

A.BELLO

ATILIM UNIVERSITY 2022

DESIGN AND IMPLEMENTATION OF IOT-BASED REFERENCE
ARCHITECTURE FOR SMART HOMES

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

ABDUSSAMAD BELLO

A MASTER OF SCIENCE THESIS
IN
THE DEPARTMENT OF COMPUTER ENGINEERING

JANUARY 2022

DESIGN AND IMPLEMENTATION OF IOT-BASED REFERENCE
ARCHITECTURE FOR SMART HOMES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

BY

ABDUSSAMAD BELLO

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF COMPUTER ENGINEERING

JANUARY 2022

Approval of the Graduate School of Natural and Applied Sciences, Atılım University.

Prof. Dr. Ender KESKİNKILIÇ
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of **Master of Science in Computer Engineering, Atılım University.**

Assoc. Prof. Dr. Gökhan ŞENGÜL
Head of Department

This is to certify that we have read the thesis DESIGN AND IMPLEMENTATION OF IOT-BASED REFERENCE ARCHITECTURE FOR SMART HOMES and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Ziya KARAKAYA
Supervisor

Examining Committee Members:

Prof. Dr. Murat KOYUNCU
Information Systems Eng. Department,
Atılım University

Asst. Prof. Dr. Ziya KARAKAYA
Computer Eng. Department,
Atılım University

Assoc. Prof. Dr. Ahmet Murat ÖZBAYOĞLU
Computer Eng. Department,
TOBB University of Economics and Technology

Date: 24th January, 2022

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Abdussamad, Bello

Signature :

ABSTRACT

DESIGN AND IMPLEMENTATION OF IOT-BASED REFERENCE ARCHITECTURE FOR SMART HOMES

Bello, Abdussamad

M.Sc., Department of Computer Engineering

Supervisor: Asst. Prof. Dr. Ziya KARAKAYA

January 2022, 62 pages

Interoperability, which is the ability of applications, systems, devices, and services to work together reliably and consistently, is one of the most important problems of current smart home systems. The lack of interoperability and the accompanying technological partitioning (that is, managing different devices in the same environment with different applications) creates a major barrier for smart home developers and resistance to consumer acceptance of IoT products in their home environments.

The aim of this study is to create a IoT-based Smart Home Reference Architecture that will manage, monitor, and process the data coming from devices and services in the smart home environment while increasing the interoperability. This study also presents a proof-of-concept solution for the proposed reference architecture using FIWARE components. In conducting this study, we made use of constructive research methodology and the ProSA-RA process to analyze existing works, their underlying issues, and then propose solutions to them.

To further bridge the gaps in the smart home ecosystem, it is suggested that smart home developers adopt the reference architecture proposed in this study while developing their architectures, applications, and devices.

Keywords: IoT, Smart Home, Reference Architecture, Smart Home PoC Application, FIWARE, ProSA-RA

ÖZ

AKILLI EVLER İÇİN NESNELERİN İNTERNETİ (IoT) TABANLI REFERANS MİMARİSİ TASARIMI VE UYGULAMASI

Bello, Abdussamad

Yüksek Lisans, Bilgisayar Mühendisliği

Tez Yöneticisi : Asst. Prof. Dr. Ziya KARAKAYA

Ocak 2022, 62 sayfa

Birlikte Çalışabilirlik olarak adlandırılan; uygulamaların, sistemlerin, cihazların ve servislerin birlikte güvenilir ve tutarlı bir şekilde çalışabilmesi günümüz akıllı ev sistemlerinin en önemli sorunlarından biridir. Birlikte çalışabilirlik eksikliği ve buna eşlik eden teknolojik bölümlenme (yani, aynı ortamdaki farklı cihazların farklı uygulamalar ile yönetilmesi) akıllı ev geliştiricileri için büyük bir bariyer ve tüketicilerin ev ortamlarındaki IoT ürünlerini kabullenilmesine karşı direnç oluşturmaktadır.

Bu çalışmanın amacı, birlikte çalışabilirliği artırırken akıllı ev ortamındaki cihaz ve hizmetlerden gelen verileri yönetecek, izleyecek ve işleyecek IoT tabanlı bir Akıllı Ev Referans Mimarisi oluşturmaktır. Bu çalışma aynı zamanda, FIWARE bileşenlerini kullanarak önerilen referans mimarisine uygun bir kavram kanıt çözümünü ortaya koymaktadır. Bu çalışmanın yürütülmesi sırasında mevcut çalışmalar ve sorunları analiz edilmiş, bunlara çözüm sunmak için ise yapıcı araştırma metodolojisi ve ProSA-RA süreci kullanılmıştır.

Akıllı ev ekosistemindeki uçurumları kapatmak üzere akıllı ev geliştiricileri, mimarilerini, uygulamalarını ve cihazlarını oluştururken bu çalışmada önerilen referans mimariyi benimsemesi önerilmektedir.

Anahtar Kelimeler: Nesneleri İterneti (IoT), Akıllı Ev Sistemleri, Referans Mimari, Akıllı Ev Kavram Kanıtı Uygulaması, FIWARE, ProSA-RA



To My Family

ACKNOWLEDGMENTS

I would like to thank my supervisor, Asst. Prof. Dr. Ziya Karakaya, for all his assistance, guidance, advice and constructive suggestions during this research.

I would also like to thank my thesis committee members Prof. Dr. Murat KOYUNCU and Assoc. Prof. Dr. Ahmet Murat ÖZBAYOĞLU for their valuable suggestions and comments.

Finally, I would like to thank my family for their love, support and encouragement which made it possible to complete this work.

TABLE OF CONTENTS

ABSTRACT.....	iii
ÖZ	iv
DEDICATION	v
ACKNOWLEDGMENTS	vi
TABLE OF CONTENTS.....	vii
LIST OF TABLES	x
LIST OF FIGURES	xi
LIST OF SYMBOLS/ABBREVIATIONS	xii
CHAPTER	
1. INTRODUCTION	
1.1 Overview of Smart Home Industry	1
1.2 Problem Statement	2
1.3 Objectives of The Research	3
1.4 Research Questions	3
1.5 Significance of The Study	3
1.6 Limitations	4
1.7 Background of The Study	4
1.7.1 Smart Homes.....	4
1.7.2 IoT.....	5
1.7.3 Reference Architecture.....	7
2. LITERATURE REVIEW	
2.1 Definition of Smart Home.....	9
2.2 History of Smart Homes	9
2.3 Smart Home Applications	10
2.4 Artificial Intelligence Application in IoT Smart Homes.....	11
2.5 Communication Channels Used in IoT Smart Homes	12
2.5.1 Wi-Fi	12
2.5.2 Bluetooth.....	13

2.5.3	Cellular	13
2.5.4	Wave	13
2.5.5	Near Field Communication (NFC).....	14
2.6	IoT vs Industrial IoT (IIoT).....	14
2.7	Reference Architecture in Smart Homes.....	15
2.8	Smart Homes Problems and Solution	16
3.	RESEARCH METHODOLOGY	
3.1	Research Design and Strategy.....	18
3.2	Reason for Selection of Methodology.....	19
3.3	Constructive Methodology Steps	19
3.4	Consolidated Process for Reference Architecture Design, Representation, and Evaluation.....	20
4.	ANALYSIS OF REFERENCE ARCHITECTURE AND SMART HOMES	
4.1	Connectivity Type.....	23
4.1.1	LAN	23
4.1.2	WAN	24
4.2	Service Type.....	25
4.2.1	Utility	25
4.2.2	Entertainment	25
4.2.3	Comfort	25
4.2.4	Security	25
4.3	Essential Characteristics of IoT Reference Architecture	26
4.3.1	FIWARE IoT Reference Architecture	27
4.3.2	ITU IoT Reference Architecture	29
4.3.3	WSO2 Reference Architecture.....	30
4.3.4	Analysis of Current Smart Home Architectures	32
4.3.5	Comparison Between Reference Architectures	36
4.3.6	Comparison Between Smart Home Architectures	36
5.	CONSTRUCTION OF IOT BASED SMART HOME REFERENCE ARCHITECTURE	
5.1	Characteristics of the Proposed IoT-based Smart Home Reference Architecture.....	38

5.2	Proposed IoT-based Smart Home Reference Architecture Diagram ..	40
5.3	Home Environment	41
5.3.1	Device Layer	41
5.3.2	IoT Gateway	41
5.3.3	Embedded Device	42
5.3.4	Service Layer	42
5.3.5	Security	44
5.3.1	Communication	44
5.4	Cloud Environment	46
6.	IOT BASED SMART HOME APPLICATION ARCHITECTURE PROOF OF CONCEPT	
6.1	Functional Requirements	48
6.2	Non-Functional Requirements	48
6.3	Implementation of IoT-based Smart Home Application Architecture Using FIWARE	48
6.4	Smart Home PoC Application Architecture Components	52
7.	DISCUSSION AND CONCLUSION	
7.1	Discussion	54
7.2	Research Questions	54
7.2	Conclusions	56
7.2	Future Works	57
	REFERENCES	58

LIST OF TABLES

TABLES

Table 4.1 A Comparison Between Reference Architectures	36
Table 4.2 A Comparison Between Smart Home Architectures	36
Table 5.1 Solution to Reference Architecture Criteria.....	39
Table 5.2 Communication capabilities of connection label 1	45
Table 5.3 Communication capabilities of connection label 2	45
Table 5.4 Communication capabilities of connection label 3	45
Table 5.5 Cloud Environment Communication Capabilities Label 5 & 6.....	46
Table 6.1 Mapping Derived Reference Architecture to Application Architecture	49

LIST OF FIGURES

FIGURES

Figure 1.1 Basic IoT Architecture.....	7
Figure 3.1 Constructive Research Methodology.....	19
Figure 3.2 The ProSA-RA Process	22
Figure 4.1 LAN smart home connectivity	24
Figure 4.2 WAN smart home connectivity	25
Figure 4.3 FIWARE reference architecture	27
Figure 4.4 ITU reference architecture	29
Figure 4.5 WSO2 reference architecture.....	31
Figure 4.6 Li et al. Smart Home Architecture.....	32
Figure 4.7 Mocri et al. Smart Home Architecture	33
Figure 4.8 Pürgstein et al. Smart Home Architecture	34
Figure 4.9 Bing et al. Smart Home Architecture	35
Figure 5.1 Proposed IoT-based Reference Architecture for Smart Homes	40
Figure 6.1 Smart Home Application Architecture	50
Figure 6.2 Keyrock Identity Management Dashboard Screen	51
Figure 6.3 Keyrock Application and Device Configuration Screen	51
Figure 6.4 Application Device Management Screen When Logged in	52
Figure 6.5 Application Device History Charts.....	53

LIST OF SYMBOLS/ABBREVIATIONS

AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
API	Application Package Interface
CoAP	Constrained Application Protocol
DSU	Data Storage Units
GDPR	General Data Protection Regulation
HVAC	Heating, Ventilation, and Air Conditioning
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IERC	IoT European Research Cluster
IoT	Internet of Things
IIoT	Industrial Internet of Things
ITU	International Telecommunication Union
JSON	Javascript Object Notation
LAN	Local Area Network
LoRaWAN	Long Range Wide Area Network
LTE-MTC	Long Term Evolution for Machine Type Communication
LWM2M	Light weight Machine to Machine
M2M	Machine to Machine
MQTT	Message Queuing Telemetry Transport
NB-IoT	Narrowband-Internet of Things
NFC	Near Field Communication
NI	Network Infrastructure
NGSI-V2	Next Generation Service Interfaces - Version 2
NGSI-LD	Next Generation Service Interfaces - Linked Data
PoC	Proof of Concept
REST	Representational State Transfer

RFID	Radio-frequency Identification
SSDB	Smart Software-defined Building
SDN	Software-defined Networking
TCP	Transmission Control Protocol
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
UDP	User Datagram Protocol
WAN	Wide Area Network
WiMax	Worldwide Interoperability for Microwave Access
VS	Virtualized Server
XMPP	Extensible Messaging and Presence Protocol
XMPP-IOT	Extensible Messaging and Presence Protocol Internet of Things



CHAPTER 1

INTRODUCTION

The Internet of Things (IoT) has brought significant changes in the world today because it has completely changed how things are done, and the way people live, interact and work. Through IoT, we are saying bye to the era of manually operated devices in our homes, places of work, cars, hospitals, and many other areas. IoT is playing a vital role in improving the quality of life and advancing the economy globally. The advancement of communication and computer technology together with IoT has resulted in the creation of smart homes. Today, IoT technologies have been integrated into homes to operate many of the functions of the house. For instance, these devices control security, heating, lighting, curtains, baths, audio-visual systems, and many other appliances in a house [1]. The IoT-based reference architecture comprises several aspects such as a server or cloud-side architecture that enables the user in managing, monitoring, interacting with, and processing data from IoT devices.

1.1 Overview of Smart Home Industry

The smart home industry has experienced tremendous growth. The first smart house was started in the late 1900s and early 2000s. Since then, electronic devices and appliances using IoT started to be developed and installed in houses. In the 20th century, system designers, engineers, and architects worked hard to create smart adoptive homes. By 2013, there were at least 2 billion smart homes in the world and by 2018 the numbers were expected to increase to 9 billion [2]. Also, Gartner [3] estimated 50 billion connected devices at the end of 2020. Today, the global smart home industry market is worth more than \$46 billion [4].

The quick growth of the smart home industry is attributed to technological advancements including IoT and increased awareness among people.

However, there is slow uptake of smart homes among the lower-class people because of the high initial investment needed [1]. Furthermore, some smart home technologies developed do not provide solutions that meet the needs of the users. Another issue that has hindered the swift progress of smart homes is the lack of accurate ecosystem interoperability. In other words, the product developers are not creating devices and systems that can work together under one platform.

There has been a recent effort to standardize IoT-based smart homes. An instance is matter “Matter” which is a protocol developed by the Connectivity Standards Alliance (formerly Zigbee Alliance) to allow intercommunication between devices. W3 “Web of Things Architecture” has also created a generic standard for device data model and architecture. However, for smart homes in particular, there has not been any universally accepted reference model or standards.

1.2 Problem Statement

Interoperability, which is the ability of applications, systems, devices, and services to function together in a reliable and consistent manner, is a problem in smart homes. Developers are supposed to adapt their devices applications to different smart home configuration. However, missing interoperability and technology fragmentation in Internet of Things is a huge barrier for developers and has contributed to the lack of acceptance of IoT ecosystems [5]. Technology fragmentation is managing different devices in the same environment with different applications. Various communication technologies are used in smart home automation systems including Wi-Fi, Bluetooth, ZIGBEE, RFID, etc. [6]. Some of these systems and technologies have some drawbacks in effective control and monitoring the smart home components. The devices and appliances used in smart homes have their own data formats, APIs, and IoT infrastructures, hence resulting in interoperability problems [7]. These issues bring challenges in enabling the devices to communicate with each other and work together effectively. These problems have hindered the development of IoT

applications and devices that can run well in cross-domain or cross-platforms. This, in turn, has prevented the introduction of IoT technologies for smart homes on a large scale.

1.3 Objectives of The Research

- To create a reference architecture for smart homes that will manage, monitor, and process data from the appliances in the home.
- Create a reference architecture that would also help solution providers to utilize data analytics and Artificial (AI) tools to produce innovative smart home solutions.
- Proposes a high-level reference architecture for smart homes based on the FIWARE technology that addresses the interoperability issue.
- Implement a proof-of-concept (PoC) solution complying with the proposed reference architecture that presents a networking model used to communicate with devices and appliances in smart homes

1.4 Research Questions

1. Is there any IoT-based smart home reference architecture already developed and being implemented?
2. What are the drawbacks of current smart home architectures?
3. Does using IoT-based reference architecture, to create devices and appliances for smart homes, helps to overcome interoperability issues?
4. Is it possible for the services, devices, appliances, applications, and systems in a smart home work together reliably?
5. How can we design a reference architecture and implement a proof-of-concept for an IoT-based Smart home?

1.5 Significance of The Study

This study starts with explaining the current state-of-the-art technology and contributes to the smart home industry by proposing a reference architecture which is

linked to the main problems in service-oriented architecture, especially addressing the interoperability problem. It will contribute to the effort to have different devices and applications in a smart home to communicate and send information and work with each other. The use of reference architecture proposed in this study will contribute to the standards that will be used in IoT devices that work together. This research will also contribute to the literature on designing smart homes, specifically, IoT-based reference architecture for smart homes.

1.6 Limitations

Our methodology did not make use of extensive expert interviews from smart home experts due to their physical unavailability. Also, when implementing the proof of concept for our design we limited it to the use of virtual devices (things). Another limitation of our study is achieving true interoperability, our design does not guarantee a complete future proof solution or backward compatibility.

1.7 Background of The Study

1.7.1 Smart Homes

There are several definitions of a smart home. A smart home can be defined as an automatic setup used in a home comprising a variety of appliances and devices used in lighting, curtains, doors, kitchen, security, entertainment, and in many other areas. A “smart home” can also be seen as a home which is automated through the application capable of reacting to requirements of the inhabitants, providing them comfort, security, safety, and entertainment.

These devices and appliances are often controlled and monitored using internet-enabled network devices and mobile phones remotely. They can also be controlled by voice commands. Another definition of a smart home is a home having an automated system that includes device controllers and sensors to offer a secure, intelligent, and comfortable environment that will enhance the quality of life [8]. Smart homes consist of major components including the intercom system, security

system, air conditioning, heating and ventilation system, lighting system, entertainment systems, and kitchen system. In most cases, these components are interconnected via the internet to give the user on-demand access using mobile phones or voice commands.

1.7.2 IoT

There are several definitions of the Internet of Things. Islam et al. [6] defined IoT as a system that uses the internet to connect devices or things to interact with each other to perform a certain action. It is also a system that offers interesting solutions to most glitches facing the world today [9]. IoT is also defined as a computing paradigm that is likely to transform how people live and perform their daily duties [10].

IoT, also known as “Web of Things”, is a concept used to describe the internetworking of devices. It is also named as “Machine to Machine Communication (M2M)”. There is no single definition to define it yet because it is a field that is fast evolving, however, there have been several attempts by different experts and institutions to explain it. Some definitions provided by standardization bodies are cited as follows.

IEEE: “A network of items—each embedded with sensors—which are connected to the Internet.” [11].

IERC: “A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.” [12].

ITU: In the Recommendation ITU-T Y.2060, “IoT has been defined as a global infra- structure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.” [13]. The Internet of Things has many applications in different industries such as surveillance, industrial

automation, smart cities, transportation, smart grid, smart health care, and smart home just to mention a few. Nevertheless, despite its application in numerous industries, its application in smart homes has drawn a lot of interest from real estate investors, clients, government, and home appliance production companies [8]. This is because smart home technologies are linked to the lives of people and affect how they live.

The building blocks of IoT include things, cloud infrastructure, network infrastructure, and gateways. Things comprise the focused areas where sensors and actuators are used to sense the information and actuate a function appropriately in case of needs. It allows communication and collection of data from the objects of concentrated areas using IoT devices such as actuators and sensors [9].

Cloud infrastructure is a component needed for computing, networking, information storage and processing. It utilizes devices such as data storage units (DSU) and virtualized servers (VS) to permit logical, analytical, and advanced computing capabilities. Network infrastructure (NI) comprises the devices such as repeaters, gateways, aggregators, and routers to allow the smooth and secure flow of information and to provide control over the information [9]. Thus, NI enables control over the information from the things to the cloud infrastructure. Gateways is another block of IoT that plays a vital role of being an intermediate block to allow strong connectivity between cloud infrastructure and things.

The goal of IoT is to measure physical parameters with sensors, transmit it for processing and then send it back to actuators to act on it or display it to an interface for interpretations. A reference architecture of IoT contains an interconnection of Sensors, Actuators, Devices, Gateway, Integration Middleware and Application [14], with each layer communicating via different protocols. The Figure 1.1 shows how these components and interfaces are stacked.

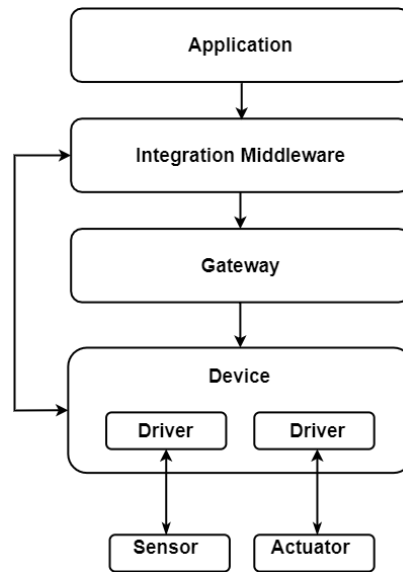


Figure 1.1 Basic IoT Architecture

Smart home architecture is different, in its dynamic nature, from general IoT applications because of the devices, the network and data model which are produced by different manufacturers and may keep changing frequently due to user preference.

Also, smart home networks can be limited to only within the home while general application interacts with other cloud-based services.

This necessitates the smart home solution to work without any cloud service interferences. The data model of smart homes also varies because device specification varies, unlike general IoT applications that might have standardized data.

1.7.3 Reference Architecture

In the IoT domain, many diverse reference architectures have been established. They have the function of either specifying a specific type of implementation or generalizing its numerous applications. There are numerous definitions of reference architecture. Reference architecture is defined as a set of documents that offer recommended structure and integration of information technology services and products to create a solution. It comprises the lists of functions as well as some

suggestions of their interactions, APIs, and interfaces. The reference architecture model signifies sophisticated multi-dimensional architecture frameworks disintegrated into different architecture outlooks for providing a comprehensive understanding of software systems [15]. Clements, Garlan, Little, Nord, & Stafford [16] defined a software reference architecture as a fundamental structure where the configurations and corresponding elements offer outlines for actual architectures in a specific domain.

Reference architectures define guidelines vital for planning the implementation of software systems, hence bringing standardization. Ataei and Litchfield [17] defined reference architecture as a guideline that helps to define the body of the system, its patterns, behaviours, relationships, key components, and limitations. The reference architecture provides a template solution used to design software systems to accomplish standardization of the discrete sub-systems. In addition to providing standardization of tangible architectures, reference architecture can also be used to recommend an initial architectural proposal that can be utilized in designing concrete architectures in specific domains [18].



CHAPTER 2

LITERATURE REVIEW

2.1 Definition of Smart Home

A smart home is a residential environment that incorporates technology to permit and allow other systems to be controlled automatically. This implies that a smart home is a dwelling environment where communication networks are incorporated to link major electrical appliances as well as services to allow them to be controlled and monitored remotely [19]. Smart homes help their inhabitants to have a life that is comfortable, independent, safe, secure, and environmentally friendly through energy conservation [20]. To Yang, Lee & Lee [21], a smart home is a combination of numerous organic subsystems that are linked to home life over advanced technologies. The technology can exchange resources and pass information within a home setting. Its main objective is to offer people a life that is comfortable, safe, and convenient, efficient as well as environmentally friendly.

2.2 History of Smart Homes

The idea of smart homes was introduced to incorporate smartness and technology into the house to enhance its security, safety, comfort, and energy conservation. The history of smart homes can be traced back to the late 1900s and early 2000s. Homes were made more sophisticated with the introduction of computers in the 1940s [1]. During the 1980s, programming was instituted in the automation of home devices. Some of the devices that were programmed to be used in the house included a digital thermostat, dishwasher, and washer-dryer. During the same period, security systems, automatic garage door openers, were introduced [1].

Today, there are smart homes that enable users to control home devices and appliances remotely. Alam, Reaz, and Ali [20] observed that there are smart homes in which the users can execute tasks even before they arrive home. There are also ambient intelligence systems that have been installed with the function of monitoring smart homes. Technology continues to advance each day and hence the future buildings and homes are expected to get smarter and more automated [22]. In the future, Smart Home solutions may need to be integrated with other Smart Solutions, such as Smart Buildings, Smart Energy (Grids), Smart City, etc.

2.3 Smart Home Applications

Marikyan et al. [23] are of the opinion that a smart home is a type of residence that employs devices that are internet-connected to allow remote monitoring as well as management of the appliances for lighting, heating. The systems of smart homes often work together, exchanging information about consumer usage among themselves and programming actions based on the preferences of homeowners. It involves the utilization of computers, regulation technology, and technology of image display as well as communication technology are linked through a network of numerous facilities combined to achieve the automation demands of the whole system for easier regulation and management as recommended by Alaa et al. [24].

With the current technological innovations, Almusaylim & Zaman [25] suggest that in all aspects of home life, the smart TVs link to the internet to access information through applications such as on-demand video, voice, gesture recognition, and music. Smart thermostats have an integrated Wi-Fi that allows occupants to program, monitor, and regulate home temperature remotely. The devices can learn the behavior of homeowners and spontaneously modify settings to offer residents maximum luxury and efficiency. Additionally, smart thermostats can analyze total energy consumed and remind the homeowners to make required changes such as a change of filters [24].

Smart locks are another type of smart home application that is employed in locking doors to give or deny permission to visitors. They can also detect when homeowners

are around and unlock the doors. Using smart home security cameras, homeowners can monitor their properties while on vacation. The smart motion detectors can acknowledge the variation between visitors, pets, and residents and send a notification to the administrators in case they detect any suspicious behavior. Kitchen appliances such as smart coffee makers, smart refrigerators can be automated to make a coffee cup at specific programmed times, track the list of products that have expired, create shopping lists, come up with recipes by examining the remaining ingredients respectively. Pet care can be programmed and linked to the feeder store to feed the pets even in the absence of the homeowners [25].

To Meier et al. [26] smart homes accommodate the preferences for user convenience, such as programming the garage door to close and open at certain times, the fireplace on or off depending on the situation at hand. All this ensures that the efficiency of a given home is enhanced. However, Marikyan et al. [23] argues that smart homes have a lot of complex programs that make it inconvenient for homeowners without technical know-how. Another challenge is that the privacy and safety of the homeowners are sacrificed more especially when hackers infiltrate the system.

2.4 Artificial Intelligence Application in IoT Smart Homes

The current business arena has changed due to IoT adoption. The IoT helps to capture a piece of incredible information from numerous sources. However, wrapping all this information coming from numerous IoT devices has made it more complex to gather, process, and examine. Calo et al. [27] through their study, postulate that the incorporation of Artificial Intelligence with IoT can help in redefining how businesses and industries are run by decentralizing and improving decision making.

Machine learning (ML) that is coupled with AI helps in predicting operation conditions and senses the parameters that need modification to guarantee ideal outcomes. Intelligent IoT provides more insights on the processes that are time-wasting and redundant as well as how to address them to ensure efficiency as outlined by Singh, Rathore & Park [28].

Moreover, Hargreaves, Wilson & Hauxwell-Baldwin [29] debated that incorporating AI and IoT helps enterprises in understanding and predicting numerous risks to come up with prompt responses to address the gap. This allows them to deal with the safety of the workers, cyber-crimes, and financial losses. The incorporation also helps in triggering new products while enhancing the previous ones. This provides businesses and consumers an opportunity to process and interpret data easily.

To Kim, Park, Lee & Kim [30], marrying AI and IoT increases the scalability of IoT making it easier and convenient to analyze data and provide summarized data from the device before it is being transferred to other IoT devices. This reduces data capacity and allows linking to numerous IoT devices. Lastly, the incorporation allows the business to predict machine failure early and come up with a maintenance schedule. This helps businesses to avoid the effects of unplanned downtime [31]. We think that all these business opportunities and capabilities are also valid for the smart home environment and solutions.

2.5 Communication Channels Used in Smart Homes

As Çorak et al. [32] stated, standardized communication channels avail several benefits to the end-users. The benefits include quality and credible communication, flexibility to innovation and interoperability, and global scalability. To Hejazi et al. [31], in the industrial and consumer segment, enterprises have several IoT protocol choices. The end-user needs to acknowledge that every protocol has distinct structures and potentials. Some major communication protocols includes;

2.5.1 Wi-Fi

Wi-Fi is wireless technology for connecting devices and used in many homes. It usually has a frequency ranging from 2.4 GHz to 5 GHz bands with data rates being 600 Mbps at maximum with 150-200 Mbps being common. The link works well in local area network (LAN) environments, where it provides an opportunity for faster transfer of data. It can process huge amounts of information, that is a reason why it is utilized by many homes and businesses [31].

2.5.2 Bluetooth

This is short-range communication technology. It is suitable when used in transferring small data for individual products. It is commonly used in mobile devices. With minimal power consumption, the technology forms the IoT foundation because it is flexible and scalable to any market innovations. Currently, new products such as Bluetooth Low-Energy and Bluetooth Smart are the new consumer products in the market [31].

2.5.3 Cellular

Cellular IoT communication protocols do not require pre-established gateways for them to come up with coverage areas. Though cellular networks can facilitate massive data flow, those that are IoT enabled employ a ton of energy. Therefore, the cellular protocols help in enhancing connectivity whenever there is a need to link objects such as streetlights, parking meters, and hospitals as well as other industrial applications. Because of their infrastructural simplicity incorporated with fifth-generation mobile network evolution, the communication protocol has gained attraction from all sectors as demonstrated by [33].

2.5.4 Wave

This is a communication protocol that is wireless, based on low power radio frequency technology. It is highly recommended for automation of home products such as sensors and lamp controllers to mention a few. The technology covers layers beginning from physical to network communication applications [33].

2.5.5 Near Field Communication (NFC)

NFC is a widespread IoT communication protocol. This is because of market opportunities for smartphones. It allows customers to make payments that are contactless through their phones. This type of IoT communication protocol employs electromagnetic induction among two aerial loops that are located within each other's

field. In this manner, it can extend the potentiality of contactless card innovation expertise and enable devices to exchange information within 4 cm. The NFC permits communication in two modes, namely passive communication, and active communication mode. The passive communication mode is where a radio frequency field is generated by only one device and the second device employs a load modulation technique to transfer information to the initiator. On the other hand, in an inactive communication mode, all the devices generate radio frequency signals from which information is exchanged [34].

2.6. IoT vs Industrial IoT (IIoT)

The IoT and IIoT often have similar acronyms, but they are not the same. They are two technologies that are parallel with similar standardized protocols that are borrowed from one another. Even though they have similar interphase, agility, as well as intelligence, their principle of operation, user, and objectives, are different.

The IoT aids in optimizing utility consumption, accentuating individual luxury, and regulating expenses, whereas IIoT works to attain efficiency that is maximum with a smooth workflow. Furthermore, the IoT is employed in automating household processes while IIoT is mainly used in production monitoring as well as business operations parameters. According to Meier et al. [26] the technology behind the IoT operations is not new. However, its utilization in customers and enterprise markets continues to revolve, whereas the solutions to industrial IoT demand the capacity to maintain its cycle life for efficient resolution.

Moreover, the IoT solutions contain programmable learning potentials in their system design to integrate the regulation and automation logic in gateways that have systems of production execution that are new. On the contrary, the IIoT architecture is designed in a manner that suits the needs of low latency when handling failures or any process malfunction through immediate independent re-routing to the stoppage system. Finally, the IIoT solutions demand several safety procedures for them to detect any malicious attacks of IoT systems in their management processes. The IIoT keeps evolving with standards that are open, giving way for disruptive technologies,

ease of utilization, and reduced cost innovations to integrate the cooperative ecosystem by synchronizing it with numerous protocols, information sets, and enterprise resource planning systems, just to mention a few [26].

2.7 Reference Architecture in Smart Homes

According to Chauhan & Babar [18], the reference architecture is used to design IoT systems to attain standardization of the discrete sub-systems. Apart from providing standardization of tangible architectures, reference architecture can also be used to recommend an initial architectural proposal that can be utilized in designing concrete architectures. A reference architecture comprises a comprehensive life cycle of instantiation of a particular type of architecture [18].

Ghirardello et al. [15] examined the development of reference architecture for smart homes to enable security analysis. They found out that there should be a high-level reference to architecture to map smart home services and products with the aim of facilitative security analysis in the inhabited internet of things systems. Ghirardello et al. [15] noted that in the IoT domain many diverse reference architectures have been established. They have the function of either specifying a specific type of implementation or generalizing its numerous applications. The reference architecture model signifies sophisticated multi-dimensional architecture frameworks disintegrated into different architecture outlooks for providing a comprehensive understanding of IoT systems.

In their study, Mazzara et al. [35], proposed a four-layered reference architecture that can be used for smart homes and buildings generally termed as Smart and Software-defined Buildings (SSDB). Their smart home reference architecture layers include application and service, management, network, and hardware. The hardware layer is found at the bottom of the stack, and it comprises the features associated with the smart home infrastructure, starting with IoT smart objects to network, actuators, sensors, devices, and storage and processing hardware facilities. The next layer is the network that provides objects, devices, and SSDB nodes that, in turn, provides solutions and mechanisms that are interconnected. Another layer is the management

layer, which has the responsibility of managing infrastructure utilized in handling smart homes [35]. The topmost layer is the application and service layer.

2.8 Smart Homes Problems and Solution

Ali, Dustgeer, Awais & Shah [36] postulated that even though the smart home offers convenience to the users, issues of security and privacy on the users have been raised. Using the WannaCry incident as an example, it is evident that the security design provides an excellent opportunity for hackers to attack and weaken devices that are commercially available in the market. This is because the devices lack essential features that can help in preventing the penetration of malicious users.

According to Stojkoska & Trivodaliev [37], several smart home devices such as Nest Smoke Alarms, Smart Body Analyzer, and Belkin WeMo motion devices are vulnerable to numerous security threats. Zheng et al. [38] proposed that the privacy of the end-user is another challenge that is facing smart home IoT because they contain a lot of individual data that malicious attackers can mine. These two issues have continued to increase over the years, and there is a need for technology innovators as well as consumers to pay attention.

In technology, no single solution exists that can be used to secure IoT devices. However, many solutions are available that consumers can embrace to increase the safety and security of their personal information.

In the business community, there is a need for a collaborative approach to increase device security. Consumers can employ the following steps to secure their devices; to begin, they should ensure that they have strong passwords for their device protection. Ensuring that their devices are turned on for automatic updates can also ensure that their devices can notify them whenever there is a malicious attack as opined by Meier et al.[26]. Moreover, the consumer router which is the major gateway to external insecure internet should have an effective Wi-Fi setting, passwords for non-default checked regularly, and regular encryption setting. Additionally, the technology experts are on with research to see the possibility of employing Software-defined Networking (SDN) to provide security for IoT smart home devices as well as

using blockchain architecture in enhancing smart home device security and privacy through low scale instantiation blockchain [39].

The significance of smart homes will continue to increase. Although the research on smart homes began a long time ago, there are still challenges in mature home intelligence solutions. They will be required to understand human behavior and efficient algorithms to address uncertainty challenges within a home. As outlined in the literature review, smart homes offer a lot of benefits to the homeowners. However, there is a need for extra security measures to be embraced to ensure that there is safety and privacy of information relating to occupants. The incorporation of AI and IoT is another field that has gained attraction from many homeowners. However, there is a need for more measures to be implemented to ensure safety and efficiency to the end-user.

CHAPTER 3

RESEARCH METHODOLOGY

The main objective was to create a reference architecture for smart homes that will manage, monitor, and process data from the appliances in the home. After reviewing the literature on the subject, we found some knowledge gaps and developed the conceptual idea of our research. We also came up with several research questions based on our preliminary studies.

- Is there any IoT-based smart home reference architecture already developed and being implemented?
- What are the drawbacks of current smart home architectures?
- Does using IoT-based reference architecture, to create devices and appliances for smart homes, helps to overcome interoperability issues?
- Is it possible for the services, devices, appliances, applications, and systems in a smart home work together reliably?
- How can we design a reference architecture and implement a proof-of-concept for an IoT-based Smart home?

3.1 Research Design and Strategy

Constructive research methodology was used for this research work due to its practical and real-life implications. This method is a systematic approach that allows for deliberate development of methods, modules, tools, and techniques that are applicable well beyond the case study that inspired their development [40]. This research methodology which was developed by Kasanen et al. [41], is used in computer science, software engineering, operations research, clinical medicine, and mathematics. It also employs qualitative, quantitative, and empirical techniques. The Figure 3.1 describes the constructive research methodology

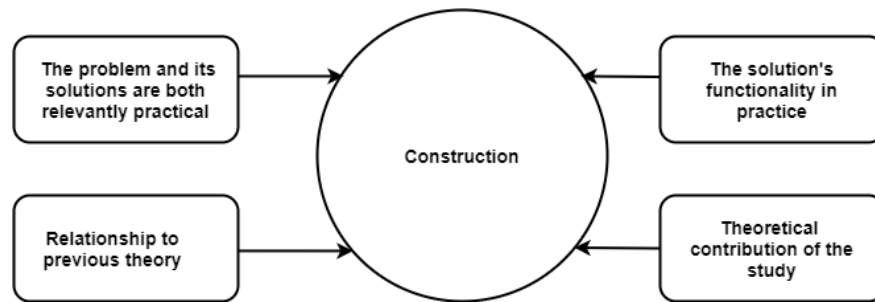


Figure 3.1 Constructive Research Methodology [41]

3.2 Reason for Selection of Methodology

We selected this methodology because of the bottom-up and top-down approach we used in designing and developing our research. This methodology allowed for maximum flexibility and innovation unlike other methodologies that might restrict the research processes and outcomes. It allows creation of new knowledge that has a relationship with previous knowledge and the outcomes have both theoretical and practical contributions.

3.3 Constructive Methodology Steps

The steps in idealized constructive research methodology are;

- Find a problem that is both practically relevant and has research potential.
- Obtain a broad and complete understanding of the subject.
- Construct a solution (Innovate).
- Verify that the solution works.
- Demonstrate the theoretical linkages and the research contribution of the solution concept.
- Examine the solution's applicability.

1. **Find an issue that is both practically relevant and has research potential:** In the introduction chapter, we gave an overview of the issue

and the objectives we aim to derive. We also stated our research question on the topic.

- 2. Obtain a broad and complete understanding of the subject:** We analyzed the current literature and works done in relation to this topic. In the methodology and discussion chapters, we broadened our analyses and gained further insights into the problem and perceived solutions. We also examined and compared several IoT reference architecture and smart home systems.
- 3. Construct a solution (Innovate):** We provided solutions to the research question by designing and implementing our reference architecture for our “IoT-based smart home”. We also used a consolidated approach to design, construct and evaluate our solution as proposed by Nakagawa et. al [42].
- 4. Verify that the solution works:** In this step we validated our construction to ensure it is functional and meets established criteria by designing and implementing the reference architecture.
- 5. Demonstrate the theoretical linkages and the research contribution of the solution concept:** We discussed the novelties and contribution of our research to the field and industry.
- 6. Examine the solution's applicability:** We described if our solution could work within and outside the scope of IoT-based shomes.

3.4 Consolidated Process for Reference Architecture Design, Representation, And Evaluation.

To come up with a replicable and reusable reference architecture, we selected the ProSA-RA process established by Nakagawa et al [42]. ProSA-RA is a method for systematically designing, representing, and evaluating reference architectures. It was selected because it is comprehensive, it was derived from established methodologies of designing software architecture, and it has also been validated. It was also selected because of its compatibility with Constructive Methodology.

The ProSA-RA process as described by the researchers is divided into four steps;

Step 1 (Select sources of information and analyze them): We selected publications from academia and industry that included proposed and existing IoT reference architectures, smart home architectures and reference models. We also got information from observing real smart homes and taking cues from off-the-shelf smart home software.

Step 2 (Perform Architectural Analysis): In this step we identified the requirements of IoT reference architectures and some capabilities of smart home systems. We also evaluated the suitability, feasibility and effectiveness of the selected architectures chosen for analysis.

Step 3 (Perform Architectural Synthesis): Developing a suitable architecture was the next step we took in following this methodology. Our solution strategy was to meet all the required criteria of IoT reference architecture and described how proposition fixes the gaps discovered in step 2. This step also included explaining the components of our architecture and how they fit in the smart home.

Step 4 (Architectural Evaluation): To evaluate the proposed architecture, we first implemented a proof of concept based on the proposed architectural synthesis in step 3. We came up with a functional and non-functional system requirement for the smart home. Then the next step was to extract the specific application architecture from the generic reference architectures. Thereafter we built the system, deployed and then we tested it to demonstrate that it works.

Steps 1 and 2 are accomplished in chapters 1 and 2. Steps 3 and 4 are also completed in the chapters 4,5,6 and 7. Figure 3.2 shows the step of the ProSA-RA process.

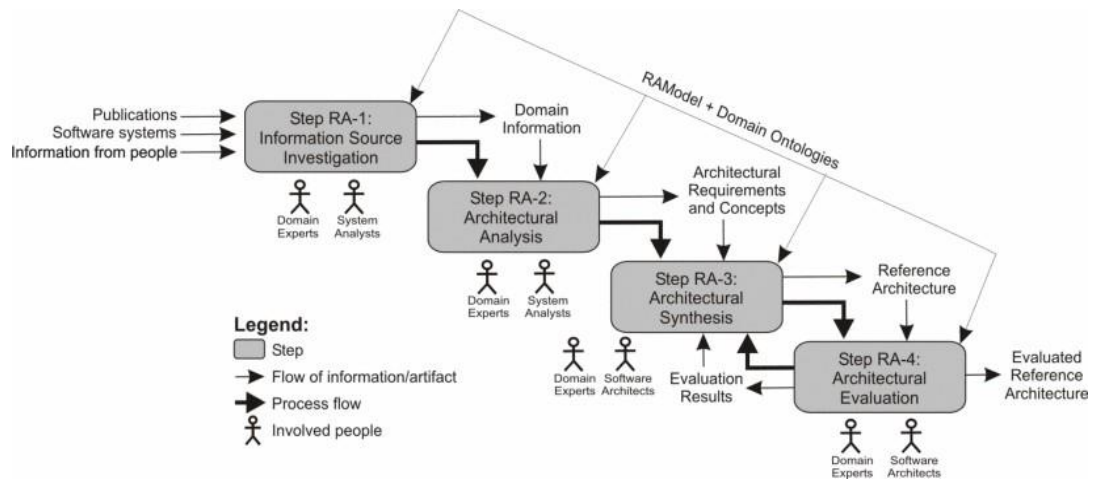


Figure 3.2 The ProSA-RA Process [42]

CHAPTER 4

ANALYSIS OF REFERENCE ARCHITECTURE AND SMART HOMES

After completing first step in the introduction and literature review chapters, in this fourth chapter we carried out the second step of the ProSA-RA process, where we identified and selected our reference architecture requirements. This chapter is also part of the second step of the constructive research method which recommends obtaining a broad and complete understanding of the subject. Therefore, we categorized smart homes, defined the criteria of our reference architecture, analyzed selected reference architecture and specific smart home architectures as well as critiqued them objectively.

We proposed that IoT-based smart home systems can be categorized across two viewpoints: Connectivity Type and Service Type.

4.1 Connectivity Type: This describes how the network of the IoT-based smart home is configured. It can also be divided into two: LAN (Local Area Network), WAN (Wide Area Network).

4.1.1 LAN: In this connection type, all devices, networks, services are connected and restricted within a building or home. It is also known as Intranet. Users of this type of configuration cannot interact with their smart home components outside the home. A typical system will consist of sensors, actuators, a network, a centralized hub for visualizing, coordinating, and processing data, and one or more control units. The devices can be connected to the hub via wired and wireless connection protocols. This Figure 4.1 shows a typical representation of a LAN smart home system.

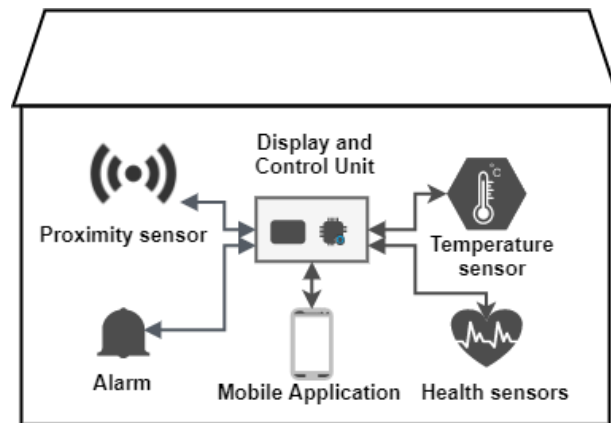


Figure 4.1 LAN smart home connectivity

In LAN based connection, the central hub (main display and control unit) usually has core operating systems to process data and coordinate communication. Some widely available IoT Operating Systems are Windows 10 IoT, Android Things, Tiny OS, Ubuntu Core, Snappy, Raspbian. There are also some other smart homes operating systems, like “Home-assistant” and “OpenHAB”.

4.1.2 WAN: Wide area connection allows the network to be broadcast outside a physical location. This also allows smart homes to be connected to the internet. Therefore, users can interact with their smart home systems from outside the home via the web. They can also integrate to third-party services available on the web. Commercial IoT-based smart home providers widely used this configuration. A typical system will consist of sensors, actuators, a network, an IoT gateway, online IoT server or platform, end user devices like phones and laptops. The Figure 4.2 shows a sample WAN smart home connection.

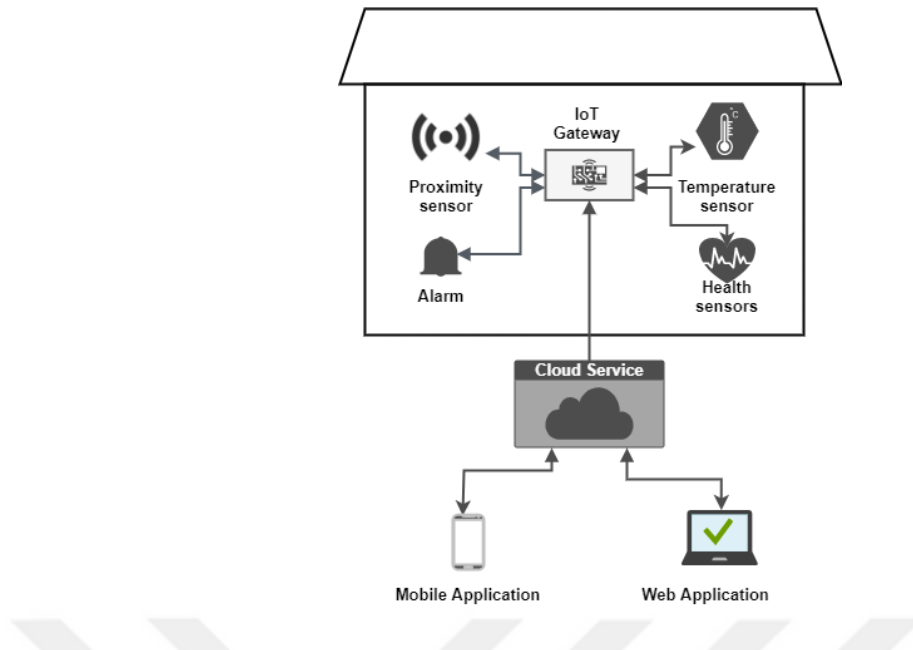


Figure 4.2 WAN connectivity

4.2 Service Type: IoT-based smart home system use-cases might be generic or specialized. Examples of numerous applications include health care, surveillance, power management, waste management, etc.

We have also been able to classify the services into four broad categories based on analyzing several research and commercial solutions. These four categories are Utility, Entertainment, Comfort and Security.

4.2.1 Utility: This service is related to crucial utility services offered to a home e.g., water, electricity, gas, waste etc.

4.2.2 Entertainment: This service is related to leisure, enjoyment, and relaxation within the home. e.g., food, drinks, TV, music, and games.

4.2.3 Comfort: This is related to the well-being and health of the occupants in a home, e.g., temperature control, light switch control, vital health monitoring etc.

4.2.4 Security: This has to do with safety from internal and external threats within a home, e.g., surveillance camera, intrusion detector, emergency alarm, biometric doors etc.

4.3 Essential Characteristics of IoT Reference Architecture

IoT ecosystems are inherently heterogeneous in terms of hardware and software, with devices with varying functionality and network protocols. There have been efforts to abstract such devices' unique characteristics from applications, promote interoperability among them, and contribute to and leverage the growth of the IoT ecosystem.

IoT reference architecture should have the following characteristics: Interoperability; Device discovery and management; Context-awareness; Scalability; Management of large volumes of data; Security, privacy, and integrity; Dynamic adaptation according to Cavalcante et al. [43].

- **Interoperability:** Supporting the variability and dynamics of IoT systems effectively.
- **Device discovery and management:** offer processes for device management and discovery
- **Context-awareness:** the ability of a system or component to detect and receive information about its surroundings at any moment and adjust its behavior as a result.
- **Scalability:** This is the ability of a system to efficiently respond to an increase in demand.
- **Management of large volumes of data:** IoT devices generate a lot of data, therefore an architecture must consider this requirement.
- **Security, privacy, and integrity:** Security in every layer is important to keep the system, data, and devices safe and away from threats.
- **Dynamic adaptation:** to guarantee application access and reliability during operation.

Furthermore, WSO2s' IoT white paper also summarized the requirements for IoT reference architecture into key categories: Connectivity and communications, Device management, Data collection, analysis, and actuation, Scalability, Security, High Availability, Predictive Analysis, Integration [44].

4.3.1 FIWARE IoT Reference Architecture

FIWARE is a market ready open-source platform used to create Smart IoT solutions. FIWARE is an ecosystem of in-house modular software components and other robust open-source software programs. FIWARE is domain agnostics, as it can be used for Smart Cities, Smart Agriculture, Smart Manufacturing etc. An illustration of FIWARE reference architecture is shown in Figure 4.3.

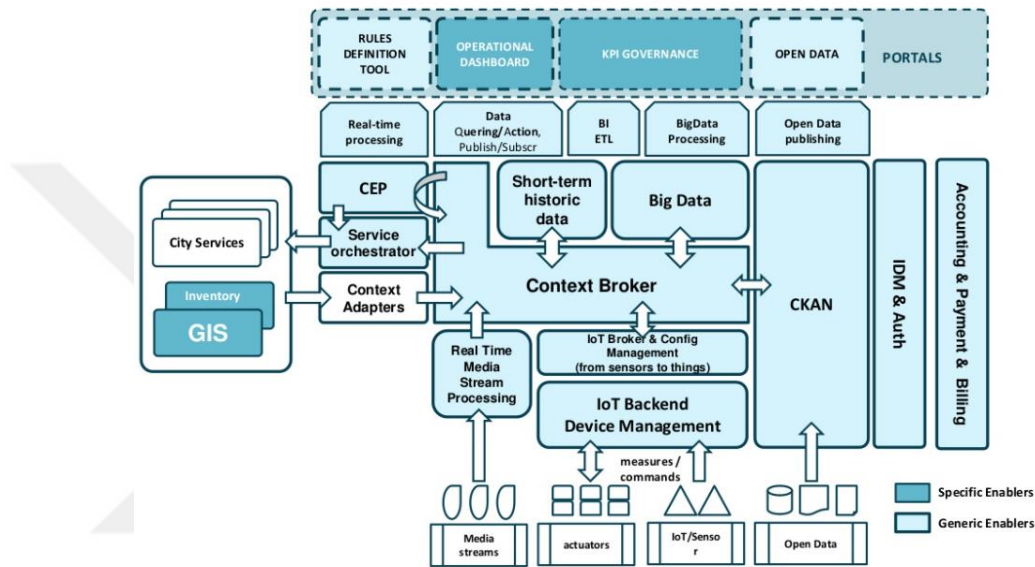


Figure 4.3 FIWARE reference architecture [44]

The context broker is the heart of the FIWARE platform, as it provides the single source of truth for other components. Applications and services can publish and subscribe to data generated from IoT devices and other services via FIWARE-NGSI (Next Generation Service Interface). For instance, IoT sensors and actuators send or receive data via the IoT Agent.

The IoT Agent sends the data to the Context Broker meanwhile another software like CKAN can subscribe to the data and monetize it. The data can also be sent to FIWARE's online dashboard "Wirecloud". Features of FIWARE Reference architecture are;

- **Interoperability:** FIWARE is interoperable and open by design. It has several components (Generic Enablers) which can be extended to accommodate new functionalities e.g., IDAS makes it easy to add new third-party connections and protocols via an easy-to-use interface. Cygnus is also “Generic Enabler” for persisting short-term historic data. FIWARE core components also use NGSI-LD or NGSI-V2 as the information model standard, and API for easy intercommunication. The core software components of FIWARE can also be packaged into a Docker container, which makes it easy to run on most computer operating systems.
- **Connectivity and communications:** It allow several communication protocols like JSON, Ultralight via HTTP/MQTT, Sigfox or LoRaWAN. This ability to translate protocols can be achieved by introducing a FIWARE IoT middleware agent like IDAS.
- **Context-awareness:** FIWARE has a solid context information management component called “Orion Context-Broker”. This engine allows real time ingesting of data from sources, including devices with various protocols, existing sources, third-party API etc.
- **Data Processing and Management:** FIWARE has components that enable data processing at scale. Cosmos is a set of generic enablers that make it easy to process stream and batch context data using Big Data processing tools like Apache Flink and Apache Spark. Cygnus is another Generic Enabler used for persisting context data into databases for analysis. Also, for real-time video processing, it adopts Kurento and Openvidu. It also makes use of FogFlow as a framework for IoT edge processing.
- **Scalability:** The FIWARE architecture is highly scalable. It is also Cloud Native and can be deployed based on different sizes and scenarios. The kubernetes template (Chart) is officially packaged on HELM. In real life scenarios, it has been used to create solutions based on Smart City, Smart Health and Smart Farms etc.
- **Security:** Keyrock is FIWARE software component that secures access to data. It can use the OAuth protocol for identity management. FIWARE also has additional components like WILMA to enforce access control on

back-end applications and AuthzForce also provides an API interface for retrieving authorization choices based on authorization policies and from PEP authorization requests.

4.3.2 ITU IoT Reference Architecture

ITU is the world's leading telecommunication standards organization. The *ITU Y.2060* reference architecture provides high-level requirements for building smart IoT solutions (*ITU Y.2060: Overview of the Internet of Things*, n.d.) [46]. They proposed four horizontal logical layers and two vertical capability approaches for their reference architecture as shown in Figure 4.4.

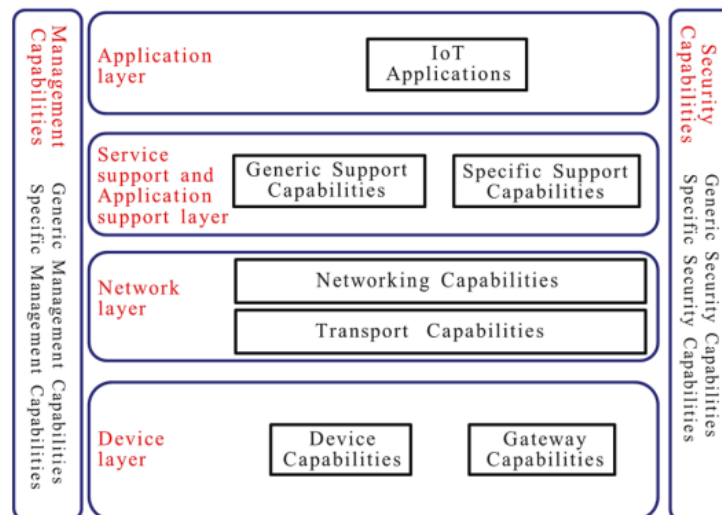


Figure 4.4 ITU reference architecture [46]

Horizontal Logical Layers: The layers are Application layer, Service support and application support layer, Network layer, Device layer.

Application layer: These are the IoT application end users interact with to visualize data and give commands.

Service support and application support layer: In this layer, general support services like data processing and data storage are done. specific support capabilities, Artificial Intelligence and Machine Learning can be applied to a domain.

Network layer: Networking capabilities is the general management of interconnection of devices and services. Transport capability is the method and format of which data is being sent.

Device layer: Device capabilities must deal with the functionalities of sensors and actuators in the IoT environment. Gateway capabilities also provide connection and interoperability between the device and the service support and application support layer.

Vertical Layer: These layers are Management capabilities, Security capabilities.

Management capabilities: This vertical cuts across all horizontal layers. Management capabilities can be general (e.g., device management, access management, configuration) or specific capabilities depending on the domain.

Security capabilities: This capability proposes a comprehensive security approach (e.g. Authorization, Authentication, Anti-Virus) of IoT devices and data. Security measures must be implemented throughout the life cycle and layers of the IoT system. Also, specific security methods and techniques should be applied to layers, domains, and services in an IoT system.

4.3.3 WSO2 Reference Architecture

WSO2 is an enterprise platform for locally and globally integrating application programming interfaces (APIs), applications, and web services. They prepared a white paper for the reference architecture, containing the requirements and proposed architecture based on their platform [44]. Their reference architecture consists of 5 horizontal layers (Client Services, Data Service, Aggregation Layer, Transport Layer, Device Layer) and two layers that cut across other layers (Identity and Access Manager, Device Manager). Figure 4.5 shows the WSO2 reference architecture.

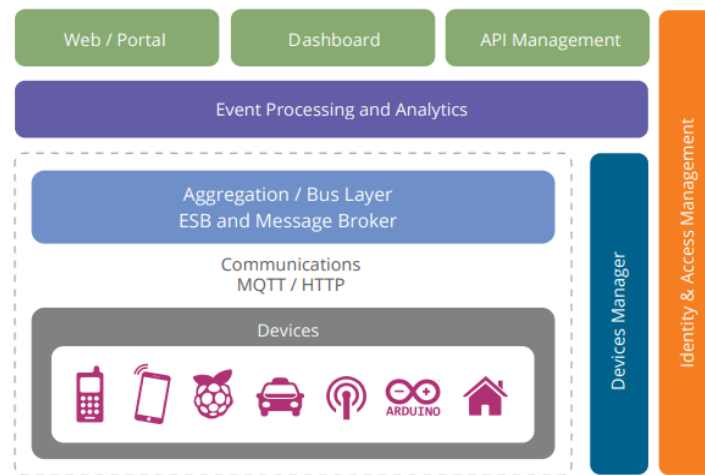


Figure 4.5 WSO2 reference architecture [44]

The horizontal layers are:

- **Client/external services-:** In this layer, end users can access applications via Web, Mobile, Dashboard and APIs.
- **Data, Analytics and Event Processing:** This is the layer where data and events from the device or client layer are processed and analyzed.
- **Aggregation layer:** Data is passed into the message broker to allow interoperability. This layer may also contain an enterprise service bus to allow intercommunication between software and services.
- **Transport layer:** This is the communication layer that transports the data in different protocols, such as HTTP, MQTT, XMPP.
- **Devices:** The device layer represents the sensors and actuators in the IoT system.

The vertical layers are;

- **Device management:** The device management layer only cuts across the device and transport layer. It is responsible for configuring devices, tracking their status, maintaining, and administering them.
- **Identity and access management:** This cuts across all other layers in the reference architecture. This vertical is to ensure security on the platform.

4.3.4 Analysis of Current Smart Home Architectures

Several researchers have introduced their architecture and references architecture for smart homes. They designed their architecture based on functionality and technologies they perceived to be important. One of the main issues with some architecture is that they are not interoperable, some are too generic while others are also too specific to accommodate other service types, devices, and other requirements.

Li et al. [47] suggested an architecture that consisted of smart home gate, smart socket and switch, community LAN, security equipment, telephone interface, utility management and billing. There were also suggestions of connecting the smart home to community and municipal services. Their domain type of smart home also covered a wide range of functionalities such as comfort, security, and utility. However, this architecture is lacking some important features of a smart home such as security, end user application, data processing, data management and context management. It also does not specify adherence to any standards for interoperability and connectivity. Figure 4.6 shows a sketch of their architecture.

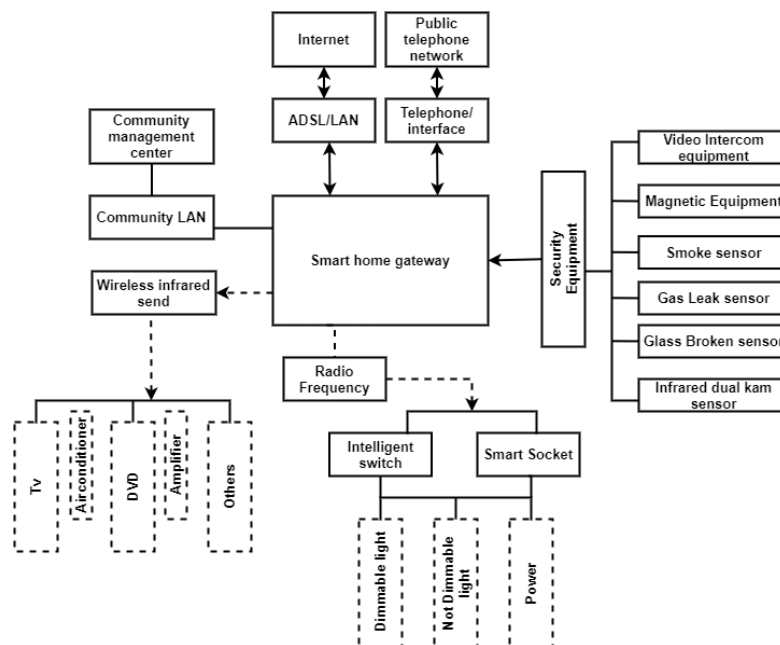


Figure 4.6 Li et al. Smart Home Architecture [47]

Mocrii et al. [48] proposes a broad cloud-based smart home architecture. The devices, appliances, sensors, and actuators are connected via LAN. These devices communicate with a gateway located at the network's edge. This permits connectivity between internal networks and the external Internet. Their architecture is generic and can be used for different service types. Consequently, still due the generic nature of their architecture they abstracted many other important layers of a smart home system. There was no emphasis on identity management, device management, security, connectivity, context management and the cloud layer. For a well-defined smart home this missing information are important for interoperability and extensibility. Figure 4.7 shows the diagram of the suggested architecture.

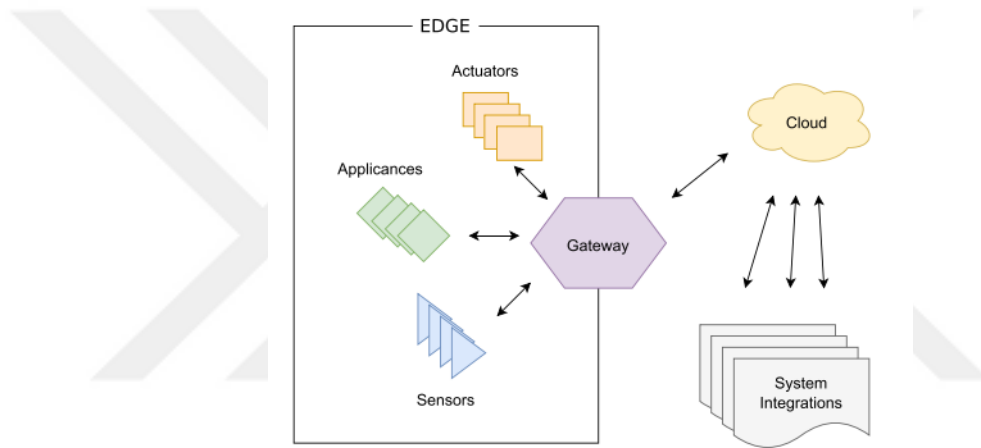


Figure 4.7 Mocri et al. Smart Home Architecture [48]

Pürgstein et al. [49] designed an architecture to mitigate the security risk in a smart home network. Their architecture was more focused on smart home LAN security. In this configuration, devices can communicate to other networks via specific gateways. They also proposed the following requirement for a secure smart home system;

- Devices should be classified depending on their domain and communication capabilities.
- Only intended communication partners are permitted to communicate with devices.

- Communication across classes is only permitted if well-defined security policies are followed.

It is, however, important to note the limitations of this smart home architecture, as it is optimized for addressing network security. Their architecture does not give enough information about the software part of a smart home, such as data management, data processing, and IoT end user applications. Although device interoperability is being addressed, they still did not completely address data interoperability, which is essential for smart homes. Figure 4.8 shows their smart home architecture.

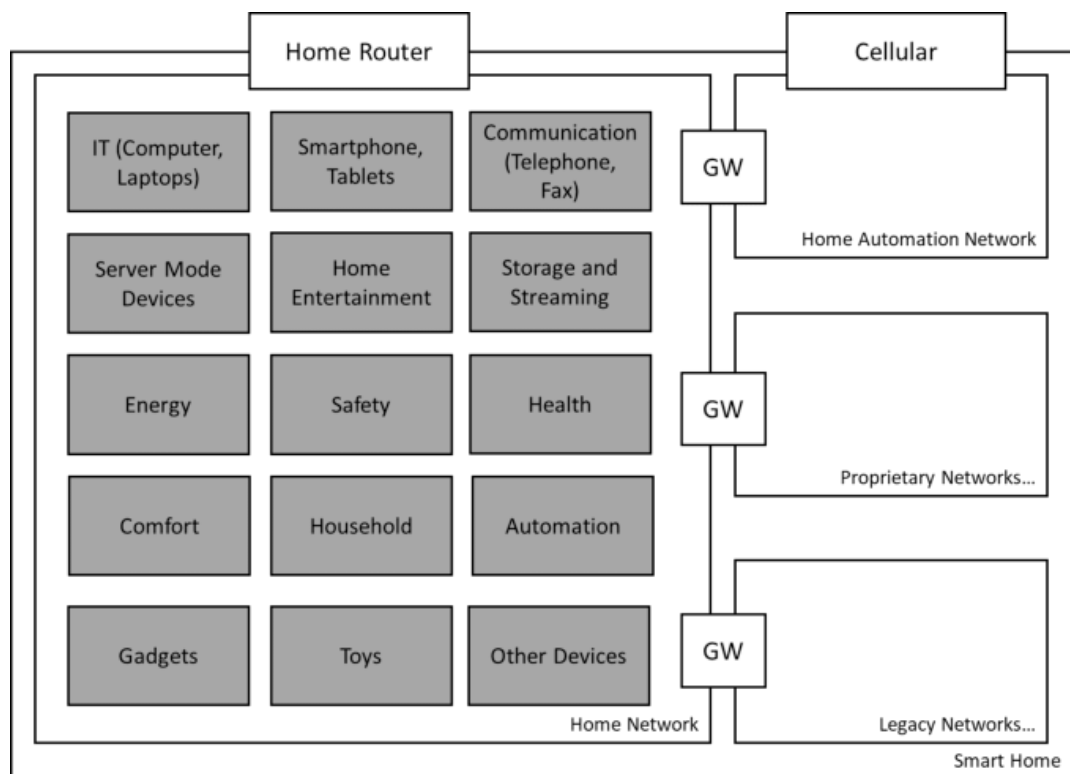


Figure 4.8 Pürgstein et al. Smart Home Architecture [49]

Bing et al. [50] proposed a 3 layered architecture (application layer, network layer, sensing layer) with several components embedded in each layer. The application layer consists of the end user software, middleware, data processing and service supporting platform.

The network layer consists of Internet and TD-SCDMA (Time Division-Synchronous Code Division Multiple Access) for communication between the sensing layer and the application layer. The sensing layer is a self-organized network where data collection and device actuation happen.

The shortcoming of this smart home architecture is that it does not address the security challenges faced by the three layers and components within, it does not describe any framework for context management, also the proposed network layer is limited to only the internet and TD-SCDMA, whereas there are other devices that might employ other communication methods. A sketch of their smart home architecture is shown in Figure 4.9.

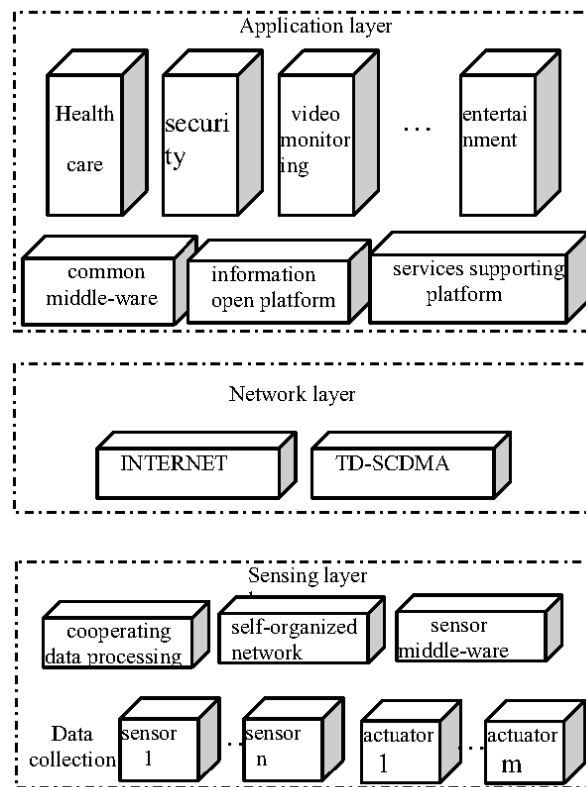


Figure 4.9 Bing et al. Smart Home Architecture [50]

4.3.5 Comparison of IoT Reference Architectures

Table 4.1 A Comparison Between Reference Architectures

	FIWARE	WSO2	ITU
Interoperability	Yes	Yes	Yes
Context-awareness	Yes, with Orion Context Broker	Yes, with Enterprise Service Bus	Yes, with generic and specific capabilities
Device discovery and management	Yes, it has an Identity and Access Manager	Yes, it has an Identity and Access Manager	Yes, with generic and specific security capabilities
Scalability	Yes	Yes	Yes
Security, privacy, and integrity	Yes	Yes	Yes
Dynamic adaptation	Yes	Yes	Yes

4.3.6 Comparison of Smart Home Architecture

Table 4.1 A Comparison Between Smart Home Architectures

	Mocrii et al.	Li et al.	Pürgstein et al.	Bing et al.
Interoperability	No	No	Partial Yes (interoperable with network but not data)	Yes
Context-awareness	No	No	No	No
Device discovery and management	Yes	Yes	Yes	Yes

Scalability	Yes	No	Yes	Yes
Security, privacy, and integrity	No	Yes	Yes	No
Dynamic adaptation	Yes	No	Yes	Yes
Connectivity Type	LAN/WAN	LAN	LAN/WAN	LAN/WAN



CHAPTER 5

CONSTRUCTION OF IOT BASED SMART HOME REFERENCE ARCHITECTURE

This part employs the third step of the constructive research methodology i.e constructing a solution. It is also the third step of the ProSA-RA. This step entails the design of our IoT-based reference architecture for smart homes and how the proposed reference architecture meets the criteria suggested in the previous chapter.

The proposed IoT-based smart home reference architecture intends to provide a layered and comprehensive description of smart home IoT systems. Our flexible design allows for various devices, configuration and use cases. Our reference architecture is a result of analyzing, comparing existing IoT reference architectures, standards, and smart home systems, and proposing appropriate solutions.

5.1 Characteristics of the Proposed IoT-based Smart Home Reference Architecture

Our smart home architecture hopes to solve some of the limitations faced by the other proposed solutions, as discussed in the previous chapters. It is designed to accommodate different connectivity types and service types. A LAN, WAN or hybrid-based connectivity type can be derived from it, so it can be used within the home or interacted with from a remote location.

Furthermore, our reference attempts address all the IoT reference architecture criteria proposed by Cavalcante et al. [43]. The table 5.1 explains how our solution meets these criteria.

Table 5.1 Solution to Reference Architecture Criteria

Interoperability	The device manager, IoT gateway, IoT Agent and cloud integration component will address the variability of devices
Context-awareness	Another software service to manage context was also introduced, along with a suggestion of adhering to the smart model standards.
Device discovery and management	This will be achieved by the provision we made in the network layer, embedded devices, device management component and IoT gateway.
Scalability	Our reference architecture can also manage large deployments through horizontal and vertical scaling.
Security, privacy, and integrity	We have also proposed an approach for comprehensive security and privacy.
Dynamic adaptation	Our layered and component-based approach allows the system to adapt to modifications.
Connectivity Type	We have the home and cloud environment in consideration. Therefore, smart home network can be connected LAN, WAN or Hybrid

5.2 Proposed IoT-based Smart Home Reference Architecture Diagram

In our Reference Architecture, we have two environments: the “HOME” and the “CLOUD”, which consist of layers. Each layer serves a specific or multiple function in the system. A layer may also consist of one or more components within them. These components can also consist of devices, application, and communication networks. Figure 5.1 shows the proposed IoT-based reference architecture for smart homes

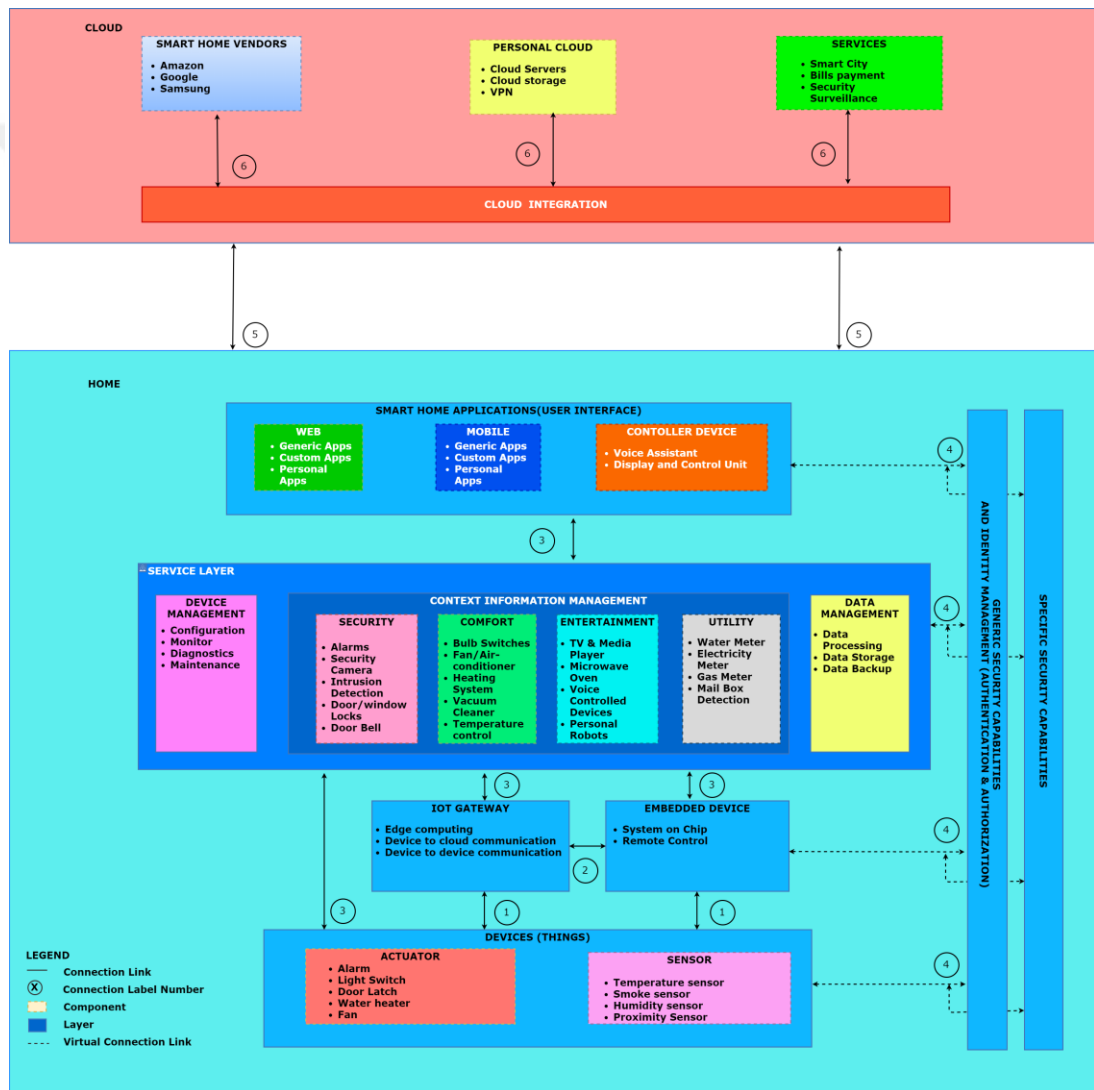


Figure 5.1 Proposed IoT-based Reference Architecture for Smart Homes

5.3 Home Environment

This comprises the device layer, support and service layer, smart homes applications layer, and security layer. It houses all the components of a LAN-based IoT smart home.

5.3.1 Device Layer

The device layer is where the perception and actuation occur. In this layer, the sensors observe and collect data from their surroundings and send it to the central system, IoT gateway, applications, or other devices. The actuators are also in this layer, they are devices that act upon data or commands received from the central system, IoT gateway, applications, and other devices.

Devices can support one or more network configurations in their physical link, transport layer and application layer. Our smart home architecture suggests handling this internetworking by using an IoT gateway. We also recommend enabling automatic device discovery, secure device enrollment, and access control through the gateway and service layer. Devices should be energy efficient to further reduce the cost of deployment and maintenance of the system. Data in transit should also be encrypted to prevent man in middle attacks and session hijacking.

5.3.2 IoT Gateway

This is a software application or hardware device that acts as a link between the service layer, cloud (web-based applications) and actuators, sensors, and smart devices. IoT gateways can also act as edge devices, where data is pre-processed before sending to the cloud or processed and sent back to an actuator. It also enables protocol translation between devices, in addition to the cloud, for improved communication and security.

5.3.3 Embedded Devices

In smart homes, embedded devices are small special purpose microprocessor-based devices that can be used to directly interact with one or many actuators and sensors without the need for the gateways or service layer. Some embedded devices can also have the capability to connect with the IoT gateway and the service layer.

5.3.4 Service Layer

This layer performs the core function of device management, data management, and context information management. These services are usually hosted and deployed within the home. This layer also opens smart home systems to web based third-party services via REST-API or other protocols. In our IoT-based reference architecture for smart homes, we propose that activities within the smart home can be classified into security, comfort, utility, and entertainment context. Consequently, devices and activities can be managed under this classification.

Context Information Management: Context awareness is an IoT concept where computers can sense and react to continuous changes in the environment. An information model represents the situation and attribute of devices and entities. Context information management helps provide organization, storage, retrieval and modification of an entity and device data in real-time and non-real-time. Therefore, smart homes should have a context information management component that will serve as an interface for other components to easily access data. A sample reference implementation is the FIWARE-ORION context broker for managing real time context data and FIWARE-CYGNUS for persisting and managing historical context data.

Device Management: Device management is a key issue for these IoT enabled devices being used in the home. This component carries out operations involving discovering, enrolling, configuring, authenticating, authorizing, monitoring, analyzing, securing, and troubleshooting devices in the smart home system. Due to the many types of devices that are always on, there is a need for better security

features so that your private data does not get hacked. To ensure the safety of your data, the device's firmware needs to be updated. This will prevent any major vulnerabilities from being exploited in the future. A strong device authentication must be adopted to further reduce risks. The device network must also have an end-to-end encryption mechanism, and network access control list.

Data Management and processing: Data management in a smart home database is critical to the smart home. The system would not function without it. The database holds all the data collected from the house, such as sensors, devices and equipment, house environment data, users, occupants and guests, house schedule, alarm system, house environment data, user's activities, communication history, user and house profile, and web services. Some of the data types stored include, but are not limited to; images, audio files, video files, and text files. In addition, location data from IoT devices, such as cameras and motion detectors, are also saved into the database for analysis purposes.

However, data privacy is a pressing issue in the areas of smart home and IoT. These devices collect and store large amounts of data that can be used for some purposes, like profiling or marketing purposes, this can be intrusive and damaging to privacy. Hence smart home developers and providers must mitigate such prevailing issues, such as working towards meeting the General Data Protection Regulation (GDPR) standards.

Smart Home Applications: End users use smart home applications to view and interact with their IoT-based smart home systems. Such applications can be built for mobile, web or controller devices. The controller devices can have buttons and touchscreen displays for user interaction. They are used to configure, control, and manage the whole smart home system. Generic commercial and open-source applications are usually connected to smart homes systems due to ease of use, quality, security, and affordability. Custom applications are sometimes built for individual smart homes to accommodate more personalization and privacy.

5.3.5 Security

Security is of utmost importance to smart home users, so it cuts across all layers of our IoT-based reference architecture for smart home automation systems. Strategies and policies are also embedded in each component's hardware and software programs to ensure full protection.

Generic Security: These are common security strategies and practices applied to different layers and components of a smart home system. They include Authentication, Authorization, Identity Management, Key Management, Trust Management, as proposed by Pal et al. [51].

Identity Management: This component involves provisioning, authentication, authorization, and managing users, services, and resources in the smart home system. The system must support different authorization models, such as self-service, role-based, and identity-driven models. This helps to improve the security of the overall system

Specific Security: Some extra security measures could also be deployed to deal with specified threats in the smart home system. For example, smart home developers can deploy advanced network intrusion and monitoring software, antivirus in support and service layer, two-factor authentication in smart home end user applications etc.

5.3.6 Communication

Our IoT-based reference architecture diagram uses physical and virtual connections labeled by the numbers. Table 5.2, 5.3, 5.4 show some communication protocols used by the connection labels.

1. The interconnection between devices (things), IoT gateway, embedded devices can be done using wired or wireless connections.

Table 5.2 Communication capabilities of connection label 1

Physical Link	Ethernet, Bluetooth, Zigbee, Z-wave, RFID, IEEE 802.11.ah, IEEE 802.15.4e, LoRaWAN, NFC, WiMax, NB-IOT, LTE-MTC, Cellular, SigFox.
Transport Layer	TCP, UDP
Application Layer	MQTT, SMQTT, CoAP, Modbus, XMPP, AMQP, M2M, LWM2M, XMPP-IOT, Ultralight 2.0

2. The IoT gateway and embedded devices can be interconnected, especially in a WAN-based smart home, so that the home can interact with a Web server, client, or middleware.

Table 5.3 Communication capabilities of connection label 2

Physical Link	Ethernet, Bluetooth, Zigbee, Z-wave, RFID, IEEE 802.11.ah, IEEE 802.15.4e, LoRaWAN, NFC, WiMax, NB-IOT, LTE-MTC, Cellular, SigFox.
Transport Layer	TCP, UDP
Application Layer	MQTT, SMQTT, CoAP, Modbus, XMPP, AMQP, M2M, LWM2M, XMPP-IOT, Ultralight 2.0

3. In some system configurations, devices can communicate directly with the service and support layer, but IoT gateways are also the main component used to accomplish this task. Service layer can also communicate with the end user smart home applications.

Table 5.4 Communication capabilities of connection label 3

Physical Link	Ethernet, Bluetooth, Zigbee, Z-wave, RFID, IEEE 802.11.ah, IEEE 802.15.4e, LoRaWAN, NFC, WiMax, NB-IOT, LTE-MTC, Cellular, SigFox.
Transport Layer	TCP, UDP

Application Layer	MQTT, SMQTT, CoAP, Modbus, XMPP, AMQP, M2M, RESTful HTTP, LWM2M, XMPP-IOT, SOAP, Websocket, HTTP/2, Ultralight 2.0
-------------------	--

4. Security is of utmost importance in smart homes. Therefore, the security component cuts across all layers, components, and protocols. The connection of the security with the smart home in this diagram is virtual and symbolic.
5. The home environment can exist in isolation in a LAN based smart home system. But in a WAN-based smart home, the home environment can also be securely connected with an integrated cloud environment.

5.4 Cloud Environment

The cloud environment is the part of the smart home systems that are hosted and deployed completely outside the home. IoT-based smart homes might need to be integrated with third-party services to accomplish such tasks, such as data storage and backup, utility billing, remote connection, security surveillance, platform software vendors and artificial intelligence services. The cloud environment can also communicate with several other Third-Party services and vendors. Table 5.5 shows the communication capabilities in connection bel 5 & 6.

Table 5.5 Cloud Environment Communication Capabilities Label 5 & 6

Physical Link	IEEE 802.11.ah, IEEE 802.15.4e, WiMax, LTE-MTC, Cellular.
Transport Layer	TCP, UDP
Application Layer	MQTT, SMQTT, CoAP, XMPP, AMQP, M2M, RESTful HTTP, XMPP-IOT, SOAP, Websocket, HTTP/2, Ultralight 2.0

CHAPTER 6

PROOF OF CONCEPT FOR IOT-BASED SMART HOME APPLICATION BASED ON PROPOSED REFERENCE ARCHITECTURE

This is the final part of the third step of the constructive research methodology i.e constructing a solution. It is also part of fourth step of the ProSA-RA process which has to do with “evaluating the proposed architecture”. We also detailed the implementation of the proposed IoT-based reference architecture proof-of-concept for smart homes in this chapter.

Application architecture is defined as the components and patterns utilized in designing and building an application. It offers the best practices and road map that should be followed when an application is being built. This results in the building of an effective and well-structured application. The application architectures are used as the starting point for an architectural design, a way of assessing components of reuse, the vocabulary of discussing the application types, and as a design checklist [52]. We made use of FIWARE components for building the simple PoC application.

6.1 Functional Requirements

- **Sensors**
 - The rooms in the home should have motion sensors to detect movement.
 - The rooms in the home should have luminosity detectors to determine light intensity.
 - The rooms in the home should have a thermometer sensor to determine the temperature.
- **Actuators**
 - The rooms should have bulbs that can respond to luminosity.

- The rooms in the home should have heating cooling and ventilation system (HVAC) that activates with changes to temperature.
- The rooms should have fans that can be turned on and off.
- The rooms should have doors that can be closed remotely.
- The rooms should have bells that can be rung remotely.

- **User Actions**

- Users should be able login with a username and password.
- Admin can manage users.
- Logged in users can view the devices in rooms.
- Logged in user and authorized users can alter devices to a state.
- Logged in users can view motion detection history.
- Logged in users can view luminosity and bulb actuation in real time.
- Users can log out of the application.
- Users can view and create complex reports and visualization.

6.2 Non-Functional Requirements

- **Secure:** Application should be secure with enforcement of privileges.
- **Customizable:** Application should be modular and allow for addition of more components. It should allow connectivity with various communication protocols and data formats.
- **Scalable:** Application should be designed to accommodate growth in size and complexity.

6.3 Implementation of IoT-based Smart Home Application Architecture Using FIWARE

From our functional and non-functional requirements, we identified the required components and layers needed for the application architecture based on the proposed reference architecture.

The smart home application architecture that we designed and implemented is based majorly on the components of the FIWARE ecosystem. A merit of FIWARE is that it enables low-cost and efficient development of IoT applications. All FIWARE modules and components are developed and released based on open-source software license. From our derived reference architecture, we can finally select the application architecture components. The table 6.1 depicts the mapping of elements between the proposed Reference Architecture and the developed concrete PoC Application Architecture.

Table 6.1 Mapping Derived Reference Architecture to Application Architecture

Derived Reference Architecture	Smart Home Application Architecture
Devices	Virtual Things (sensor and actuators)
IoT Gateway	FIWARE IoT Agent
Context Information management	FIWARE Orion Context Broker & MongoDB
Device Management	Keyrock and custom smart home application
Identity Management	Keyrock
Data Management	QuantumLeap, CrateDB, MySQL & MongoDB
Smart Home Application	custom smart home application

In addition, in FIWARE, applications and data storage are "loosely coupled", the context information also follows the NGSI-LD/NGSI-V2 standards. As a result, it will be easier to manage the system and modify the services. It will also be easier to deploy applications based on the reference data model of standards and other successful implementations. Several smart data models have already been released in areas such as "environment", "transportation", "waste management" and "weather". Figure 6.1 shows the smart home application architecture using FIWARE components.

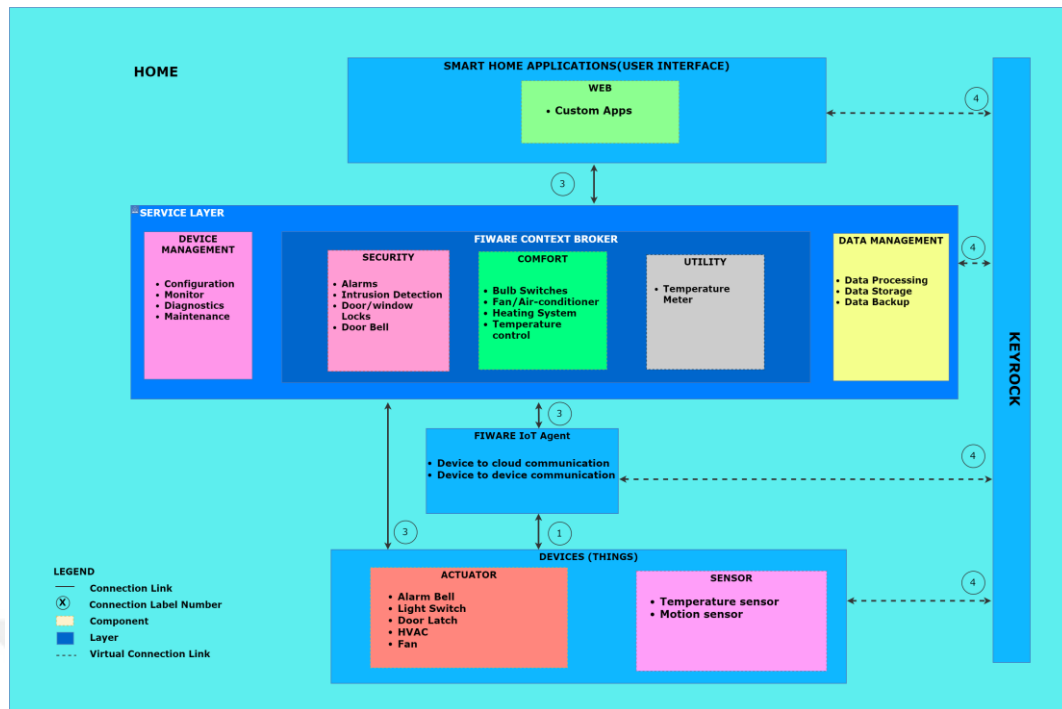


Figure 6.1 Smart Home PoC Application Architecture

6.4 Smart Home PoC Application Architecture Components

1. **Orion Context Broker:** It manages the whole lifetime of context information of entities which includes updates, queries, registrations, and subscriptions. It is a server based on NGSIv2, that manages context information and makes it available. Its core is written in C++ implementation, and it is maintained by FIWARE.
2. **IoT Agent:** The IoT Agent an interface between the IoT devices/sensors and the Orion context broker. It translates various sensor protocols/formats (Ultralight, LWM2M, LoRaWAN, JSON) to a form (NGSIv2, NGSI-LD) understandable by the context broker.
3. **Devices:** These are sensors and actuators within an IoT environment. They are also known as things. In a smart home they can be TVs, refrigerators, camera, bulbs, switches, alarms etc.
4. **MongoDB:** This is the most popular open-source non-relational database. It is cross platform, and it stores data in a document-oriented format. In our IoT-based smart home application it used the database to store and retrieve our context information.

5. **Keyrock:** This is responsible for Identity Management of our components. It enables us to add authorization and authentication mechanisms to our applications. It also has an out of the box OAuth server implementation. Users can be grouped, assigned roles and permission in a fine-grained manner. It also has its own administration dashboard to carry out management functions. Figure 6.2 shows interfaces from the Keyrock application and Figure 6.3 shows the application and device configuration screen.

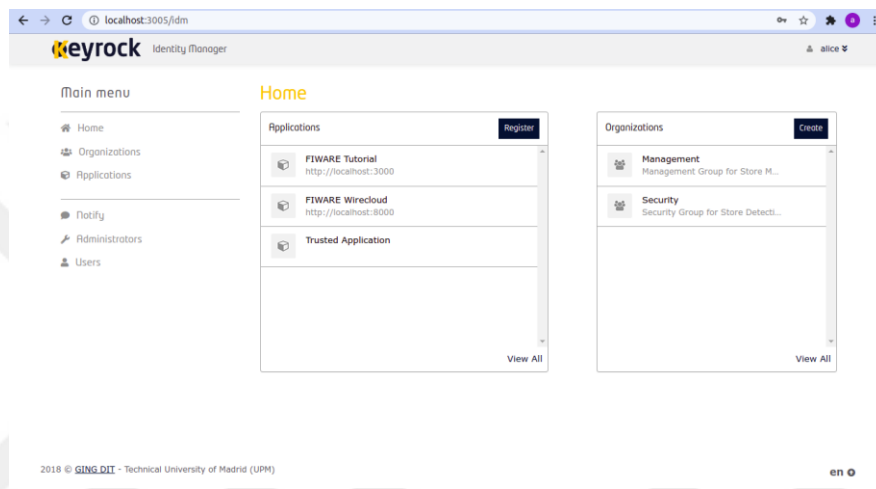


Figure 6.2 Keyrock Identity Management Dashboard Screen

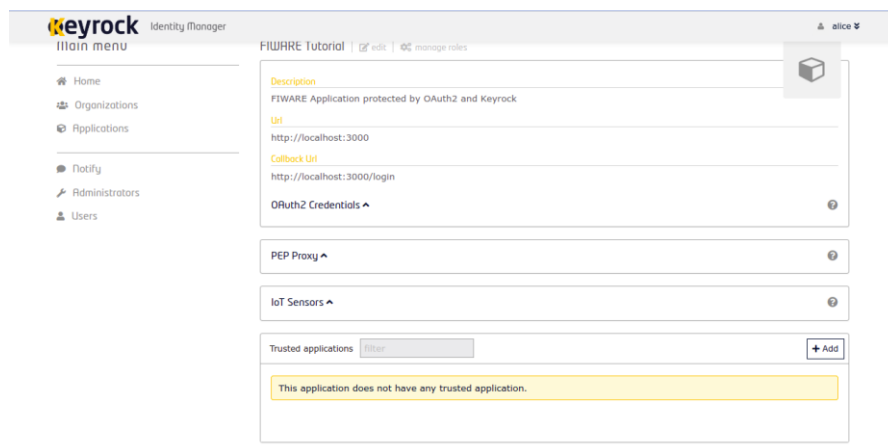


Figure 6.3 Keyrock Application and Device Configuration Screen

6. **Quantum Leap:** It is a REST utility for persisting, querying, and fetching “space - time” NGSI v2 and NGSI-LD data. This service converts NGSI semi-structured data to a time-series database (e.g. Crate DB) record, with each database record corresponding to a discrete time interval and, if present in the NGSI data, a location on Earth.
7. **Crate DB:** This is an open-source distributed SQL database management system that also fully integrates with document-oriented data stores. It is based on “Shared-nothing architecture”, it is fast and highly scalable. It is written as JAVA and includes components of elastic search and Lucene. It can also store time-series data as used in our smart-home architecture.
8. **Smart Home Management Application:** Our simple smart home application was built by modifying and extending of the official FIWARE tutorials. It allows users to login using their email and password or using OAuth2 protocol on Keyrock. It allows users to view and interact with sensors in rooms, Figure (6.4,6.5). It also allows them to interact with certain devices based on their roles and permission as in Figure 6.4. The short-term history of each device can also be streamed and viewed through another interface, Figure 6.5.

SMART HOME IOT DEVICES (ULTRALIGHT OVER HTTP)

A user must be logged in to activate devices, only security staff are able to **unlock** doors and only security and managers can **ring** the alarm bell.

Devices in Room urn:ngsi-ld:Room:001

door001 s|OPEN
bell001 s|OFF
motion001 c|1
lamp001 s|ON||1996
temperature001 tmp|15
fan001 s|ON||1991
hvac001 mode|HOT

Fan On Send

Devices in Room urn:ngsi-ld:Room:003

door003 s|CLOSED
bell003 s|OFF
motion003 c|0
lamp003 s|OFF||0
temperature003 tmp|22
fan003 s|OFF||0
hvac003 mode|OFF

Open Door Send

Devices in Room urn:ngsi-ld:Room:002

door002 s|LOCKED
bell002 s|OFF
motion002 c|0
lamp002 s|OFF||0
temperature002 tmp|17
fan002 s|OFF||0
hvac002 mode|OFF

Open Door Send

Devices in Room urn:ngsi-ld:Room:004

door004 s|LOCKED
bell004 s|OFF
motion004 c|0
lamp004 s|OFF||0
temperature004 tmp|5
fan004 s|ON||904
hvac004 mode|OFF

Lamp On Send

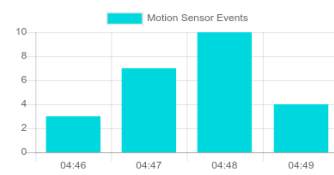
NORTHBOUND TRAFFIC

- 3:01:36 PM HTTP POST http://iot-agent:7896/iot/d7i=lamp001&k=4jggokgpepnvsb2uv4s40d59ov s|ON||1996
- 3:01:36 PM HTTP POST http://iot-agent:7896/iot/d7i=temperature001&k=4jggokgpepnvsb2uv4s40d59ov tmp|15
- 3:01:36 PM HTTP POST http://iot-agent:7896/iot/d7i=temperature002&k=4jggokgpepnvsb2uv4s40d59ov tmp|17

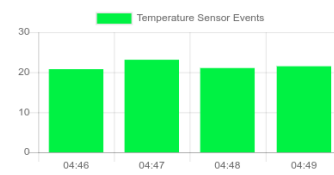
Figure 6.4 Application Device Management Screen When Logged in

Devices in Room urn:ngsi-ld:Room:001

MOTION SENSOR



TEMPERATURE SENSOR



SMART LAMP

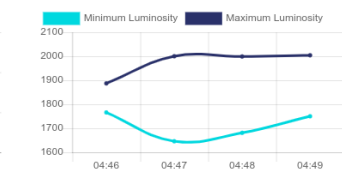


Figure 6.5 Application Device History Charts

CHAPTER 7

DISCUSSION AND CONCLUSION

7.1 Discussion

This study aims to develop a reference architecture for smart homes that will manage, monitor, and process data of the appliances in the home. In chapter 4, we proposed the categorization of smart homes into service types and connectivity types. We also compared various IoT reference architectures and smart home architectures.

The proposed reference architecture was constructed following the recommended steps outlined by the ProSA-RA process discussed in chapter 3. The layers and components of the proposed reference architecture were explained in chapter 5.

Finally, in chapter 6, we implemented a PoC application to create an instance solution of proposed Reference Architecture. The reason for utilizing FIWARE components for this implementation was due to its open and interoperability features.

7.2 Research Questions

RQ1) Is there any IoT-based smart home reference architecture already developed and being implemented?

There are some well-known generic IoT Reference Architectures already developed, such as the ITU, FIWARE and WSO2. Although they are not specifically designed for the Smart Home, they can be used to create a domain-specific Reference Architecture. There are many such attempts to create a Reference Architecture for Smart Energy, Smart City, Smart Industry etc.

On the other hand, there are several Smart Home Reference Architectures proposed by some other researchers, but they have some shortcomings in providing the characteristic features revealed by IoT Reference Architectures holistically, as discussed in Chapter 4. A comparative analysis was also done between the architectures in the same chapter.

RQ2) What are the drawbacks of current smart home architectures?

As detailed in chapter 4, the current drawback is that they are not comprehensive enough to meet the needs of modern smart homes, and many architectures are designed to address only a specific aspect of the smart home. They also failed to display all the characteristics of IoT architectures, such as Interoperability, Context-awareness, Device Discovery and Management, Scalability, Security, Privacy, Integrity and Dynamic adaptation.

RQ3) Does using IoT-based reference architecture, to create devices and appliances for smart homes, helps to overcome interoperability issues?

It is important for developers to consider of all the different types of devices that will connect to an IoT system. The use of IoT-based reference architecture for smart home can help smart home developers overcome interoperability issues by providing them with a common framework and information about components, layers, and protocols in a smart home architecture.

RQ4) Is it possible for the services, devices, appliances, applications, and systems in a smart home to work reliably together?

It is critical to understand how numerous smart devices will function together if you are building a smart home with several smart devices. Essentially, we must know what the different devices can accomplish, as well as their limits, and whether they will function consistently. Our study shows that these devices can work reliably together. We can achieve this by first using an IoT gateway to bridge devices using different communication technologies. Secondly, we can use the devices

management component in the software and support and service layer to enroll and configure devices into an IoT network. Finally, the end user applications can be used to send commands to the devices, and view device data in real time.

RQ5) How can we design a reference architecture and implement a proof-of-concept for an IoT-based Smart home?

To design the proposed reference architecture, we first defined our IoT reference architecture criteria, then we analyzed the existing reference architecture and synthesized how to solve lapses they had. Then, to develop a proof-of-concept solution, we specified the scope and requirements. Thereafter, we derived an application architecture from the proposed reference architecture for the potential scenarios that fits its purpose. Then we defined and identified the key components for the server and client. Finally, we developed and deployed a smart home PoC application in the desired environment and did an end-to-end test. This was detailed in chapter 3 to chapter 6.

7.3 Conclusions

Creating an IoT-based reference architecture for smart homes is essential for the success and future of smart homes. There have been several research and approaches that discuss issues and solutions about IoT, smart homes, reference architecture and interoperability. This study takes a comprehensive account of these issues and proposes solutions to them. In an effort, we constructed an IoT-based reference architecture and implemented proof-of-concept.

Based on this, smart home developers may consider adopting this reference architecture in developing their architectures, applications, and devices to further bridge the gaps in the smart home ecosystem.

Finally, this study does not claim to provide a perfect solution to the stated research questions, and therefore we suggest more research into issues raised in this study.

7.4 Future Works

The following are examples of prospective research projects that could be used to further this subject.

- Designing or developing a reference model for smart homes to further improve interoperability and taxonomy.
- Evaluating the proposed IoT-based reference architecture for smart homes.
- Developing a hardware proof of concept based on this reference architecture



REFERENCES

- [1] Richard Harper, *Inside the smart home*. London; New York: Springer, 2003.
- [2] L. King, “*The evolution of the smart home*,” *Raconteur*, Apr. 14, 2015. <https://www.raconteur.net/the-evolution-of-the-smart-home/> [Jan. 02, 2022].
- [3] Gartner (2018). Gartner says Worldwide PC, tablet and mobile phone combined shipments to reach 2.4 Billion Units in 2013. <http://www.gartner.com/newsroom/id/2408515> [Jan. 02, 2022].
- [4] Statista. (2021). Global smart home market revenue 2016–2022. <https://www.statista.com/statistics/682204/global-smart-home-market-size/> [Jan. 02, 2022].
- [5] A. Bröring et al., "Enabling IoT Ecosystems through Platform Interoperability," in *IEEE Software*, vol.34, no.1, pp.54-61, Jan.-Feb.2017.
- [6] M. M. Islam, M. N. Farook, S. M. G. Mostafa and Y. Arafat, "Design and Implementation of an IoT Based Home Automation," *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, 2019, pp.1-5.
- [7] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in Internet of Things: Taxonomies and Open Challenges,” *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, Jul. 2018.
- [8] 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,” *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, June, 2018.
- [9] N. M. Kumar and P. K. Mallick, “The Internet of Things: Insights into the building blocks, component interactions, and architecture layers,” *Procedia Computer Science*, vol. 132, pp. 109–117, Jan. 2018.
- [10] J. Soldatos, *Building blocks for IoT analytics: internet-of-things analytics*. Gistrup: River Publishers, 2017.
- [11] R. Minerva, A. Biru, and D. Rotondi. “Towards a Definition of the Internet of Things (IoT)”. *IEEE Internet Initiative I* , pp. 1–86, May. 2015.

- [12] “IERC-European Research Cluster on the Internet of Things,” www.internet-of-things-research.eu. http://www.internet-of-things-research.eu/about_iiot.htm [Jan. 02, 2022].
- [13] V. P. Kafle, Y. Fukushima, and H. Harai, “Internet of things standardization in ITU and prospective networking technologies,” *IEEE Communications Magazine*, vol. 54, no. 9, pp. 43–49, Sep. 2016.
- [14] J. Guth et al., “A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences,” *Springer Link*, [Online], 2018. Available: https://link.springer.com/chapter/10.1007%2F978-981-10-5861-5_4 [Jan.02, 2021].
- [15] K. Ghirardello, C. Maple, D. Ng and P. Kearney, "Cyber security of smart homes: Development of a reference architecture for attack surface analysis," *Living in the Internet of Things: Cybersecurity of the IoT* - 2018, 2018, pp. 1-10.
- [16] P. Clements, D. Garlan, R. Little, R. Nord, and J. Stafford, “Documenting software architectures: views and beyond,” *25th International Conference on Software Engineering, 2003. Proceedings.*, 2003.
- [17] P. Ataei and A. Litchfield, “Big Data Reference Architectures, a systematic literature review,” *Australasian Conference on Information Systems (ACIS) 2020*, Wellington, New Zealand, 2020.
- [18] M. A. Chauhan and M. A. Babar, “Using Reference Architectures for Design and Evaluation of Web of Things Systems,” *Managing the Web of Things*, pp. 205–228, 2017.
- [19] A. Maeder and P. Williams, “Health Smart Homes: New Challenges,” *Studies in health technology and informatics*, no. 245, pp. 166–169, 2017.
- [20] M. R. Alam, M. B. I. Reaz and M. A. M. Ali, "A Review of Smart Homes—Past, Present, and Future," in *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1190-1203, Nov. 2012.
- [21] H. Yang, W. Lee, and H. Lee, “IoT Smart Home Adoption: The Importance of Proper Level Automation,” *Journal of Sensors*, vol. 2018, pp. 1–11, 2018.
- [22] M. Sultan and K. Nabil, "Smart to Smarter: Smart Home Systems History Future and Challenges", *Future of HBI: Human-Building Interaction Workshop ACM CHI '16*, 2016.
- [23] D. Marikyan, S. Papagiannidis, and E. Alamanos, “A systematic review of the smart home literature: A user perspective,” *Technological Forecasting and Social Change*, vol. 138, pp. 139–154, Jan. 2019.

- [24] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," *Journal of Network and Computer Applications*, vol. 97, Future of HBI: Human-Building Interaction Workshop ACM pp. 48–65, Nov. 2017.
- [25] Z. A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)," *Wireless Networks*, vol. 25, no. 6, pp. 3193–3204, Mar. 2018.
- [26] J. Meier, I. Tsalicoglou, and R. Mennicke, "The future of NDT with wireless sensors, A.I. and IoT", 2018. Available: https://www.ndt.net/events/APCNDT2017/app/content/Paper/273_Frehner.pdf. [Jan.02, 2021]
- [27] S. B. Calo, M. Touna, D. C. Verma, and A. Cullen, "Edge computing architecture for applying AI to IoT," *2017 IEEE International Conference on Big Data (Big Data)*, Dec. 2017.
- [28] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence," *Future Generation Computer Systems*, Sep. 2019.
- [29] T. Hargreaves, C. Wilson, and R. Hauxwell-Baldwin, "Learning to live in a smart home," *Building Research & Information*, vol. 46, no. 1, pp. 127–139, Feb. 2017.
- [30] S. Kim, M. Park, S. Lee, and J. Kim, "Smart Home Forensics—Data Analysis of IoT Devices," *Electronics*, vol. 9, no. 8, p. 1215, Jul. 2020.
- [31] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive IoT," *IEEE Xplore*, [Online] Jan. 01, 2018. Available: <https://ieeexplore.ieee.org/document/8325598> [Jan. 02, 2022].
- [32] B. H. Çorak, F. Y. Okay, M. Güzel, Ş. Murt, and S. Ozdemir, "Comparative Analysis of IoT Communication Protocols," *IEEE Xplore*, [Online], Jun. 01, 2018. Available: <https://ieeexplore.ieee.org/document/8530963> [Jan.02, 2022].
- [33] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration," *ACM Computing Surveys*, vol. 51, no. 6, pp. 1–29, Jan. 2019.
- [34] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," *IEEE Xplore*, [Online], May 01, 2017. Available: <https://ieeexplore.ieee.org/abstract/document/8079928> [Jan.02 ,2022].

- [35] M. Mazzara, I. Afanasyev, S. R. Sarangi, S. Distefano, V. Kumar, and M. Ahmad, "A Reference Architecture for Smart and Software-Defined Buildings," *IEEE Xplore*, [Online], Jun. 01, 2019. Available: <https://ieeexplore.ieee.org/abstract/document/8784011> [Jan. 02, 2022].
- [36] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions," *2017 23rd International Conference on Automation and Computing (ICAC)*, Sep. 2017.
- [37] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, no. 3, pp. 1454–1464, Jan. 2017.
- [38] S. Zheng, Q. Zhang, R. Zheng, B.-Q. Huang, Y.-L. Song, and X.-C. Chen, "Combining a Multi-Agent System and Communication Middleware for Smart Home Control: A Universal Control Platform Architecture," *Sensors*, vol. 17, no. 9, p. 2135, Sep. 2017.
- [39] S. G Tzafestas, "Synergy of IoT and AI in Modern Society: The Robotics and Automation Case," *Robotics & Automation Engineering Journal*, vol. 3, no. 5, Sep. 2018.
- [40] C. McGregor, "Using Constructive Research to Structure the Path to Transdisciplinary Innovation and Its Application for Precision Public Health with Big Data Analytics," *Technology Innovation Management Review*, vol. 8, no. 8, pp. 7–15, Aug. 2018.
- [41] E. Kasanen, K. Lukka, & A. Siitonen. "The constructive approach in management accounting research", *Journal of Management Accounting Research*, Vol. 5 No. 3, pp. 243-64, 1993.
- [42] E. Y. Nakagawa, M. Guessi, J. C. Maldonado, D. Feitosa, and F. Oquendo, "Consolidating a Process for the Design, Representation, and Evaluation of Reference Architectures," *2014 IEEE/IFIP Conference on Software Architecture*, Apr. 2014.
- [43] E. Cavalcante, M. P. Alves, T. Batista, F. C. Delicato, and P. F. Pires, "An Analysis of Reference Architectures for the Internet of Things," *Proceedings of the 1st International Workshop on Exploring Component-based Techniques for Constructing Reference Architectures - CobRA '15*, 2015.
- [44] P. Fremantle, "A REFERENCE ARCHITECTURE FOR THE INTERNET OF THINGS," 201. Available: https://wso2.com/wso2_resources/wso2_whitepaper_a-reference-architecture-for-the-internet-of-things.pdf. [Jan. 02, 2022].

- [45] J. Hierro, "FIWARE: an open standard platform for smart cities," www.slideshare.com, Nov.16, 2014. Available: <https://www.slideshare.net/JuanjoHierro/fiware-a-standard-platform-for-smart-cities>. [Jan. 02, 2022].
- [46] "Y.2060:Overview of the Internet of Things," Available: www.itu.int, 2012. <https://www.itu.int/rec/T-REC-Y.2060-201206-I>. [Jan. 02, 2022]
- [47] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang, "Smart Home: Architecture, Technologies and Systems," *Procedia Computer Science*, vol. 131, pp. 393–400, 2018.
- [48] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1–2, pp. 81–98, Sep. 2018.
- [49] L. Pürgstein and H.-J. Hof, "A system to save the internet from the malicious internet of things at home," Sep. 2017. Available: https://www.researchgate.net/publication/319932617_A_System_to_Save_the_Internet_from_the_Malicious_Internet_of_Things_at_Home. [Jan. 02, 2022].
- [50] K. Bing, L. Fu, Y. Zhuo, and L. Yanlei, "Design of an Internet of Things-based smart home system," *2011 2nd International Conference on Intelligent Control and Information Processing*, Jul. 2011.
- [51] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security Requirements for the Internet of Things: A Systematic Approach," *Sensors*, vol. 20, no. 20, p. 5897, Oct. 2020.
- [52] I. Sommerville, "Architectural design." in *Software Engineering*, 9th ed., USA: Addison-Wesley, 2010, pp 165.