeling, the IoT communication networks, the QoS of wireless networks, and artificial intelligence (AI) technologies. His practical works concerned with programming and embedded systems.

AHMED M. ABBAS received the B.Sc. degree in electronics and communications engineering from the Thebes Higher Institute for Engineering, Cairo, Egypt, in 2006, and the M.Sc. degree in electronics and communications engineering and the Ph.D. degree in radio resources management of IoT networks from Ain Shams University, Cairo, in 2012 and 2021, respectively. He was with the Thebes Academy, Cairo, from 2006 to 2008. From 2009 to 2010, he was with Egyptian National Company for Telecommunications. Since 2010, he has been with the Egyptian Atomic Energy Authority (EAEA) as a part of the communications systems research team for the Egyptian Nuclear Program. His previous publications include the article "An SDL Design and Implementation of Radiation Monitoring Network Using WCDMA," *Journal of Communication and Computer* (David Publishing, May 2012) [ISSN 1930—1553 (online) 9 (2012) 602-612.], "NB-IoT Optimization: Holistic View for Smart Cities Applications With Smart Meters Networks Case Study," *IET Communications*, in 2020, [pp. 1-14 (DOI: 10.1049/cmu2.12063.)], and "Simulink-Based Modeling and Performance Analysis of NB-IoT Uplink Scheduler," JAC-ECC 2020, book *Radiation Monitoring Network Using WCDMA* (Lampert Publishing) (ISBN 978-3-659-55784-2).

ASHRAF MOHAMED ALI HASSAN was born in Giza, in 1979. He received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electrical engineering from Cairo University, in 2002, 2005, and 2009, respectively. He was an Associate Professor in electronics and communication engineering with the Supreme Council of Universities, Egypt, in 2019. He is currently an Associate Professor with the October High Institute for Engineering and Technology, 6th of October, Egypt. He has published more than 25 international papers. He was awarded a certificate of appreciation for the supervision with the high performance and lasting contribution to the graduation project with the title of "Vertical Handover Implementation and Application" and this project is the first on the level of the Egyptian University. His research interests include digital signal processing and the synthesis of electronic circuits.

WAEL M. F. ABDEL-REHIM received the Ph.D. degree in computer science from Suez University, Suez, Egypt, in 2016. He has been an Assistant Professor with the Faculty of Computers and Information, Suez University, and an Adjunct Assistant Professor with the Faculty of Computer Science and Engineering, King Salman International University. He studied for a semester with The University of Edinburgh, U.K. Moreover, he is a reviewer in many international computer science journals. He has 16 publications in various international journals and conferences. His current research interests include high-performance computing applications, parallel computing, convolutional neural networks, metaheuristic optimization, and scheduling problems.

AHMED EMAM received the B.Sc. degree from Ain Shams University, Cairo, Egypt, the M.Sc. degree from Menoufia University, Menoufia, Egypt, and the Ph.D. degree from the Computer Science and Computer Engineering Department, Speed Engineering School, University of Louisville, Louisville, KY, USA, in Summer 2001. He is currently a Professor in information systems with the College of Computer and Information Systems, King Saud University, where he teaches database systems, data mining, and big data analytics.

SAEED MOHSEN received the B.Sc. degree (Hons.) in electronics engineering and electrical communications from the Thebes Higher Institute, Cairo, Egypt, in 2013, and the M.Sc. and Ph.D. degrees in electrical engineering from Ain Shams University, Cairo, in 2016 and 2020, respectively. He is currently an Assistant Professor with the Al-Madinah Higher Institute for Engineering and Technology, Giza, Egypt. He has made intensive research on the applications of artificial intelligence (AI), such as deep learning and machine learning. He has published a number of papers in specialized international conferences and peer-reviewed periodicals. His research interests include biomedical engineering, wearable devices, energy harvesting, analog electronics, and the Internet of Things (IoT).