Int. J. Nonlinear Anal. Appl. In Press, 1–15
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2023.29905.4289

A review of security methods in smart homes

Mahsa Shahim

Department of Computer Engineering, Faculty of Engineering, Payame Noor University, Tehran, Iran

(Communicated by Seyed Hossein Siadati)

Abstract

A smart gateway, which plays an important role in a smart home, generally connects the internal and external networks of the home, and also jointly manages the smart Internet of Things (IoT) devices equipped with the smart home. Protocols collect generated data from nearby devices and even perform some local data processing tasks. In this paper, we first review the entire research field of smart homes, focusing on a framework based on edge computing and multiple intelligent agents. Then, we divide the evolution of smart gates into three generations based on the timeline and various criteria including quality of experience (QoE), AI support, software-defined networking, etc. Next, we will discuss the key technologies and components of smart gateways such as operating systems, wireless communication protocols, and security. Finally, we examine the challenges and trends of smart gates. This article examines the importance of building a secure smart home system.

Keywords: security, smart homes, network
2020 MSC: 68M25, 74M05

1 Introduction

With the rapid development of micro-electromechanical systems, microcontrollers, micro-sensors and wireless communication technologies, the smart home (also called smart home or home automation) has attracted increasing attention from companies, communities, as well as researchers, and has gradually entered daily life. It becomes us. The smart home can provide a variety of automation scenarios to make our lives efficient and convenient, help us increase security and safety in the smart space, help disabled people and the elderly especially to take care of their health [2, 38, 62] As one of the main components of the smart home, the smart gateway plays a very important role, because through it, not only the internal and external networks of the home, but also all kinds of digital electronic and electrical equipment in the home can be connected and managed. In addition, the smart gate can collect various information from home appliances, sensor devices, and users or occupants and process the collected information for further needs. Specifically, using this smart gateway, on the one hand, users can easily control and schedule home appliances and home sensors, upload and download resources through external networks (such as the Internet) and cloud platforms. do On the other hand, users' behavioral patterns can be acquired and learned to improve users' service QoE [2]. In this case, connectivity, interaction and services are built around the main gateway. Currently, there are a variety of emerging technologies, standards and products, especially smart gateways in smart homes, originating from large companies or companies such as Intel, IBM, Microsoft, TI, AT&T, Apple, Google, Sony. These companies contribute to the rapid evolution of smart homes in various perspectives, from new chips, operating systems (OS) to many practical applications. Practically the current situation is that everyone is trying to build their own standards

Email address: m_shahim84@yahoo.com (Mahsa Shahim)

Received: November 2022 *Accepted:* February 2023

and ecosystem, which makes sense but is a weakness for the development of smart gates. They are waiting for unified and common standards. On the other hand, scalable software architectures and functions in smart gates should provide configurable and personalized services for different users and residents and be fully or partially open source for wider design support. In addition, with the implementation of smart home and the increasing number of smart devices in smart homes, the accumulated big data of users/residents and devices needs high-performance coordination, management and analysis. At the same time, this data processing also requires the help of the computing system. The cloud computing system is not a unique optimal design that should be combined with fog and edge computing systems and comprehensively consider computing performance, security, latency, data storage, dynamic service placement, etc. [13, 24, 31, 32, 35, 45, 73] Although many companies and researchers are trying different smart gateway technologies and methods from different angles, from hardware to system structure and software, from functions to services and applications, or, from cloud to fog computing. and edge, including QoE, intelligent agent, software defined. network (SDN), network function virtualization (NFV) and network slicing, [3, 6, 17] but there is still a long way to tackle those problems and achieve those goals. Therefore, it is necessary to review and discuss the development of smart gates in terms of system architecture, technology, security, etc. In addition, we believe that this work not only directly provides a complete reference for companies and researchers, but also indirectly contributes to the formation of standardization and customization of smart gates. In this paper, we focus on several related aspects of smart gates, namely operating system, wireless communication technologies, security, flow control, future challenges and trends. In the continuation of the article in part 2, the works related to the smart home are reviewed. In Section 3, three generations of smart gates are presented based on the timeline and related technology criteria. In Section 4, recent smart gateways are reviewed. In Section 5, the main technologies for smart gates are listed and discussed. In Section 6, challenges and trends are explored.

2 Smart home

The concept of smart home is associated with the term smart environments, while smart environments originate from pervasive computing [60, 70, 71]. Today, smart home often appears in public media and becomes one of the familiar words. Smart home is also referred to in various names such as home automation, electronic home, smart home, digital family, home network, or home area network (HAN) systems, etc. In the case of smart home, although these names are different, their main meaning and function are almost the same. Since the emergence of the world's first smart building in the United States in 1984, many large IT companies and companies, investment firms, and electronics manufacturers have investigated and invested in various aspects of the smart home. Together, they began to support research and development in the smart home and invested heavily in this area. At present, famous international companies and enterprises (such as Intel, IBM, Microsoft, Vivint, ADT, AT&T, Apple, Google, Sony, Samsung, Huawei, Haier, etc.) have successively established their branches. Meanwhile, many large, medium and small companies have been involved in the smart home field in almost every aspect, from low-end system hardware and software to applications and services. As Strategy Analytics predicts in 2018 that the smart home market will reach $155 billion by 2023, these smaller companies are also hoping to quickly launch new products and innovations to capitalize on market concerns, thereby taking the lead. Take on the future competition. From small-scale smart electronic devices, such as smart sensors, smart switches, and smart sockets to large-scale smart home gateways and systems, various smart home products have been produced one after another, bringing great convenience and comfort to our daily lives. According to Lee et al., [40] there are three generations of smart homes based on the levels of automation from the bottom up. The first generation of smart homes is dominated by wireless technologies (such as Zigbee, Wi-Fi, Bluetooth, etc.) with proxy servers. The second generation is that artificial intelligence (AI) controls various sensor devices such as the Amazon Echo. The third generation is that ih robots can interact and cooperate with humans, such as Rovio Robot [8]. In [61], with a project called "GatorTech Smart House", designed and implemented a smart home based on a large number of personal smart devices: mailbox, entrance and exit, bed, bathroom and floor. All these parts are equipped with sensors and actuators that are connected to an operating system to make life easier for the elderly. The GatorTech Smart Home also uses a high-precision ultrasonic tracking system to locate users or residents, assess their habits, and control the environment. Mozer [49] designed and developed a home system with adaptive performance, called adaptive control of the home environment (ACHE), which uses neural network principles to control air conditioning, heating, and lighting systems and requires Eliminates previous manual programming. Additionally, the system hopes to save energy while respecting the lifestyle and privacy of its residents. ACHE continuously monitors the environment and observes the actions taken by the occupants (for example, using lights or adjusting the thermostat), so that it infers the behavior patterns and habits of the user. The basic stochastic dynamic programming strategies used in it facilitate the prediction of future behavior. Vastenburg et al. [64] developed an autonomous home controller with distributed agents that was deployed in a simulated smart home environment. They aim to automate some of the daily human activities to improve efficiency and quality of service (QoS). The simulated smart house has four rooms: bedroom, living room, bathroom and kitchen. Various smart agents (water heater, coffee maker, air conditioner, dishwasher, etc.) control the entire home environment by using a robot to move things from one place to another. Intelligent agents must share resources through interaction and cooperation (for example, dishwashers use electricity and hot water that may be used by others). Intelligent agents must be able to measure different actions and adapt their behavior to changing conditions. The laboratory scenario is also created and designed through the multi-agent survival simulation environment and Java framework, which can evaluate the agents and their cooperation ability. Kidd et al. [29] built a smart home called ”perceived family” for everyday life research, which aims to improve users' perception and quality of quality. Schulzrinne et al. [57] proposed a global-scale system that supports security and multi-user management and integrates a variety of software and hardware (achieving a global pervasive computing requirement). The system is based on Session Initiation Protocol (SIP), uses Bluetooth devices for location awareness, uses Service Location Protocol for service discovery, and introduces context-aware location information to enhance service discovery and user communication. Meyer et al [47] pointed out that the next generation of home system should seamlessly integrate people, devices and computing. They analyzed and summarized relevant research work on how to improve the quality of people's daily lives based on context-aware computing. Crabtree et al. [12] investigated the concepts and daily activities related to pervasive computing in the family and analyzed a large number of technical applications in people's daily activities that lead to attention to the locations of pervasive computing devices. Westenburg et al. [64, 65] pointed out that the acceptance of notification messages by users in the ubiquitous family computing environment mainly depends on the urgency of the message. If someone thinks it is an urgent message, they hope that the message can be notified and displayed immediately. This study proposed a method for subjective measures of controllable notification and acceptance. Bregman et al [9] pointed out that since there are many devices, interfaces and controllers in the home environment, some problems arise for this kind of OSGi Domotic framework.

These components usually perform a separate function and cannot be easily synchronized with each other, so an integrated model is needed to address this issue. The design of this model should emphasize the following three principles: (1) This model can guarantee the quality and availability of higher equipment and interfaces. (2) Using this model can greatly reduce the cost of the product. (3) The model can synchronize different types of devices. In addition to considering the application and the design of various communication interfaces, the architectural model should include a centralized management unit and an internal database for intelligent device integration and create complex pre-programmed scenarios and dynamic storage device lists. slow Recently, many researchers have studied and reviewed smart homes almost comprehensively. However, they have focused less on smart gates. Xu et al. [75] proposed an SDN-based smart home scheme and presented its challenges and opportunities. Ben Azoz et al. [6] investigated programmable HAN designs from the perspective of SDN, or a combination of SDN with NFV and network slicing, to flexibly control and manage HAN, increase QoS and QoE, improve security, and customize bandwidth usage. Meanwhile, depending on a virtualized and programmable residential gateway, they proposed an adaptive security scheme for HAN. Mukri et al. [48] investigated the structure of software including operating systems and data tracking and processing components, wireless and wired communication technologies, security and privacy in smart homes. They also presented a cloud-based architecture of a smart home. In this structure, the smart home is considered as an intelligent agent as proposed by Das et al. [14] proposed an agent-based negotiation approach (ABNA), which combines agents with a negotiation mechanism and enables services with opposing characteristics to work simultaneously. In particular, they presented a formal specification of ABNA using context-aware environment computation, demonstrated the practicality of ABNA, and analyzed and verified the correctness of ABNA. Although ABNA is a deterministic scheme, as its performance relies on predefined criteria, Alfakieh et al predicted that, in the future, a more intelligent scheme will be provided by employing a self-learning mechanism. However, the main component of the smart home is still the smart gateway, whether it is virtualized or virtualized, or programmable or non-programmable. In addition, Li et al. [39] first proposed six main features of smart home, which include understanding the interaction between the user and the smart grid, guiding the rational and scientific use of electricity, increasing convenience, safety and convenient lifestyle, monitoring and discovering processing. It was unusual and timely, providing smart service and more. Then, they investigated the structure of the smart home from the perspective of the smart network. Finally, they analyzed the smart home power service system after discussing interactive power service technologies and smart community support technologies. Zaidan et al [77] reviewed almost all potential applications in the smart home. Li et al. [40] analyzed generations, estimated popularity, evaluated home automation systems using big data analysis, and reviewed recent technologies that can realize sustainable development in smart homes. They also concluded that the benefits of smart homes are driven by resident knowledge rather than financial conditions. Mendez et al [46] reviewed almost all wireless communication technologies, application requirements and integrations in smart homes.

Johari et al. [28] proposed a layered smart home architecture that supports cloud services, integrates energy and health management with common wired and wireless communication techniques, investigates the security and privacy protection of health and energy data. and visualizes this data in an intelligent architecture. Home On the one hand, the scheme not only monitors the health care and well-being of residents, but also provides remote counseling. On the other hand, it can provide intelligent energy monitor to plan energy consumption in a way that saves energy. Recently, to optimize energy consumption, save cost, and assist in rapid decision-making and forecasting, Diyan et al. [17] proposed a multi-tasking intelligent Internet of Things (IoT) gateway that supported heterogeneous energy data processing and management. Especially, in order to reduce the delay of data processing and transmission and ensure the effectiveness of classification in the cloud environment, the data loading and storage module and the hybrid data classification module of Adaboost multilayer perceptron are further coordinated. Finally, they confirmed that the plan worked. The smart gateway is a main agent with powerful and rich functions that can perform very complex processing at the edge of the smart home network before sending big data to the cloud or cloud, as shown in Figure 1. End devices are able to communicate with the smart gateway located at the edge of the network. Furthermore, some agents whose sensors and actuators are fully integrated can perform multiple tasks independently, while others cannot perform tasks independently because their sensors and actuators are compartmentalized. All factors including the smart gateway aim to optimize rewards in the smart home, such as minimizing energy consumption, or maximizing QoE as well as data awareness in the smart home.

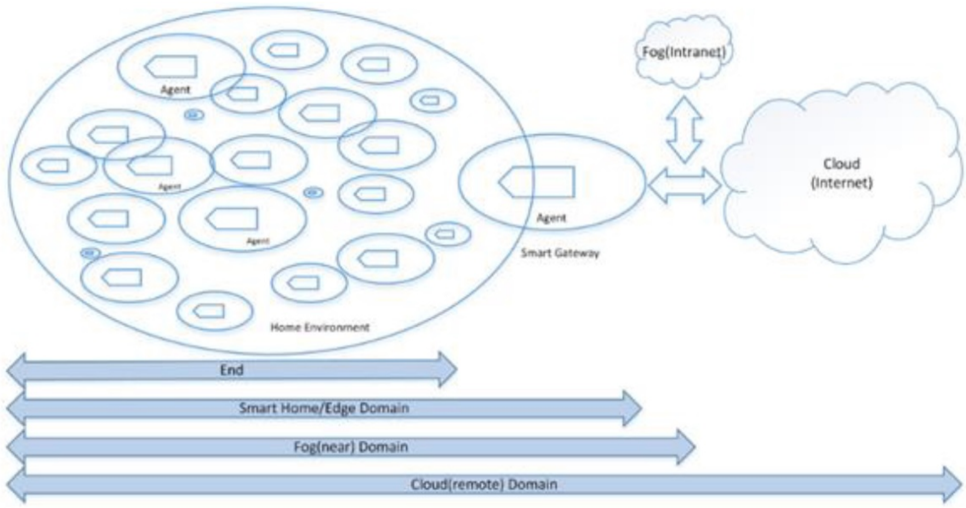

Figure 1

3 Three generations of smart gates for smart homes

Different classifications of smart gates have been proposed as shown in Figure 2. Depending on the specific type of functions or services supported, they are divided into three subgroups: multimedia gateway, QoS gateway, and OSGi domotic DOG gateway [5]; Depending on the number of access terminals and the types of services supported, gateways are classified into five subgroups [22]: virtual gateway, web-based central gateway, thin server gateway, set-top box gateway and multi-service gateway. Based on the OSI reference model, they can be type A gateways (operating at the physical layer, for example, layer 1), type B gateways (operating at the physical layer and data link layer), type C gateways (operating at layers from physical layer to the transport layer), type D gateway (operating at the session layer and application layer), type E gateway (operating across layers from the network layer to the application layer), and type F gateway (operating across all layers) [23]. Depending on the timeline, they are divided into four subgroups [10]: modems, routers, switches, and service gateways. Obviously, the different classifications include all smart gateways, from gateways used in main networks to gateways used in homes, offices or other indoor spaces. In addition, in the reporter classification, service gateway, OSGi gateway, or E-type gateway, respectively, are studied more than others.

3.1 The first generation of smart gates

The first generation of smart gateways are used to connect a home network, especially a PC, to the Internet, and possibly use wired cables to connect computers, phones, printers, and fax machines on-site. At the beginning of the

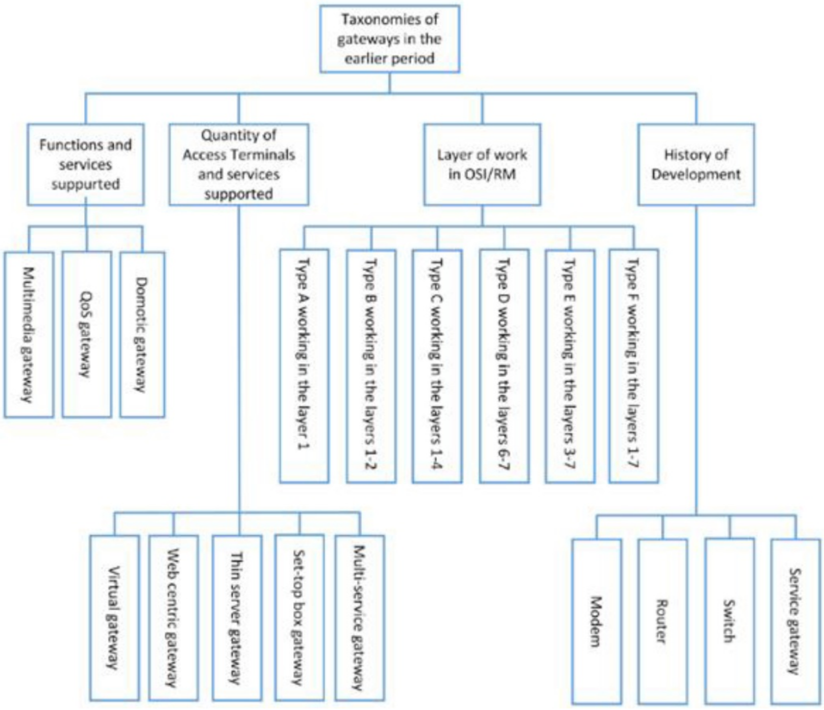

Figure 2: Different classifications of smart gates

design, these types of gates cannot manage household appliances and other surrounding devices. They have a low data rate. At the same time, since the storage scale is high, the memory size is small. Generally, they are configured through a predefined template and collect only running state information. That is, they rarely collect the data of the residents and the surrounding area. For the first generation, the traditional 56K (kilobit per second) modem is one of the paradigms. Despite the low data rates, it is still widely used today by users/residents in remote rural areas, where broadband gateways are not available, or people are unwilling to pay high fees.

3.2 The second generation of smart gates

Compared to the first generation, the second generation of smart gates is almost dominated by wireless technologies, in addition to wired network technologies, thanks to the rapid development of technology in Wi-Fi, Zigbee, and Bluetooth, etc. Second generation smart gateways run on IPv4 and IPv6 compatible networks. They have a higher data rate compared to the first generation. Data rates can be on the order of magnitude of tens of megabits per second or even hundreds of megabits per second, but rarely gigabits per second (gigabit per second). Meanwhile, in terms of the second generation of smart gates, the storage volumes and performance of the microcontroller unit (MCU) or the network processing unit (NPU) are also more advanced than the first generation, respectively. Accordingly, some basic functions of data storage and analysis have been introduced, but they are not yet rich and powerful. Data storage is based on periodic overlap mode, and data analysis is mainly offline processing. The second generation of smart gates are widely used today. Here, their paradigm is the xDSL modem, often called a broadband router. However, they still do not freely control and manage all heterogeneous electrical appliances and other smart devices, as these peripheral devices are usually close-sourced or follow different IoT standards from different companies. Therefore, smart homes based on smart gates become a routine reality. These gates need constant upgrading and improvement, which still has a long way to go.

3.3 The third generation of smart gates

Compared to the previous two generations, the third-generation gateway will run on IPv4 and IPv6-compatible networks or even IPv6-only networks, make full use of THz technology as well as traditional wired and wireless technologies, and flexibly support smart home appliances and sensor devices. is surrounded by All devices around the 3G gateway, especially heterogeneous devices from different companies, can freely connect to each other and seamlessly switch from one zone/channel to another. These gateways have a more efficient data rate than the second generation, which means the data transfer speed is surprisingly the fastest among the three generations. In general, data speeds can reach gigabit per second levels, often several gigabits per second or even more. In the third generation, the storage volume and MCU/NPU performance in smart gateways are respectively the strongest. Therefore, the frequency of overlapping data in local storage increases. Instead of offline, data analysis uses an online style with the help of machine learning. When the storage space reaches the threshold, the historical data is uploaded to the cloud/fog server. In addition, when the performance of NPU/MCU reaches the bottleneck of development, the third generation of smart gate may become a new generation which may rely on quantum chip or biochip. In addition, for the third generation of smart gateway, intelligent agent architecture will be used, which integrates SDN, cloud/fog/edge technology, NFV, Web of Things, QoE/QoS, etc. One of the emphasis of this generation of smart gates is on understanding and analyzing the usual actions and behaviors of users through the integration of the self-learning capacity of artificial intelligence. In addition, voice and gesture commands will be activated easily. However, this type of smart gateway is still an early design, which needs more effort to convert the conceptual architecture into the actual deployment of the system.

4 Smart gates

In this section, we review and compare emerging smart gates. As mentioned above, they mainly belong to the second generation. Wang et al., on the one hand, pointed out that the traditional gateway supports QoS measurement, network optimization, and client behavior analysis. They then investigated a smart gateway framework that relied on a lightweight plug-in scheme to collect data and awareness in smart home systems [67, 68]. At the same time, the framework was integrated with a cloud-based controller for further updates of controlled policies, in addition to implementing a general control policy for data collection and local awareness. In addition, the authors proposed multiple awareness schemes (including service-oriented, application-oriented, location-oriented, QoS, device-oriented, and subscriber-oriented) to achieve more accurate data awareness in this smart gateway. Finally, performance was demonstrated in terms of data collection efficiency and data awareness accuracy. On the other hand, Wang et al. extended and proposed the SDN-HGW (Home GateWay) structure to better guide self-organizing smart home networks and enable the SDN controller in the core network. For SDN-HGW, which can respectively use three deep learning algorithms (multilayer perceptron, stack autoencoder, and convolutional neural network) to classify encrypted data in open datasets. Finally, they demonstrated the relevant performance metrics by conducting experiments. Obviously, the former focused on a smart gateway structure, but the latter focused on the development of three DateNets based on three deep learning algorithms because the authors considered the SDN-HGW core as the data network. Compared to other works, both of them are more focused on data collection, management, processing and user-oriented awareness, i.e. QoE.

MLP is a class of feedforward artificial neural network (ANN) as shown in Fig. 3. A MLP consists of three or more layers. The first layer is for input data, i.e., a PBV X_i. One or more hidden layers extract features from the input. The last layer outputs a classification result. Each hidden layer, e.g., the i-th layer, is composed of multiple neurons that is mainly a nonlinear activation function as follows:

$$f(x) = \sigma(W^{(i)} \cdot x + b^{(i)}), \tag{4.1}$$

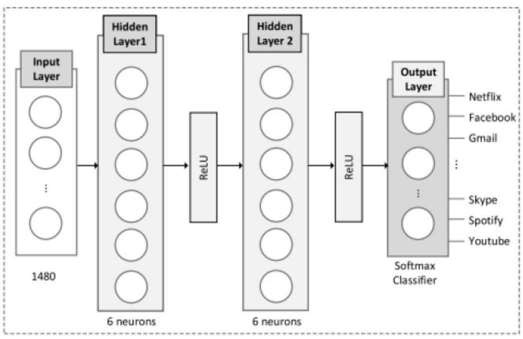

Figure 3: Overview of the MLP based DataNet.

where $\sigma(\cdot)$ is an activation function, e.g., $\sigma(x) = \tanh(x)$. The important characteristic of the activation function is that it provides a smooth transition as input values change. $W(i)$ is a weight matrix and $b(i)$ is a bias vector. There may be more than one hidden layer. Each layer passes through the same function with a different weight matrix and a bias vector. The final layer outputs the results of the last hidden layer, e.g., layer j, as follows:

$$o(x) = g(W^{(j)} \cdot x + b^{(j)}). \tag{4.2}$$

The MLP structure specified for the proposed packet classifier is shown in Fig. 3. It consists of one input layer, two hidden layers and one output layer. Using the full size of the data packet as an example, the input layer has 1480 inputs. The two hidden layers are composed of 6 and 6 neurons respectively. The output layer is composed of 15 neurons with Softmax as classifier. The classification process is defined as follows:

1. Input PBV $X_i = \{x_{i1}, x_{i2}, ..., x_{in}\}$ to the first hidden layer and compute the output as follows:

$$z^{(1)} = W^{(1)}\sigma(X_i) + b^{(1)}, \tag{4.3}$$

   where $\sigma(\cdot)$ is the activation function, i.e. a rectified linear unit (ReLU). ReLU is a non-linear operation as follows:

$$ReLU(x) = \max[0, x]. \tag{4.4}$$

2. For hidden layer 2 compute the output as follows:

$$z^{(2)} = W^{(2)}\sigma(z(1)) + b^{(2)}, \tag{4.5}$$

3. A fully-connected layer with a Softmax classifier output the final results as follows:

$$\hat{y} = \frac{exp\ z^j}{\sum exp\ z^j} \tag{4.6}$$

   where z^j is the output of the j-th neuron. $\hat{Y} = \{\hat{y}_1, \hat{y}_2, \hat{y}_3, ..., \hat{y}_N\}$ is the complete set of classes, and N denotes number of classes. The output with the highest probability indicates the class of the input value.

In MLP model, we use cross entropy as loss function and the calculation of gradient and updates of weights and bias are defined as follows:

1. Calculate the loss function of cross entropy between the output value and the label value as follows:

$$L = -\sum_{i=1}^{n} yi\ \ln f(x_i, \theta), \tag{4.7}$$

2. Update weights and bias using gradient descent as follows:

$$\begin{aligned} w &\longleftarrow w - \eta\frac{\partial L}{\partial w} \\ b &\longleftarrow b - \eta\frac{\partial L}{\partial b} \end{aligned} \tag{4.8}$$

To start the training process, training parameters are set as $\{N_e, M, \eta\}$, where N_e is the maximum number of Epoch, M is the size of mini_batch used in the stochastic gradient method, η is the learning rate. The complete process for the training process is summarized in Alg. 1. Without loss of generality, the algorithm only summarizes the basic structure of the process. Stopping criteria such as validation is not given in the description

Chattopadhyay et al [11] proposed a lightweight and connectionless IoT smart gateway framework that relies on multiple micro-agents. In this smart gateway design, the end devices can be loaded dynamically without disturbing the remote data transmission between the gateway cloud services and the Internet of Things, because the data exchange is done in the micro-agents between the sensor block or actuator block and the end devices. Meanwhile, individual device micro-agents can perform specific read and write tasks. Furthermore, this hybrid approach resulted in a plug-n-play component agent architecture that combines the flexibility of Message Queuing Telemetry Transfer (MQTT) with the RESTful compatibility of LWM2M. Finally, the authors evaluated the performance of this smart gateway framework through different loaded protocols. Unfortunately, the security of this plan, although discussed, needs to be strengthened. Next, we examine the efficiency estimation model [11].

Algorithm 1 MLP Based DataNet Training

Require: Training data, training parameters

Ensure: MLP based DataNet.

for $t = 1$ to N_e **do**
  for each batch of M input data **do**
    For each training samples $X_i \in X$:
    Compute the output using Eq. (4.3);
    Process with activation function Eq. (4.4);
    Compute the output using Eq. (4.5);
    Process with activation function Eq. (4.4);
    Output classification results according to Eq. (4.6);
    Compute the training error according to Eq. (4.7);
    Update weights and bias according to Eq. (4.8);
  end for
end for

5 Performance Estimation Model

Our proposed architecture has two major layers - LWM2M stack working on request/response principle and MQTT based microagents working on pub/sub fashion. S. Oh et al. published an mathematical model [51] to estimate performance impact for pub/sub vis-a-vis request/response model. Assuming event generation and consumption follows Poisson process pub/sub round trip time (RTT) approximately equals the pub-sub cost per event generated. We assume same cost analysis holds true in our MQTT layer. For the LWM2M part a performance estimation model may be conceptualized as a hypothesis describing the factors that impact the response times. We apply queueing theory to estimate a relationship between the response time for LWM2M requests and the number of concurrent Rest requests (GET/PUT). Assuming a steady state queue Little's law can be applied in the performance measurement as per the following formula [44]:

$$N = TP * (RT + TT), \tag{5.1}$$

where N is the number of concurrent request, TP is the throughput, RT is the response time, and TT is the think time. TP is dependent on computing capacity of the home gateway and load on the gateway. The relationship between response time and the number of clients may be assumed to be a non-linear function like a simple $M/M/1$ open queuing model:

$$RT = ST + QT = ST + (ST * u/(1 - u)), \tag{5.2}$$

where RT, ST, and QT are the Response Time (RT), Service Time (ST) and Queue Time (QT), respectively, and u is the utilization of bottleneck computing resource that serves the web request. The response time increases exponentially due to lack of resource as the utilization of this resource approaches its full capacity limit. Kingman's formula can be used to estimate QT [30]. Now in our proposed architecture ST is also dependent on latency due to message publishing and subscribing by microagents plus the sensor-block payload processing overhead k which will be constant for a given payload schema. So time delay between event occurrence and notification to subscriber equals to $(p + s)$ where p is latency for publish and s is latency for subscribe of sensor events. If we assume probability of publishing of any event e is $P(e)$ then modified service time can be estimated as:

$$ST' = ST + (p + s + k) * P(e). \tag{5.3}$$

we can assume event publishing is a Poisson process to calculate P. So that results modified response time as:

$$RT' = ST' + (ST' * u/(1 - u)). \tag{5.4}$$

Obviously this model holds true on assumption of a steady state system with all microagents are working; if any microagent is down it should be restored immediately. It can further evolve factoring different constraints and conditions for more accurate estimation.

Linh and Kim [43] proposed a Z-wave based smart home gateway and evaluated the performance in terms of command execution delay and its feasibility using Raspberry. Krishna et al. [21] designed and implemented a bidirectional Zigbee gateway that acts as a bridge between Zigbee networks and Wi-Fi-based MQTT networks, and this gateway provides storage and remote control functions. gave Rahmani et al. first proposed a conceptual framework of e-health smart gateway, then explored how to use the strategic position of the gateway to provide new functions for e-health and considering the challenges. UT-GATE provides efficient functions for health monitoring applications such as local storage, bioelectrical signal processing and data streaming, web socket servicing, protocol conversion and tunneling, firewall, notification and data analysis, and mining. and so on. Finally, by deploying it in a clinical scenario, they evaluated the system's energy consumption performance, interoperability, reliability, and security. In another step, Rahmani et al. extended this intelligent e-health gateway to the fog computing framework by providing an intelligent geographically distributed middle layer between cloud devices and sensors [55, 56]. With the help of fog, this plan can deal with many problems at a comprehensive level. Then, they presented UT-GATE and the entire system implementation in more detail, from development to hardware and software, to early warning scores of a fog-based clinical scenario. Finally, they demonstrated an IoT-based electronic health monitoring system with improved intelligence, mobility, energy efficiency, interoperability, reliability, and security. Ding et al. [16] studied a unified access gateway that can communicate with the machine-to-machine platform operator and provide multiple functions and service interfaces, from node configuration to service access, such as security including authentication. Authorization and decryption, QoS, web-based configuration. In addition, Ding et al. also created a test bed to test the performance of this gateway in terms of flexibility and deployment complexity. Considering the increase in the lifetime of sensors and energy acquisition, Galinina et al [18] discussed a Bluetooth-based smart gateway and smart home system with wireless energy transfer by a wireless energy transfer interface (WETI) from the home gateway to all battery-powered sensors. They built a dynamic flow-level 3D model to further estimate the data and energy transfer capabilities and thoroughly studied the performance limitations of WETI. Hosek et al [26] first discussed smart gateway technologies and then proposed an OSGi middleware home gateway based on IP Multimedia Subsystem with SIP. Ni et al. [50] designed and implemented a directional wireless IoT gateway made of S3C2440, JN5148 and VT6656 modules and evaluated the performance of this gateway by comparing with Wi-Fi-Bluetooth and Wi-Fi-ZigBee gateways. they did Yan et al. designed and implemented a multi-service, multi-interface intelligent gateway for smart home, which consists of IXP425, CS8016, BCM6338, Atmege128L, and CC2420 chipsets, and demonstrated the performance of the intelligent gateway in terms of throughput and light control command. they put [76] Zhang designed and implemented a home goal based on the triple play. He first presented hardware design and software design based on RTL8196C and MSM6290 chipsets and embedded Linux system respectively. Then he built a test environment and evaluated the performance of the system [54]. Angove and colleagues [4] proposed a mobile gateway framework that can provide long-distance interaction with mobile phones and wireless sensor nodes and short-range interaction with Bluetooth nodes. Unfortunately, the authors did not provide enough detail and did not evaluate their designs. Entering smart gateways that support cloud/fog computing, Pankakoski first analyzed and pointed out the complexity of home network management, the difficulty of content management, and the diversity of new network-enabled services as three key challenges during home development [66]. Therefore, to deal with these three problems, the author proposed a gateway-based system in an integrated way, which consists of a virtualization-based gateway framework, a gateway-based scheme to build social networks among different homes. The networks had a cloud-based file system for content management and sharing, and several other mechanisms for sharing resources between different gateways. Finally, the author evaluated the effectiveness of the prototype by running some case-based experiments. He and colleagues presented a home gateway framework based on cloud computing, which consists of four layers: physical layer, virtual devices layer, device management layer, and cloud access layer [69]. Although the above two gateways in [66] and [69] are only conceptual frameworks, they are the first two smart gateways based on the cloud framework in the smart home.

Sridhara et al [59] proposed a microservice-based IoT gateway scheme that enables sensor-to-cloud connectivity across different types of sensors, RF communication protocols, data packet formats, and even cloud service providers. The scheme can support an application-specific edge analysis module and a database to maintain sensor telemetry locally by providing 6LowPAN for sensor communication and Azure for cloud services. In smart gateways without cloud/fog computing support, Jae-Chul et al. [27] proposed a HNGS gateway architecture to connect home network and Internet. Based on Java technology and real-time operating system, this gateway is designed and developed by single-board X86 machines and Vxworks. As a prototype, this gateway only provides one Ethernet port, one IEEE1394 port, one internal and external interface, and does not support remote management and multi-service. Similarly, in order to connect different heterogeneous networks, Xie et al also proposed an embedded gateway architecture, but only focused on some data structures [74]. Valtchev et al [63] presented an OSGi service gateway architecture based on Java technology from a web services perspective. Although this architecture integrates some popular wired and wireless protocols, it is only a service gateway. Coincidentally, Bonino et al. [7] studied a DOG based on OSGi and Semantic Web technology, used a lightweight method to manage different internal networks, and tested the design ideas of generalization and authentication services. Arrizabalaga et al. [5] studied an OSGi MRG (Multiresidential Gateway) that supported VLAN, security, QoS, and multimedia services. In order to adapt to the dynamic environment and interoperability, Wu et al. [72] designed a peer-to-peer service-oriented architecture smart home system based on OSGi and mobile agent. Based on fuzzy logic and fuzzy neural networks, Lan and et al. [33] designed and implemented a smart home based on information integration from information acquisition, wireless and wired communication, intelligent control technology and user interface. Grill et al. designed and implemented a wireless smart home automation system that integrates a common gateway, Zigbee and Wi-Fi technologies [20]. In order to save energy, some smart home electrical systems have been developed and implemented as part of smart homes [52, 58]. Key components to implement smart gates In this section, we review and compare the key components for implementing smart gateways, namely the main operating systems and wireless technologies. operating systems The operating system plays an important role in the smart gateway and smart home system, because it not only provides the interface between hardware and applications, but also acts as a basic platform for the entire smart home software ecosystem. In general, two types of operating systems are used for smart homes: one for smart meters and the other for smart gateways [48]. For smart sensing devices, operating systems must consume little storage space and respond quickly, as surrounding sensors have only limited storage and processing capacity. For the smart gateway, the required performance of the operating system is higher than the previous one. Because a smart gateway typically has larger storage space, deals with more complex applications and services, runs different communication protocols, and supports more functions and security policies, the operating system must be a full-featured operating system. Mocrii et al [48] have reviewed many operating systems for sensor devices and gateways. Unfortunately, some important operating systems that can be used in smart gateways have not been investigated and reviewed, such as OpenWrt/LEDE, Raspbian, Windows CE (recently called Windows Embedded Compact), and Google Fuchsia.

6 Wireless communication technologies

In smart homes, wireless communication technologies are essential for the development of smart gateways, including Zigbee, WM-Bus, Z-Wave, DECT ULE, Bluetooth, Bluetooth LE, 6LowPAN, 802.11 series, Terahertz, etc. Mendez et al [46] comprehensively reviewed and compared wireless technologies. Unfortunately, DECT technologies especially DECT ULE, Wi-Fi below 1 GHz and terahertz are not included. Mocrii et al. did not discuss the aforementioned wireless technologies. DECT ULE is the latest version of DECT, which is one of the new generation of DECT or CAT-iq (advanced wireless technology-internet and quality) series. In addition, DECT ULE offers many outstanding features, such as low cost, low power consumption, long range, no interference, highly stable bit rate, value-added complementary audio and video capabilities. Compared to Wi-Fi and Z-Wave, DECT ULE has the advantage that the 1.9 GHz wavelength penetrates walls, floors and ceilings better. IEEE 802.11 is one of the most popular wireless standards, although it is also an evolving specification. In the 802.11 family, Wi-Fi IoT below 1 GHz has attracted much attention due to its support for IoT, which is related to 802.11af and 802.11ah 13. The first one, also called White-Fi or Super Wi-Fi, enables the implementation of WLAN in the television white space spectrum in the UHF and VHF bands from 54 to 790 MHz. The latter, also known as Wi-Fi HaLow, uses the 900 MHz license-exempt bands, supports lower power consumption and a large number of sensors. Compared to Bluetooth, 802.11ah has a competitive data rate and wider coverage range. THz band communication is considered as one of the primary wireless communication techniques to fulfill the future needs in 5G and beyond, its frequency band is from 0.1 to 30 THz (but it is usually 0.3-3 THz in practice) [1, 15, 19, 25, 53]. The use of the THz band addresses the spectrum shortage and capacity limitations of current wireless communications, thus enabling the Internet of Nanothings from the micro-smart home to macro-scale smart space and environmental intelligence. Data speeds can reach up to 100 Gbps or even terabits per second (terabits per second). Finally, THz communications facilitate high security and privacy as quantum cryptography can be applied.

6.1 Security and flow control

In smart homes, security issues mainly arise from the use of wireless communication technology due to their open channels as well as software security. Li et al. thoroughly reviewed the Internet of Things and investigated the related security and privacy [34, 36, 37, 41, 42]. In terms of wireless communication, recent smart gateways often use WPA/WPA2, AES-128 or even AES-256. and so on. In terms of software security, operating system security is very important for smart gates. Taking the OpenWrt operating system as an example, in order to facilitate security and intelligent gateway flow control, this system uses the Netfilter/Iptables technology provided by Linux. Netfilter is a Linux kernel firewall framework supported on advanced Linux distributions. The framework is both compact and flexible, and supports many security policy applications such as packet filtering, packet processing, transparent proxying, address hiding, dynamic network address translation (NAT), and filtering based on user and media access control addresses. Enables status, packet rate limiting, etc. Iptables is an advanced management tool based on the Netfilter framework. Defines tables, chains, and rules in Iptables to manage packets passing through various Netfilter hook points. The predefined Iptables tables are datagram modification table, datagram filter table and NAT table. Future challenges and trends in smart homes, QoE as well as data awareness is a key aspect in the long run. The smart gateway should connect the home network and the Internet, connect different types of smart appliances, convert different communication protocols between heterogeneous equipment, especially sense and process big data efficiently. In this sense, a smart gateway will face the basic challenges of a smart home system. We list them below, which shows the evolution of smart gates. (1) Usability For ease of use, the smart gateway should facilitate a simple and convenient operation, allow users to quickly install and configure the gateway, show concise and intuitive operation status, an easy-to-use management interface, locally or remotely. Give away. In addition, these require very fast system response and precise device synchronization, especially when the gateway also needs to send feedback from other devices to the user. This will lead to very critical challenges in system architecture design, protocol design and very good business collaboration between device suppliers. (2) Compatibility As smart home devices and IoT cloud platforms are becoming more complex, smart gateways must have a certain adaptability, that is, be compatible with different communication protocols and specific functions to collect and distribute data to smart devices. Smart gateways should also be compatible with different platforms and cloud services. Compatibility and adaptability bring great convenience to users and effectively increase the quality of user experience.

Scalability Deployment and use of smart homes is a gradual expansion process. Increases and decreases in the future are inevitable, so smart gates must adapt to different scales. Nowadays, smart home devices are very diverse. Gate design cannot consider all aspects comprehensively. Hardware and software interfaces and internal implementations must follow certain specifications, reduce coupling, have certain redundancy and extensibility capabilities, and be ready for future upgrades. In addition, in addition to fulfilling the necessary functions, the smart gate must also have a certain added value. At this stage, user behavior analysis can be a candidate. It often relies on a large amount of user data and complex learning algorithms, which are generally implemented in the remote cloud, so that many related factors can be learned together to optimize the smart home system. However, as hardware performance improves and algorithms become simpler, data analysis and learning algorithms become more decentralized to local devices, which requires matching software architecture and high hardware processing performance. In order to achieve the above goals, some basic techniques should also appear in the list of design components, such as SDN, AI, edge computing and data visualization. (4) Security issues are becoming more critical every day. Consider the smart home scenario, smart devices collect a large amount of user information and greatly affect the living environment and human activities. The smart home gateway must have a strong anti-attack capability. This means it can prevent illegal intrusion, malicious access, leakage of personal identity and authentication information in all possible processes such as user login, management and data interaction. It can also block unknown ports at risk to reduce equipment vulnerability. During data transmission, lightweight and complete encryption algorithms should be adopted to prevent damage and hacking by malicious people. There should also be a warning system in place when these do not work. Based on an established monitoring system, artificial intelligence techniques and visual analytics can also be applied to security. In the future, quantum communication and quantum encryption can also be used. (5) Privacy Not all actions aim to attack the smart home system. Instead, many individuals or organizations collect user data for specific business purposes, such as sorting out user habits and creating advertisements, or simply sell personal information for various uses. This may harm the privacy of information. A smart gateway should be able to erase collected or stored data and reconstruct the information when needed. A problem in this case is that when it is necessary to avoid excessive data storage on the cloud side, an efficient local or distributed storage scheme must be designed. In general, the next generation smart gateway will be a comprehensive gateway that will use advanced technologies including SDN, AI, edge computing, etc. to maximize QoE as well as data awareness in smart homes. Conclusion Smart homes enter our daily life, and the smart gateway as a main component in the smart home system bridges the home network and the Internet, connects different smart appliances, and converts different protocols among heterogeneous equipment. he does. In this paper, smart gateways were investigated and also the framework of smart home dependent on several smart agents was investigated. First, based on the timeline and different criteria, smart gates are divided into three generations. In the following, the smart gateways, which mainly belong to the second generation, are examined from the perspective of user awareness and data awareness. In addition, relevant core technologies for smart gateways, including operating system, wireless communication technologies, security, and flow control, are reviewed. Finally, the challenges and trends of smart gates are discussed. This article pointed out that the next generation smart gateway will be a comprehensive gateway that will use advanced technologies including SDN, AI, edge computing, etc. to maximize QoE along with data awareness.

References

[1] I.F. Akyildiz, C. Han and S. Nie, *Combating the distance problem in the millimeter wave and terahertz frequency bands*, IEEE Commun. Mag. **56** (2018), no. 6, 102–108.

[2] M. Alaa, A.A. Zaidan, B.B. Zaidan, M. Talal, M.L.M. Kiah, *A review of smart home applications based on internet of things*, J Netw. Comput. Appl. **97** (2017), 48–65.

[3] A.S. Alfakeeh, A.H. Al-Bayatti, F. Siewe and T. Baker, *Agent-based negotiation approach for feature interactions in smart home systems using calculus of the context-aware ambient*, Trans. Emerg. Telecommun. Technol. **33** (2019), no. 2, p. e3808.

[4] P. Angove, M. O'Grady, J. Hayes, B. O'Flynn, G. O'Hare and D. Diamond, *A mobile gateway for remote interaction with wireless sensor networks*, IEEE Sens. J. **11** (2011), no. 12, 3309–3310.

[5] S. Arrizabalaga, P. Cabezas, J. Legarda and A. Salterain, *Multi-residential gateway: an innovative concept and a practical approach*, IEEE Trans. Consum. Electron. **54** (2008), no. 2, 444–452.

[6] A.L. Ben and I. Jamai, *SDN, slicing, and NFV paradigms for a smart home: a comprehensive survey*, Trans. Emerg. Telecommun. Technol. **30** (2019), no. 10.

[7] D. Bonino, E. Castellina and F. Corno, *The DOG gateway: enabling ontology-based intelligent domotic environments*, IEEE Trans. Consum. Electron. **54** (2008), no. 4, 1656–1664.

[8] R. Borja, J.R. De La Pinta, A. Lvarez and J.M. Maestre, *Integration of service robots in the smart home by means of UPnP: a surveillance robot case study*, Robot Auton. Syst. **61** (2013), no. 2, 153–160.

[9] D. Bregman and A. Korman, *A universal implementation model for the smart home*, Int. J. Smart Home **3** (2009), no. 3, 15–30.

[10] P.M. Bull, P.R. Benyon and P.R. Limb, *Resident gateways*, BT Technol. J. **20** (2002), no. 2, 73–81.

[11] D. Chattopadhyay, A. Samantaray and A. Datta, *Device microagent for IoT home gateway: a lightweight plug-n-play architecture*, ACM SIGBED Rev. **15** (2018), no. 2, 16–23.

[12] A. Crabtree, T. Rodden, T. Hemmings and S. Benford, *Finding a place for UbiComp in the home*, UbiComp 2003: Ubiquitous Computing: 5th Int. Conf., Seattle, WA, USA, Springer Berlin Heidelberg, 2003, pp. 208–226.

[13] G. Cui, Q. He, X. Xia, F. Chen, H. Jin and Y. Yang, *Robustness-oriented k edge server placement*, 20th IEEE/ACM Int. Symp. Cluster Cloud Internet Comput. (CCGRID), IEEE, 2020, pp. 81–90.

[14] S.K. Das, D.J. Cook, A. Battacharya, E.O. Heierman and T.-Y. Lin, *The role of prediction algorithms in the MavHome smart home architecture*, IEEE Wirel. Commun. **9** (2002), no. 6, 77–84.

[15] S.S. Dhillon, M.S. Vitiello, E.H. Linfield, A.G. Davies, M.C. Hoffmann, J. Booske, C. Paoloni, M. Gensch, P. Weightman, G.P. Williams and E. Castro-Camus, *The 2017 terahertz science and technology roadmap*, J. Phys. D Appl. Phys. **50** (2017), no. 4, 1–49.

[16] F. Ding, A. Song, E. Tong and J. Li, *A smart gateway architecture for improving efficiency of home network applications*, J. Sens. **2016** (2016), 1–10.

[17] M. Diyan, S.B. Nathali, J. Han, Z.B. Cao and K. Han, *Intelligent internet of things gateway supporting heterogeneous energy data management and processing*, Trans. Emerg. Telecommun. Technol. **2020** (2020), no. 3, e3919.

[18] O. Galinina, K. Mikhaylov, S. Andreev, A. Turlikov and Y. Koucheryavy, *Smart home gateway system over Bluetooth low energy with wireless energy transfer capability*, EURASIP J. Wirel. Commun. Netw. **2015** (2015), no. 1, 178–185.

[19] S. Ghafoor, N. Boujnah, M.H. Rehmani and A. Davy, *MAC protocols for terahertz communication: a comprehensive survey*, IEEE Commun. Surveys Tutor. **22** (2020), no. 4, 2236–2282.

[20] K. Gill, S.-H. Yang, F. Yao and X. Lu, *A Zigbee-based home automation system*, IEEE Trans. Consum. Electron. **55** (2009), no. 2, 422–430.

[21] K.P. Gopi, K.S. Ravi, K.H. Kishore, K. Krishnaveni, K.N.S. Rao and RD. Prasad, *Design and development of bi-*

directional IoT gateway using ZigBeeand Wi-Fi technologies with MQTT protocol, Int. J. Eng. Technol. **7** (2018), no. 2, 125–129.

[22] M. Greeson, *Residential gateways: testing the waters of market viability*, In Proc. Residential Gateway European Forum 2001 Pre-Forum Wksp, 2001.

[23] F.T.H. Hartog, M. Balm, C.M. Jong, J.J.B. Kwaaitaai, *Convergence of residential gateway technology*, IEEE Commun. Mag. **42** (2004), no. 5, 138–143.

[24] Q. He, G. Cui, X. Zhang, F. Chen, S. Deng, H. Jin, Y. Li and Y. Yang, *A game-theoretical approach for user allocation in edge computing environment*, IEEE Trans. Parall. Distrib. Syst. **31** (2020), no. 3, 515–529.

[25] H. Elayan, O. Amin, R.M. Shubair and M. Alouini, *Terahertz communication: the opportunities of wireless technology beyond 5G*, Int. Conf. Adv. Commun. Technol. Network. (CommNet), IEEE, 2018, pp. 1–5.

[26] J. Hosek, P. Masek, D. Kovac, M. Ries and F. Kröpfl, *IP home gateway as universal multi-purpose enabler for smart home services*, Elektrotech. Informat. **131** (2014), no. 4-5, 123–128.

[27] M. Jae-Chul, L. Hyo-Sang and K. Soon-Ju, *Real-time event kernel architecture for home-network gateway set-top-box (HNGS)*, IEEE Trans. Consumer Electron. **45** (1999), no. 3, 488–495.

[28] S. Jaouhari, E. Palacios-Garcia, A. Anvari-Moghaddam and A. Bouabdallah, *Integrated management of energy, wellbeing and health in the next generation of smart homes*, Sensors **19** (2019), no. 3, p. 481.

[29] C.D. Kidd, R. Orr, G.D. Abowd, C.G. Atkeson, I.A. Essa, B. MacIntyre, E. Mynatt, T.E. Starner and W. Newstetter, *The aware home: a living laboratory for ubiquitous computing research*, Proc. Second Int. Workshop Cooperative Build., Pittsburgh, USA, Springer-Verlag **191** (1999), 191–198.

[30] J.F. Kingman, *The single server queue in heavy traffic*, Math. Proc. Camb. Philos. Soc. **57** (1960), no. 4, 902–904.

[31] P. Lai, Q. He, M. Abdelrazek, F. Chen, J. Hosking, J. Grundy and Y. Yang, *Optimal edge user allocation in edge computing with variable sized vector bin packing*, In Service-Oriented Comput.: 16th Int. Conf., ICSOC 2018, Hangzhou, China, Springer Int. Pub. **16** (2018), 230–245.

[32] P. Lai, Q. He, G. Cui, F. Chen, M. Abdelrazek, J. Grundy, J. Hosking and Y. Yang, *Quality of experience-aware user allocation in edge computing systems: a potential game*, IEEE 40th Int. Conf. Distrib. Comput. Syst. (ICDCS), IEEE, 2020, pp. 223–233.

[33] Z. Lan, L. Henry and K. Chan, *Information fusion based smart home control system and its application*, IEEE Trans. Consum. Electr. **54** (2008), no. 3, 1157–1165.

[34] Y. Li, *Design of smart home gateway based on Wi-Fi and ZigBee*, AIP Conf. Proc., AIP Publishing LLC **1955** (2018), no. 1, 040112.

[35] S. Li, *Editorial: zero trust based internet of things*, EAI Endors. Trans. IoT. **5** (2020), no. 20.

[36] S. Li, L. Da Xu and S. Zhao, *The internet of things: a survey*, Inf. Syst. Front. **17** (2015), no. 2, 243–259.

[37] S. Li, L. Da Xu and S. Zhao, *5G internet of things: a survey*, J. Ind. Inf. Int. **15** (2018), 1–9.

[38] S. Li and D.J. Deng, *Editorial: smart technologies improve our daily lives*, EAI Endor Trans IoT **5** (2019), no. 18.

[39] M. Li, W. Gu, W. Chen, Y. He, Y. Wu and Y. Zhang, *Smart home: architecture, technologies and systems*, Proc. Comput. Sci. **131** (2018), 393–400.

[40] R.Y.M. Li, H. Li, C. Mak and T.B. Tang, *Sustainable smart home and home automation: big data analytics approach*, Int. J. Smart Home **10** (2016), no. 8, 177–198.

[41] S. Li, H. Song and M. Iqbal, *Privacy and security for resource-constrained IoT devices and networks: research challenges and opportunities*, Sensors **19** (2019), no. 8, 1935.

[42] S. Li, T. Tryfonas and H. Li, *The internet of things: a security point of view*, Internet Res. **26** (2016), no. 2, 337–359.

[43] A.P. Linh and T. Kim, *A study of the Z-wave protocol: implementing your own smart home gateway*, 3rd Int. Conf. Comput. Commun. Syst. (ICCCS), IEEE, 2018, pp. 411–415.

[44] J.D. Little, *A proof for the queuing formula*, Oper. Res. **9** (1961), no. 3, 383–387.

[45] G. Liu, J. Wang, Y. Tian, Z. Yang and Z. Wu, *Mobility-aware dynamic service placement for edge computing*, EAI Endor. Trans. IoT. **5** (2019), no. 19.

[46] T.D. Mendes, R. Godina, E.M. Rodrigues, J.C. Matias and J.P. Catalão, *Smart home communication technologies and applications: wireless protocol assessment for home area network resources*, Energies **8** (2015), no. 7, 7279–7311.

[47] S. Meyer, A. Rakotonirainy, *A survey of research on context-aware homes*, Proc. Aust. Inf. Secur. Workshop Conf. ACSW Front. **21** (2003), 159–168.

[48] D. Mocrii, Y. Chen and P. Musilek, *IoT-based smart homes: A review of system architecture, software, communications, privacy and security*, Internet Things **1-2** (2018), no. 9, 81–98.

[49] M. Mozer, *The neural network house: an environment that adapts to its inhabitants*, In Proc. AAAI Spring Symp. Intell. Environ. **58** (1998), 110–114.

[50] Y. Ni, F. Miao, J. Liu and J. Chai, *Implementation of wireless gateway for smart home*, Commun. Netw. **5** (2013), no. 01, 16–20.

[51] S. Oh, J.H. Kim and G. Fox, *Real-time performance analysis for publish/subscribe systems*, Future Gener. Comput. Syst. **26** (2010), no. 3, 318–323.

[52] A. Pal, C. Bhaumik, J. Shukla and S. Kolay, *Energy information gateway for home*, Second Int. Conf. Intell. Syst. Modell.d Simul., IEEE, 2011, pp. 235–240.

[53] V. Petrov, J. Kokkoniemi, D. Moltchanov, J. Lehtomaki, Y. Koucheryavy and M. Juntti, *Last meter indoor terahertz: Wireless access performance insights and implementation roadmap*, IEEE Commun. Mag. **56** (2018), no. 6, 158–165.

[54] Z. Qifeng, *Research and implementation of intelligent home gateway based on triple play*, PhD Thesis, Yanshan University, 2012.

[55] A.M. Rahmani, T.N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang and P. Liljeberg, *Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: a fog computing approach*, Futur. Gener. Comput. Syst. **78** (2018), 641–658.

[56] A.M. Rahmani, N.K. Thanigaivelan, T.N. Gia, J. Granados, B. Negash, P. Liljeberg and H. Tenhunen, *Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems*, 12th Annual IEEE Consumer Commun. Network. Conf. (CCNC), IEEE, 2015, pp. 826–834.

[57] H. Schulzrinne, X. Wu, S. Sidiroglou and S. Berger, *Ubiquitous computing in home networks*, IEEE Commun. Mag. **41** (2003), no. 11, 128–135.

[58] L. Shaowei, L. Weimin, P. Xianmin and Z. Wei, *The communication model based on SIP and ZigBee for intelligent home electricity system*, Int. Conf. Multimedia Technol., IEEE, 2011, pp. 5594–5597.

[59] P. Sridhara, N. Kamath and S. Srinivas, *A microservices-based smart IoT gateway system*, Smart Intell. Comput. Appl. **2** (2019), 619–630.

[60] H.B. Stauffer, *Smart enabling system for home automation*, IEEE Trans. Consum. Electron. **37** (1991), no. 2.

[61] H. Sumi, *The gator tech smart house: a programmable pervasive space*, Comput. **38** (2005), no. 3, 50–60.

[62] A. Tsutsui, *Latest trends in home networking technologies*, IEICE Trans. Commun. **91** (2008), no. 8, 2470–2476.

[63] D. Valtchev and I. Frankov, *Service gateway architecture for a smart home*, IEEE Commun. Mag. **40** (2002), no. 4, 126–132.

[64] M.H. Vastenburg, D.V. Keyson and H. Ridder, *Considerate home notification systems: a field study of acceptability of notifications in the home*, Pers. Ubiquit. Comput. **12** (2008), no. 8, 555–566.

[65] M.H. Vastenburg, D.V. Keyson and H. Ridder, *Considerate home notification systems: a user study of acceptability of notifications in a living-room laboratory*, Int. J. Hum.-Comput. Stud. **67** (2009), no. 9, 814–826.

[66] P. Veikko, *Experimental design for a next generation residential gateway*, PhD Thesis, Aalto University, 2010.

[67] P. Wang, F. Ye and X. Chen, *A smart home gateway platform for data collection and awareness*, IEEE Commun. Mag. **56** (2018), no. 9, 87–93.

[68] P. Wang, F. Ye, X. Chen and Y. Qian, *Datanet: deep learning based encrypted network traffic classification in SDN home gateway*, IEEE Access **6** (2018), 55380–55391.

[69] Z. Wei, J. Li, Y. Yang and D. Jia, *A residential gateway architecture based on cloud computing*, IEEE Int. Conf. Software Engin. Service Sci., IEEE, 2010, pp. 245–248.

[70] M. Weiser, *The computer for the 21st century*, Sci. Am. **9** (1991), 94–104.

[71] M. Weiser, R. Gold and J.S. Brown, *The origins of ubiquitous computing research at PARC in the late 1980s*, IBM Syst J. **38** (1999), no. 4, 693–696.

[72] C.-L. Wu, C.-F. Liao and L.-C. Fu, *Service-oriented smart-home architecture based on OSGi and mobile-agent technology*, IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. **37** (2007), no. 2, 193–205.

[73] X. Xia, F. Chen, Q. He, G. Cui, P. Lai, M. Abdelrazek, J. Grundy and H. Jin, *Graph-based optimal data caching in edge computing*, Service-Oriented Comput.: 17th Int. Conf., ICSOC 2019, Toulouse, France, Springer Int. Pub. **17** (2019), 477–493.

[74] X. Xie, D. Deng and X. Deng, *Design of embedded gateway software framework for heterogeneous networks interconnection*, Proc. 2011 Int. Conf. Electron. Optoelect., IEEE, 2, 2011.

[75] K. Xu, X. Wang, W. Wei, H. Song and B. Mao, *Toward software defined smart home*, IEEE Commun. Mag. **54** (2016), no. 5, 116–122.

[76] W. Yan, Z. Wang, K. Zhang, J. Li and D. Zhang, *A multiple interfaces and multiple services residential gateway scheme*, Y. Tan, Y. Shi and H. Mo, (eds.) Int. Conf. Swarm Int., Berlin, Heidelberg/Germany, Springer, 7929, 2013, no. 376–384.

[77] A.A. Zaidan and B.B. Zaidan, *A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations*, Artif. Intell. Rev. **53** (2020), no. 1, 141–165.