SCALABLE, SECURE AND INTEROPERABLE DESIGN FOR THE INTERNET OF THINGS

AMMAR JAMEEL HUSSEIN, AL BAYATI

FEBRUARY 2016

SCALABLE, SECURE AND INTEROPERABLE DESIGN FOR THE INTERNET OF THINGS

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

BY
AMMAR JAMEEL HUSSEIN, AL BAYATI

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

FEBRUARY 2016

Title of the Thesis: **Scalable, Secure and Interoperable Design for the Internet of Things**

Submitted by **Ammar Jameel Hussein, AL BAYATI**

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

Prof. Dr. Halil EYYUBOĞLU
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Müslim BOZYİĞİT
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Reza HASSANPOUR
Supervisor

Examination Date: 05.02.2016

Examining Committee Members

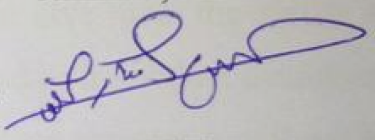
Assist. Prof. Dr. Reza HASSANPOUR (Çankaya Univ.)

Assist. Prof. Dr. Barbaros PREVEZE (Çankaya Univ.)

Assist. Prof. Dr. Kasım ÖZTOPRAK (Karatay Univ.)

STATEMENT OF NON-PLAGIARISM PAGE

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	:	Ammar , AL BAYATI
Signature	:	
Date	:	05.02.2016

ABSTRACT

SCALABLE, SECURE AND INTEROPERABLE DESIGN FOR THE INTERNET OF THINGS

Ammar Jameel Hussein, AL BAYATI
M.Sc., Department of Computer Engineering
Supervisor: Assist Prof. Dr. Reza HASSANPOUR
February 2016, 80 pages

A vast number of "things" have been used to meet innumerable commitments of ICT in our contemporary world. Most of these "things" are placed in different locations and regularly work to serve individual users or groups and give them the ability to access them by using their own networking, applications and/or individual databases. Most of these applications run these data exclusively. For these reasons, it will not be easy to integrate a third party application within them or ensure the security and privacy of collected data. Moreover, end users face difficulties in accessing these data from anywhere in a unified form. At the present moment, the adoption of delivering this technology in new ways is growing rapidly. In this thesis, a new design for the Internet of Things is proposed, which we call "Web IoT." The new design can play a role between things and stakeholders by virtualizing these entities and making them available to end users from anywhere. It also offers a wide range of tools and options for stakeholders to host many types of entities in one place, thereby giving them the ability to control and manage content, share this content in social networks, apply more personalization, dynamically update, and much more. Our design was tested in terms of scalability, functionality and flexibility. Web IoT will help to overcome the limitation of collected data in a secure and scalable manner.

Keywords: Internet of Things (IoT), Internet of Everything (Io-E), Virtual Sensor, Cloud Sensor, Sensor Network, Cloud Computing.

ÖZ

NESNELERİN İNTERNETİ (IoT) İÇİN ÖLÇEKLENEBİLİR, GÜVENLİ VE BİRLİKTE ÇALIŞABİLİR TASARIM

Ammar Jameel Hussein, AL BAYATI
Yüksek Lisans Derecesi, Bilgisayar Mühendisliği Bölümü
Danışman: Assist Prof. Dr. Reza HASSANPOUR
Şubat 2016, 80 sayfa

Çok sayıda "nesneler", çağdaş dünyamızdaki Bilgi ve İletişim Teknolojileri'nin (ICT) sayısız taahhütünü karşılamak için kullanılmıştır. Bu "nesnelerin" çoğu, farklı yerlere yerleştirilir ve bireysel kullanıcılar ya da gruplara servis vermek için düzenli olarak çalışırlar ve onlara kendilerinin ağ, uygulamalar ve/veya bireysel veritabanlarını kullanmaya erişim hakkı verirler. Bu uygulamaların çoğu sadece bu verileri özel çalıştırırlar. Bu nedenlerden dolayı, onları üçüncü parti bir uygulamaya entegre etmek ya da toplanan verilerin güvenliğini ve gizliliğini sağlamak kolay olmayacaktır. Ayrıca, son kullanıcılar herhangi bir yerdeki birleştirilmiş bir formattan bu verilere erişirirken zorluklarla karşılaşırlar. Günümüzde, bu teknolojinin yeni yollardan dağıtımının benimsenmesi hızla artıyor. Bu tezde, Nesnelerin İnterneti için yeni bir tasarım önerilmekte; biz bunu "Nesnelerin İnternetinin Ağı" olarak adlandırıyoruz. Bu yeni tasarım, nesneler ve ilgili kimseler arasında bu oluşumları sanallaştırma ve onları son kullanıcıların her yerden kullanımına sunmasında bir rol oynayabilir. Bu aynı zamanda ilgili kimseler için birçok çeşit oluşumu bir yerde barındırmak, onları kontrol etmek ve içerik yönetmek, bu içeriği sosyal ağlarda paylaşmak, daha fazla kişiselleştirme uygulamak, dinamik olarak güncellemek ve çok daha fazlası için yetkinliği verme açısından çok sayıda araçlar ve seçenekler sunar. Tasarımımız ölçeklenebilirlik, fonksiyonellik ve esneklik açısından test edilmiştir. Nesnelerin İnternetinin Ağı (Web IoT) güvenli ve ölçeklenebilir bir şekilde toplanan verilerin sınırlamasını aşmak için yardımcı olacaktır.

Anahtar Kelimeler: Nesnelerin İnterneti (IoT), Her şeyin İnterneti (IoE), Sanal Sensör, Bulut Sensör, Sensör Ağ, Bulut Bilişim

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisor, Dr. Reza HASSANPOUR, whose expertise, understanding, and patience added considerably to my graduate experience. His vast knowledge and skill in many areas is greatly appreciated.

I would also like to thank my family for the support they provided me throughout my entire life, without whose love, encouragement and editing assistance, I would not have finished this thesis.

I also extend my thanks to the Iraqi Board of Supreme Audit Iraq/Baghdad (Government Body), which provided me the opportunity to study.

TABLE OF CONTENTS

STATEMENT OF NON PLAGIARISM..... iii

ABSTRACT..... iv

ÖZ..... v

ACKNOWLEDGEMENTS..... vi

TABLE OF CONTENTS..... vii

LIST OF FIGURES..... xi

LIST OF TABLES..... xiii

LIST OF ABBREVIATIONS..... xiv

CHAPTERS:

1. INTRODUCTION..... 1

1.1. Introduction..... 1

1.2. Objectives..... 2

1.3. Thesis Layout 2

2. BACKGROUND..... 3

2.1. Sensor Network..... 3

2.2. Cloud Computing..... 4

2.2.1. Software as a Service (SaaS)..... 5

2.2.2. Platform as a Service (PaaS)..... 6

2.2.3. Infrastructure as a Service (IaaS)..... 6

2.3. Virtual Sensors..... 6

2.3.1. Virtual Cloud Sensor..... 6

2.4. The Internet of Things 8

2.4.1. Things That Think 10

2.4.2. Internet of People 11

2.4.3. The Web of Things..... 11

2.5. Sensor Model and Standardization..... 12

2.5.1. Sensor Web Enablement (SWE)..... 12
2.5.1.1. SensorML..... 13
2.5.1.2. Sensor Observation Service (SOS)..... 13
2.6. The Internet of Things Applications..... 13
2.6.1. Smart Cities..... 14
2.6.2. Smart Agriculture..... 14
2.6.3. Smart Water..... 14
2.6.4. Retail and Supply Chain Management..... 15
2.7. Sensor Network Security..... 15
2.7.1. Limited Resources..... 15
2.7.2. Unreliable Communication..... 16
2.7.3. Unattended Operations..... 16
3. LITERATURE REVIEW..... 17
3.1. Evaluation of Methodology..... 17
3.1.1. Internet of Things Paradigm..... 18
3.1.1.1. Mobility First Future Internet Architecture..... 18
3.1.1.2. Cloud Assisted Remote Sensing..... 19
3.1.1.3. Internet of People..... 20
3.1.2. Sensor Cloud Paradigm..... 21
3.1.2.1. Virtualized Sensors on Cloud Computing..... 21
3.1.2.2. Virtual Cloud Sensor..... 22
3.1.2.3. Cloud for Sensing..... 23
3.1.3. The Web of Things Paradigm..... 24
3.1.3.1. Web of Things Framework..... 24
3.1.3.2. The Virtual Environment of Things..... 25
3.1.3.3. Social web of Things..... 25
3.2. Security and Privacy Requirements..... 26
3.2.1. Data Confidentiality..... 26
3.2.2. Availability..... 26

3.2.3. Data Freshness…….. 26
3.2.4. Data Integrity and Authentication…… 27
3.2.5. Time Synchronization…….. 27
3.2.6. Self-Management……. 27
3.2.7. Secure Localization…….. 28
3.3. Research challenges..... 28
3.3.1. Big Data…… 28
3.3.2. Lack of Standardization…… 28
3.3.3. Identity Management…… 29
3.3.4. Connectivity Robustness…….. 29
3.3.5. Security and Privacy……. 29
4. DESIGN AND IMPLEMENTATION…..... 30
4.1. Web-based Internet of Things (Web IoT)..... 30
4.1.1. Proposed Reference Architecture……. 30
4.1.1.1. Application Layer……. 31
4.1.1.2. Middleware Layer……. 32
4.1.1.3. Network Layer…….. 33
4.1.1.4. Physical Layer…….. 34
4.2. Experiment Workbench..... 34
4.2.1. Lab Components……. 35
4.2.2. Lab Environment……. 36
4.2.3. Backend Implementation……. 36
4.2.4. Frontend Implementation…… 37
4.2.5. Overall Workbench Structure……. 37
5. RESULTS AND DISCUSSION..... 38
5.1. Web IoT Features..... 38
5.1.1. Web Content Management……... 38
5.1.2. Flexibility……. 40
5.1.3. Scalability……. 43

5.1.4. Reliability……. 44
5.1.5. Security and Privacy……. 45
5.1.6. Documents and Media Repository……... 46
5.1.7. Unified Access……. 47
5.2. Comparative Related Paradigms..... 47
5.3. Performance Evaluation……. 49
5.4. Compare System Performance…….. 53
6. CONCLUSION AND FUTURE WORK..... 54
6.1. Conclusion……. 54
6.2. Future Works……. 55
REFERENCES..... R1
APPENDICES..... A1
A. CURRICULUM VITAE.....…..…….....…… A1

LIST OF FIGURES

FIGURES

Figure 1	Three Types of Cloud Services……..	5
Figure 2	Internet of Things (IoT) Vision…….	8
Figure 3	IoT five layers schema……..	9
Figure 4	Middleware Services...…….……..	18
Figure 5	CARS Fourth Layers Architecture…….	19
Figure 6	IoP Middleware Architecture…….	20
Figure 7	Sensor Virtualization Proposed Architecture…….	21
Figure 8	Sensor Cloud Proposed Architecture……..	22
Figure 9	Cloud for Sensing Architecture……..	23
Figure 10	WoT Proposed Architecture……...	24
Figure 11	SoT Structure…….	25
Figure 12	Web IoT Abstract layer Architecture……	31
Figure 13	Web IoT Middleware Layer Reference Architecture……	32
Figure 14	Web IoT Net Work Zone Layers……..	33
Figure 15	Test Lab Components…….	35
Figure 16	Web IoT Overall Workbench Structure……..	37
Figure 17	Web IoT Main Page……	39
Figure 18	Web IoT Welcome Page…….	39
Figure 19	Web IoT Admin Page…….	40
Figure 20	Web IoT User 1 Home Page……...	41
Figure 21	Web IoT User 2 Home Page……...	42
Figure 22	Web IoT User 3 Home Page……...	43
Figure 23	Web IoT Available Tools……...	44
Figure 24	Web IoT UTM Dashboard……...	45
Figure 25	Web IoT Storage Repositories Login Page……	46
Figure 26	Web IoT Medea Stream Repositories…….	46

Figure 27 Web IoT File Storage Repositories……..... 47
Figure 28 Test Plan Implementation……... 49
Figure 29 100 Threads Run 100 Times Results…….. 50
Figure 30 150 Threads Run 100 Times Results…….. 51
Figure 31 200 Threads Run 100 Times Results…….. 51
Figure 32 250 Threads Run 100 Times Results…….. 52
Figure 33 300 Threads Run 100 Times Results…….. 53

LIST OF TABLES

TABLES

Table 1	Related Work Paradigms Comparison……	48
Table 2	Test 1-100 Threads Run 100 Times Results……	50
Table 3	Test 2-150 Threads Run 100 Times Results……	50
Table 4	Test 3-200 Threads Run 100 Times Results……	51
Table 5	Test 4-250 Threads Run 100 Times Results……	52
Table 6	Test 5-300 Threads Run 100 Times Results……	52
Table 7	Comparing System Performance…….	53

LIST OF ABBREVIATIONS

CARS	Cloud Assisted Remote Sensing
CoAP	Constrained Application Protocol
DMZ	Demilitarized Zone
GPS	Global Positioning System
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
Io-E	Internet of Everything
IoP	Internet of People
IoT	Internet of Things
IPS	Intrusion Prevention System
Java ME	Java Platform Micro Edition
Java SE	Java Platform Standard Edition
JRE	Java Runtime Environment
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
O&M	Observations & Measurements
OGC	The Open Geospatial Consortium
PaaS	Platform as a Service
RFC	Request for Comments
RFID	Radio Frequency Identification
SaaS	Software as a Service
SAS	Sensor Alert Service

SC	Sensor Cloud
SensorML	Sensor Model Language
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SOA	Service Oriented Architecture
SOS	Sensor Observation Service
SoT	Social web of Things
SPS	Sensor Planning Service
SRA	Internet of Things Strategic Research Agenda
SSO	Single Sign-On
SWE	Sensor Web Enablement
TML	Transducer Model Language
UTM	Universal Thread Management
VEoT	The Virtual Environment of Things
VM	Virtual machine
WNS	Web Notification Services
WoT	Web of Things
WSDL	Web Services Descriptive Language
XML	Extensible Markup Language
6LowPAN	IPv6 over Low Power Personal Area Network

CHAPTER 1

INTRODUCTION

1.1 Introduction

Worldwide demand to develop information and communication technology is constantly growing at an increasing rate. As a result of this enormous development and continuous need for a number of ever more powerful smart things, (such as smartphones, smart TVs, smart cars and many more other things), a wide range of physical objects such as sensors have been used for multiple purposes in our life. These have been applied in a wide range of application areas such as health care, environmental monitoring, the military sector, transportation and many other applications. These smart devices, smart applications, physical objects and many other entities with their own unique identifier along with the embedded system, gives them the ability to send or share data over communication lines. We can now refer to these as “things” [1]. In the context of the Internet of Things (IoT) [2], these “things” use different types of technology to gather data or sense data from both objects and areas. For the most part, they link to private or public networks. The growing need for these things significantly impacts the global traffic volume in the ICT world, which includes data, multimedia, information as well as our interest in ICT. This has changed the vision of our life, more or less. The Virtual Cloud Sensor, the Internet of Things (IoT) and the Internet of Everything (Io-E) [3, 2, and 4] are newer suggested models for interacting respectively with sensors, human beings and anything. They aim to build an intermediate middleware layer between things and stakeholders with the possibility of machine-to-machine talking and zero human interaction. Such designs will overcome limitations of resources and improve the efficiency of using science and technology to serve a new information and communication technology vision.

1.2 Objective

In this research, we will discuss the manner, applications and issues of the Internet of Things (IoT). The core objectives of this research will be to introduce a secure and scalable design for the Internet of Things (IoT). The design consists of multiple layers and plays a role of dealing with different types of things that reside in diverse locations and operate using different applications while considering security and integrity issues. Additionally, we will speculate upon the future of this technology, i.e., the Internet of Everything (Io-E). This research will cover the following areas:

1. Design a scalable platform for the Internet of Things that enables different types of things placed in a huge geographical area to be accessible and deployed from anywhere.
2. Deploy a flexible host application on top of resource-constrained things that can host multiple things in one place.
3. Deploy a secure model to secure our platform and to ensure security and privacy of communication lines and sensing data.

1.3 Thesis Layout

The layout of the remainder of this document is structured as follows:
Chapter 2 expounds upon the backgrounds and the theoretical part. In this chapter, we will provide an overview of the most important components that serve our research criteria.
Chapter 3, literature review, is divided into three parts: the evaluation of the methodology, security requirements and research challenges. The methodology is evaluated according to the established paradigms that have been used in related research. It is classified into three groups: the Internet of Things Paradigm, the Sensor Cloud Paradigm and the Web of Things Paradigm.
Chapter 4 presents the design and implementation. Here, we discuss the proposed reference architecture and workbench implementation.
Chapter 5 presents design features, a comparison of related paradigms and analyses of the results obtained from the implementation.
Chapter 6 presents our conclusions and future work.

CHAPTER 2

BACKGROUND

2.1 Sensor Network

Sensor networks, or wireless sensor networks, are self-deploying networks that involve a vast number of sensor components, i.e., self-sensor devices or sensors as components inside other devices such as mobile phones, TVs, etc. These sensors are linked to each other over a network. These networks mostly use wireless communication, a station, or nodes in a single-hop or multi-hop fashion to send and receive sensing data [5]. These sensors gather the data required by the sensor design objective itself and send identifying sensing data to a vital network station or node for more advance handling and processing. Currently, a Sensor Network takes on the main role in several fields, such as video and audio surveillance, catastrophe and natural disasters, environmental applications, healthcare applications, and military sector applications, in addition to being increasingly and rapidly used in new paradigms such as the Web of Things, the Internet of Things (IoT), the Internet of Everything (Io-E) and the Things that Think and Sense Web [6]. Nevertheless, sensors have become low-slung cost devices. Moreover, they have some limitations, such as limited resources (energy and power source, unit processing, memory, communications channel and availability). Most designers of Sensor Networks these days take this into consideration, particularly power source constraints such as battery life, which can limit the life period of a sensor itself. Additionally, many of the considerations above are still open research issues in science and technology.

As a result, many of the effective power performance methods have improved and almost all protocols that have been used in sensor networks are enhanced to decrease power feeding. These improvements include working in different layers, including the Transport Layer [7], the Network Layer [8], the Physical Layer [9] and the Medium Access Control Layer [10]. In the meantime, the communicating process

Needs extra power relative to the data process handling tasks. A variety of additional machineries have been suggested and improved to save power. These include external-network handling [11], topology restructuring [12, 13], Time Synchronization [9] and Node Architecture [14].

Correspondingly, the security and privacy of a sensor node and communications line is also a major standing issue in the sensor network [15]. Sensing and carrying data more often has its own private use and nature. Many challenges in this aspect have been issued. Furthermore, many proposals for solutions have been applied, including cryptography and steganography. However, such techniques are extremely costly to be implanted in such devices, i.e., time considerations, especially in real-time applications. Others have suggested solutions that include adding security information hooked on to the data packet. Again, this will cost in terms of processing and memory. Lastly, another aspect of the challenge in sensor networks can be the availability and operational costs as a result of unreliable communications lines, environmental conditions and restrictions of energy sources.

2.2 Cloud Computing

Cloud computing exists as a paradigm to assist network access from anywhere upon user demand, whether in a public and private concept role [16]. It is built on top of physical networks and data centers by using a shared resources model (e.g., servers, applications, services, networks, and storages). This model component can swiftly reduce the number of network management tools required in addition to lower requirements for administrator interaction.

A cloud computing podium dynamically supplies, forms and reforms of all its components depending on user need and user choice. Some of these components may be available as a virtual machine (VM) or as a physical one. Recently, cloud computing achieved the two main milestones in ICT [17], the first being high efficiency that was achieved over the extremely scalable access to software and hardware resources and the second being mobility, which was achieved by providing a corresponding parallel process, business analyses and real-time collaboration applications that effectively react to user demand.

The primary advantages of cloud computing lie in the technical details, such as transparency for the end consumer; e.g., they do not need to be concerned regarding the exact site of services or servers and they can easily control their own applications by linking to cloud servers and running them without any difficulty.

Cloud computing usually offers three classes of service [18], namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Figure (1) depicts three types of Cloud Service.

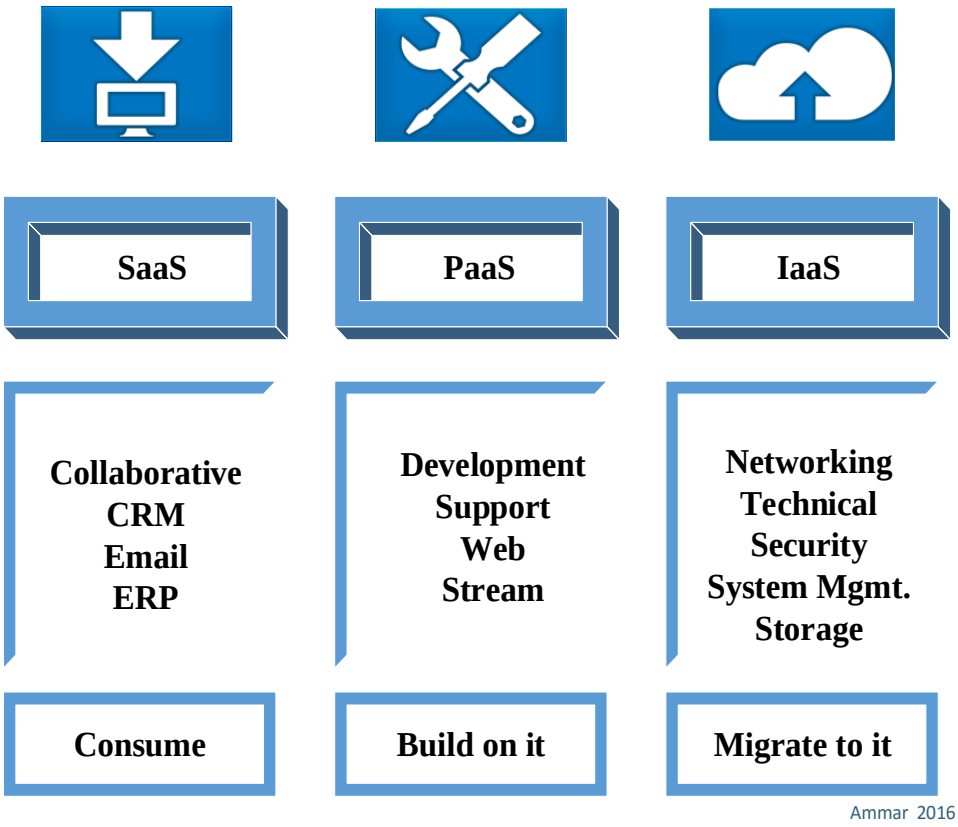


Figure (1) Three Types of Cloud Service

2.2.1 Software as a Service (SaaS)

Software as a Service [18] mentions applications that function through a cyber-link. It can be obtained for the end consumer on a pay-as-you-go basis. The consumer does not need to install or maintain any application. In its place, the only requisite is a cyber-link for admission to the required service being leased by the Software as a Service cloud provider.

2.2.2 Platform as a Service (PaaS)

Platform as a Service [18] offers a cloud podium to construct services and applications along with all essential resources and necessary toolkits.

2.2.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service [18] offers storage and computation as services on a leasing basis. It has arisen from the idea of the consumer not needing to buy a server or storage devices even if the consumer has minor tasks. The consumer can forward a task to the Infrastructure as a Service cloud provider at a reasonable price. By using storage in the cloud, the consumer can store and access data from anywhere using a cyber-link.

2.3 Virtual Sensors

The term of sensor virtualization or virtual sensor [3] can be clearer if it is defined as attempting simulation or emulation of the physical sensor in the real world that gains its statistics/data from fundamental physical sensors. These sensors can be attached to a group of virtual sensors. Moreover, this type of virtual group can offer a custom-built view, hide technical details for the end consumer and use resource sharing and site transparency.

In a sensor network, a sensor device is intelligent enough to handle several tasks simultaneously to serve multiple users and applications on demand. Furthermore; virtual sensors can have their own programing code that can be reused in data processes to create composite inquiries by the user.

2.3.1 Virtual Cloud Sensor

A cloud of sensors is involved in a set of virtual sensors as a layer builds-up on top of existing physical sensors or sensor networks so that the consumer can dynamically establish or withdraw his application demands [3]. This method has a number of advantages, including offering an enhancement to sensor administration ability, the consumer being able to customize his own view and functions for a diversity needs

for example, selection of region of interest, privacy, security and latency. Additionally, data in virtual cloud sensors can be shared among many customers in a unified form [19]. This can also decrease the total cost required for data gathering in both sidewise systems and consumers, Moreover, redundant statistics/data are decreased and system efficiency increases. Finally, it has the same concept of cloud computing, which means consumers do not need to concern themselves with sensor details, including types of sensors being used, sensor codes and how to design or configure them. The Sensor Cloud dynamically handles technical issues. Individual virtual sensors or a group of these sensors can be configured to have one to four diverse structures [20], such as many to one, one to many, many to many, and derived structures.

1. Many to One Structure

   These structures take a geographical region of sensors and reallocate them into zones where each zone has one or more physical sensors or sensor networks. When the user demands one zone, all corresponding physical sensors within that zone are involved in this demand.

2. One to Many Structure

   One physical sensor is attached to many virtual group sensors, i.e., one physical sensor serves multiple users with simultaneous demands.

3. Many to Many Structure

   This structure is a grouping of the many to one and one to many structures, i.e., many physical sensors in a zone can respond to a single user. It can also be one physical sensor linked to many virtual group sensors.

4. Derived structure

   Derived configuration denotes a multipurpose configuration of different virtual sensor groups resulting from a mixture of different physical sensor types even though the virtual sensor groups join only the same type of physical sensor in the above three structures.

2.4 The Internet of Things

The Internet of Things (IoT) [2] is a novel architecture that uses the Internet to connect things. These things may be objects, smart devices or any type of entity. The Internet of Things allows these things to organize themselves, achieve smartness and share information about themselves. Moreover, they can access information that has been collected by other things. IoT permits things and people to be linked to anything, anywhere at any time by anyone. It ideally uses any connecting network to provide services and uses the Internet as a backbone. The Internet of Things (IoT) was first announced as a term by Kevin Ashton in 1998 as the then upcoming future of the Internet and computing [21]. Figure (2) shows the Internet of Things (IoT) vision.

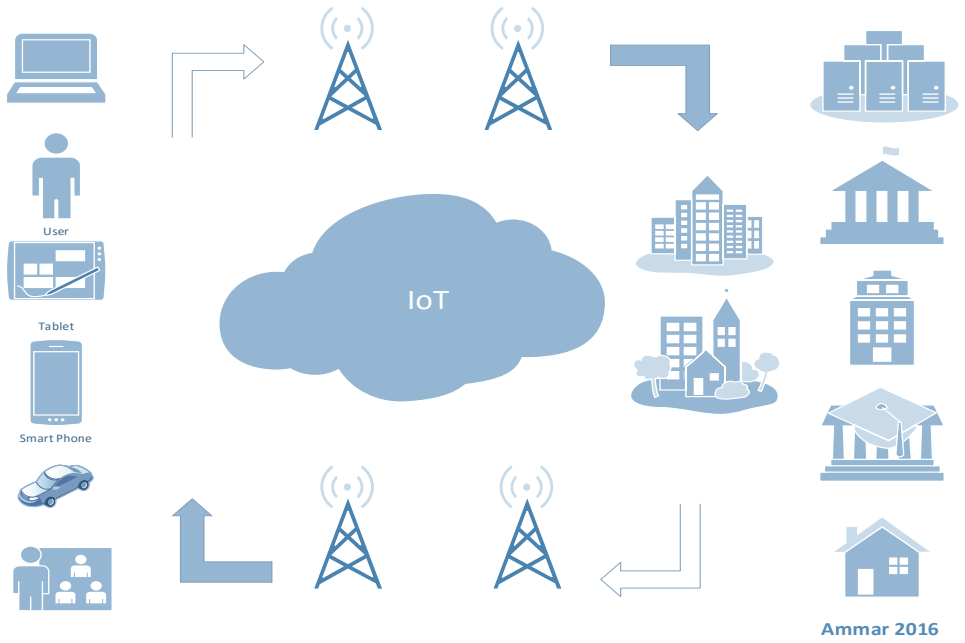


Figure (2) Internet of Things (IoT) Vision

The Internet of Things uses many technologies to connect things. These things can turn out to act as communication nodes over the Internet by using data communication resources such as Radio Frequency Identification (RFID). The Internet of Things also contains smart things which can accomplish specific tasks without human interaction, including machine-to-machine talking. Therefore, the Internet of Things can be considered not only as a hardware and software model but also be considered to contain social characteristics and zero human interaction [22].

The Internet of Things paradigm generally includes three layers: an application layer, a network layer and a physical layer. However, some new research suggests adding two more layers: a business layer and a middleware layer [23, 24]. Figure (3) shows the five layers in the IoT schema.

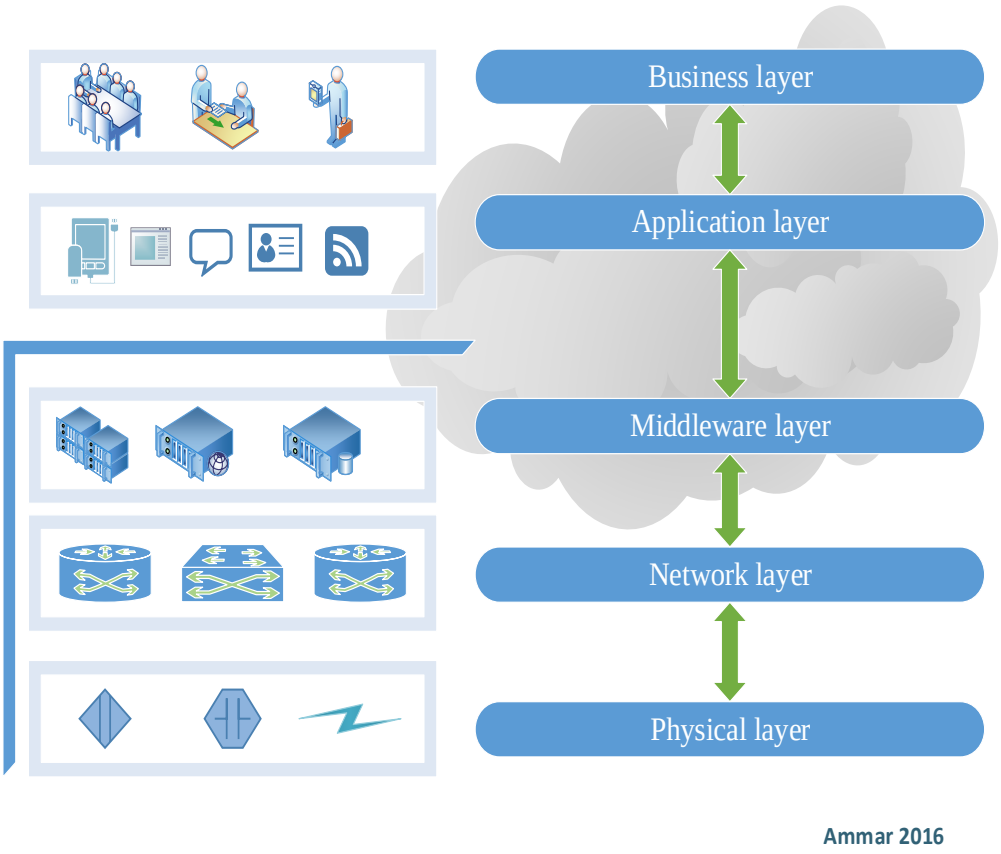


Figure (3) IoT five layers schema

1. Physical layer

   The physical layer is the lowest layer in the Internet of Things model. The main objective of this layer is to identify data from things/objects, e.g., data gathering, sensing data, which is also considered to be a task carried out by this layer [25]. Connecting sensors, object labels, GPS, RFID tags, etc.

2. Network Layer

   The Network layer serves the up and down layers by forwarding the gathered data packets received from the physical layer to the application layer and vice versa. Its role is similar to the network layer of the TCP/IP model [24] the main function of this layer is to provide network gateways with one or more network interfaces on both sides of the sensor network and Internet. This layer should handle all network protocols.

3. Middleware Layer

   The main objectives of the middleware layer are information processing, service management, authentication and storage management [24]. This layer can react dynamically depending on the results obtained.

4. Application layer

   This layer carries out the final demonstration of data. It receives data from middleware layer and gives the consumer a general view of its handling within the application offering this data [23]. This founded data is based on authentication from the middleware layer and only the authorized consumer can view his own data at this stage. Moreover, the consumer can share his own data with any other consumer. This data can form in multiple ways depending on the service types being offered, e.g., smart home, smart city, smart transportation, smart health and many other applications.

5. Business layer

   This new suggested layer is concerned with money [23] or how to reform the service that is already offered to meet a new consumer need. This layer actually attempts to give received data more than one form.

Finally, the Internet of Things acts based on machine to machine talking with zero human interaction, but it's not restricted by it, people and non-connected object, even non-smart device, can be part of the Internet of Things. For this reason the Internet of Things has two actors, things and peoples, some IoT component briefly described below.

2.4.1 Things That Think

Things in the context of the Internet of Things can be any object, smart devices, entities that can be linked to a network and provide information regarding the purpose for which it was designed whether with or without computing abilities [26]. Usually these objects have mobile ability and can be active or passive power sources.

Some objects have their own batteries and others are powered by sources from the environment and natural surroundings, such as light, water, heat, etc. Mobility denotes a communication link between an object and the main station or nodes that are wireless.

2.4.2 Internet of People

The Internet of people (IoP) [27] is a new developed paradigm that attempts to extend the usage of the Internet of Things by involving the things around people so as to interact with them positively and meaningfully in their normal daily lives.
In the Internet of Things, the main goal of integrating things is to have these things become involved in our life and to make them more easily accessible for the consumer by having a machinery model work for them effortlessly. On the other hand, the Internet of People suggested that these things can analyze data and make decisions depending on data acquired from consumers themselves and then respond to these data accordingly.

2.4.3 The Web of Things

The Web of things (WoT) is a new paradigm that attempts to extend the concept of the Internet of Things. The Web of Things is an impression of typical lives that assumes that conventional objects and sensors are fully connected and integrated using Web 2.0 technology [28]. The Web of Things presents several benefits in web society and has suggested a new web application paradigm. These applications can be simply built on top of objects using Web development utilization; this may include blogging, securing, searching, linking, caching, etc. The Web of Things paradigm provides a scalable and remarkable model and because of this, some researchers have faith that this model will be suitable for connecting objects in uniform edges and be simply applied by following these steps:

1. Linking the object to the Internet by using IPv4 or IPv6
2. Enabling a Web service on these objects
3. Utilizing these services and putting them into the Web model
4. Representing these services as Web resources

Essentially, the Web of Things process can be achieved in two different ways: the first method includes enabling web services with an object or by deploying another device to act as a gateway. The main objective of this gateway is protocol conversion from TCP/IP protocols to the protocol being used by a specific object, including ZigBee, Bluetooth, etc. Gateway methods are preferred as it is not likely to attach a TCP/IP stack within objects, such as barcodes and RFID tags [29]. A new study [30] on the issues in the Web of things discusses the global detection of objects, Web services enablers in objects, time synchronizations, interaction through the web and language standardization.

2.5 Sensor Model and Standardization

In the present day, there are many efforts to characterize sensor data as standard data entities. This helps to build a based structure model for sensor systems. These new data representations attempt to produce a standardized model for sensor networks.
This model can support diverse sensor applications to alter data effortlessly between sensor networks.

2.5.1 Sensor Web Enablement (SWE)

This first model was developed for this aspect, namely Sensor Web Enablement (SWE) standards founded by the Open Geospatial Consortium (OGC) organization [31], who formulated a set of standards/model and schema to gather so as to serve geographic interoperability. Sensor web enablement standards deliver essential structure encodings that permit a real-time combination of various sensors. Engineers, developers and application designers can use these standards to create their product platforms and applications. To enable the web in these devices, Open Geospatial Consortium members work with many services and encodings. SWE encoding includes Sensor Model Language (SensorML), Observations & Measurements (O&M), Transducer Model Language (TML) and SWE services which include the Sensor Observations Service (SOS), Web Notification Services (WNS), Sensor Alert Service (SAS), and Sensor Planning Service (SPS).

2.5.1.1 SensorML

Sensor Modeling Language (SensorML) [32] is a data model language similar to Extensible Markup Language (XML).SensorML attempts to offer a mechanism to describe the data of sensor systems and their communicator podiums. Every single sensor will be modeled as a functional operator that is an essential portion of the system. These essential operators cover input and output performance. The model metadata delivers information regarding measured phenomenon, calibration information, location information, time stamp for measurements, and the purpose of the measurement. However, this standard model still has many restrictions as it is assumed that the application and consumers have the ability to identify their requirements by labeling the operatives prerequisite for a specific assignment manually, Moreover, it does not adaptively address issues as it is assumed that there are no constraints on sensor data resources.

2.5.1.2 Sensor Observation Service (SOS)

This web service standard has been approved by the Open Geospatial Consortium [31] and describes a web service edge to enable detection and the retrieval of data in real-time applications. It is encoded in SensorML and measures values with O&M encoding.

2.6 The Internet of Things Applications

There are many application areas that can use the Internet of Things concept and these applications can be various and extended in all areas in people's daily lives. Such applications change our vision of life more or less. The main applications that affect people's daily lives may be in environmental, business and societal domains. Almost all Internet of Things applications can be classified according to one of these domains. The Internet of Things Strategic Research Agenda (SRA) in 2010 [33] added six more application domains: *Smart Cities, Smart Buildings, Smart Living, E-Health, Smart Energy* and *Smart Transportation*.Other research surveys for the Internet of Things (also during 2012) [34] presented fourteen domains: *Smart City, Smart Home, Smart Transportation, Smart Factory, Smart Life Style, Environment,*

Energy, Agriculture, Retail, Health Care, Supply Chain, Emergency, Culture and Tourism, and *Smart Water*. Some important domains are briefly overviewed below.

2.6.1 Smart Cities

The Internet of Things has a dynamic role in expanding applications in smart cities [35]. Such applications include parking applications, checking the physical conditions of bridges and building structures for vibrations and states of health, monitoring annoying sounds in some areas inside cities, light adaptively inside cities, tracking vehicles within cities, monitoring levels of garbage, waste accumulation, smart highways and smart roads, traffic jams, smart transportation systems and green buildings, etc. Most of these applications use different technologies to connect to the network. These technologies include WSN, RFID or individual sensors as a component in the Internet of Things.

.

2.6.2 Smart Agriculture

Internet of Things applications offer assistance to improve agriculture [36], such as monitoring soil validity, the level of humidity in the air and soil, monitoring distillation levels, control over the timing and amount of irrigation, monitoring environmental conditions surrounding crops to maintain the quality of produce, analyses of weather conditions and providing alerts in cases of atmospheric instability (winds, rain and snow), controlling the temperature inside a greenhouse, etc. These types of applications usually use WSN.

2.6.3 Smart Water

Internet of Things applications play a vital role in water administration. These applications may contain [37] control reservoirs and dams that monitor elements such as water level, times of loading and unloading, water level in rivers and stability, detection of water pollution, detection of fluids out of tanks and pipelines and warning of tsunamis, etc. These types of applications are usually used with WSN, and underwater sensor technology to server their purpose.

2.6.4 Retail and Supply Chain Management

The Internet of Things has many applications that can be used in retail and supply chain administration along with providing numerous benefits [38, 39]. These benefits include product tracking, controlling storage conditions, monitoring supply chain life cycles, monitoring expense processing attached to activity and location, monitoring production life cycle and product transportation, etc. Some other types of applications in this domain offer different types of services such as direction, preselected shop lists, guidelines, automatic check out, detection of product quality, modified product prices automatically controlling product shortages or surpluses, or providing warnings in cases of expiration, etc. This type of application usually uses WSN and RFID tags.

2.7 Sensor Network Security

Sensor networks usually have several restrictions similar to other network types. Therefore, it is not logical to implement a conventional security policy such as the traditional security steps [40, 41]. Consequently, to build a security operational platform for the Internet of Things, we need first to understand the nature of these restrictions on the form of the network. Some sensor network restrictions are briefly described below.

2.7.1 Limited Resources

Security mechanism procedures need a specific volume of resources to be available at least to implement this mechanism, including processing units to handle code, memory resources and power in sensor devices to carry out tasks in a timely manner. It is axiomatic that these resources are very scarce in the context of sensor networks. The two main restrictions are the power and memory needed [42, 43].

2.7.2 Unreliable Communication

Implementation of security mechanism procedures hinges on the implementation of a set of protocols [42], which ultimately hinges on the reliability of the communication line within the network. This can break down the security mechanism in different ways.

1. Unpredictable Communication links
   Security network packets may be damaged, due to link errors packets dropped in high data traffic congested within the interior of the network.

2. Interference
   Wireless sensor networks use a space to broadcast and because of the nature of link competition, interference, collisions and crashes may occur in the wireless packets.

3. Latency
   Because of the load in data traffic and the process time needed, delays may occur in the sensor network. This will directly impact the security mechanism in real-time applications.

2.7.3 Unattended Operations

Wireless sensor networks are designed to operate in natural conditions [42]. Sometimes these natural conditions may be beyond our control, including natural disasters, animal attacks, storms, etc. Therefore, physical attacks can occur in a sensor network.

CHAPTER 3

LITERATURE REVIEW

3.1 Evaluation of Methodology

The Internet of Things, the Sensor Cloud and the Web of Things are the three main paradigms that deal with sensors or things, these things may be accessible from anywhere by anyone. This has captured the attention of many researchers in several fields nowadays. Basically, these three paradigms deal with sensors in the context of things, gather data and perform the processing through many sensor networks. The accumulation of information empowers sharing of this information on large-scale form and enables applications collaboration on cloud computing. Agreeing with Gartner (the world's leading information technology research and advisory company) [44], research carried out in 2013 and republished in 2014, *"There will be nearly 26 billion devices on the Internet of Things by 2020"* [45]. Another study accomplished by ABI Research [46] states that *"More than 30 billion devices will be wirelessly connected to the Internet of Things by 2020"* [47]. Moreover, there are new studies conducted by Cisco that introduce a new paradigm, namely the Internet of Everything [48]. This also reflects rising demand in this industry. Furthermore, there is an urgent need for a new addressing system has arisen to cover this enormous number of expected link of things to a network. The Internet Engineering Task Force[49] introduced RFC 4919 and after some time, RFC 4944 demonstrated in what manner an IPv6 stack might be put on top of the IEEE Standard 802.15.4 to help covering of a huge addressing scale needed in the context of connecting things. The new standard called (6LowPAN) [50], Other researchers and organizations focused on providing standard ways to deal with sensor data, including Sensor Model Language [32], Web Services Descriptive Language [51] and Simple Object Access Protocol [52], In this Section, a discussion for the related research will be reviewed in three sub-sections, classified according to the established paradigms.

3.1.1 Internet of Things Paradigm

Many researchers have been interested in the development of Internet of Things paradigms. They have proposed a new architecture and addressed many issues in this regard.

3.1.1.1 Mobility First Future Internet Architecture

Jun Li et al [53] introduced a new architecture called *"Mobility First Future Internet Architecture*." [54] This project aimed to exchange the client/server model with a new model based on a mobile platform/application. They also claimed that this architecture will be a design for the following generation Internet or a future of the Internet paradigm. It is worth mentioning that this paradigm is not fundamental yet. Consequently, they show the need for change in the type of service provided, a move forward to a new structural design and a new management methodology. Figure (4) summarizes the three services in middleware layers, the key goals of this project are the mobility of things, enhancement of security and the privacy of things, energy constraints in things and sensors, and enabling the Internet of Things mobility services. In these partial services, they divided the middleware layer of the Internet of Things to be presented as a service in the context of mobility, i.e., architecture to reduce the accreditation of the middleware layer. Consequently, they reduced the cost of building and maintaining this layer. On the other hand, maintaining security and privacy has become unclear.

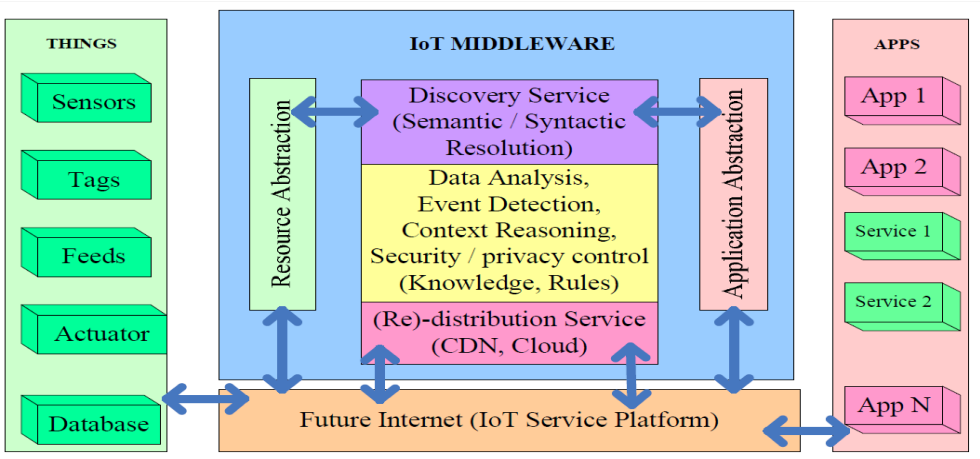


Figure (4) Middleware Services [53]

3.1.1.2 Cloud Assisted Remote Sensing

Sherif Abdelwahab et al [55] introduced a new paradigm that can provide smart cloud services and can be considered the first attempt to activate the concept of the Internet of Everything. The project aimed to facilitate data sensory gathering, remote data access, the improvement of data sharing, the provision of a pay-as-you-go cost per service and the marginalization scaling problem. Furthermore, they introduced a design architecture, including four layers proposed as an Internet of Everything enabler architecture. The first layer was labeled the Fog Layer and played the role as a physical layer in the TCP/IP model. The second layer was labeled the Stratus Layer. This layer focused on the Cloud of Things and the cloud sensory provider. The third layer was named the Alto-Cumulus Layer. It functioned as a middleware layer that served the upper and lower layers. The fourth was named the Cirrus Layer as this layer had the same role as the applications layer in the Internet of Things paradigm. Figure (5) shows the fourth layer architecture, the services provided by this architecture can be used as a smart cloud service and is considered to be the first attempt for the Internet of Everything enabler. On the other hand, the cost and keys requirement to enable this service is relatively high.

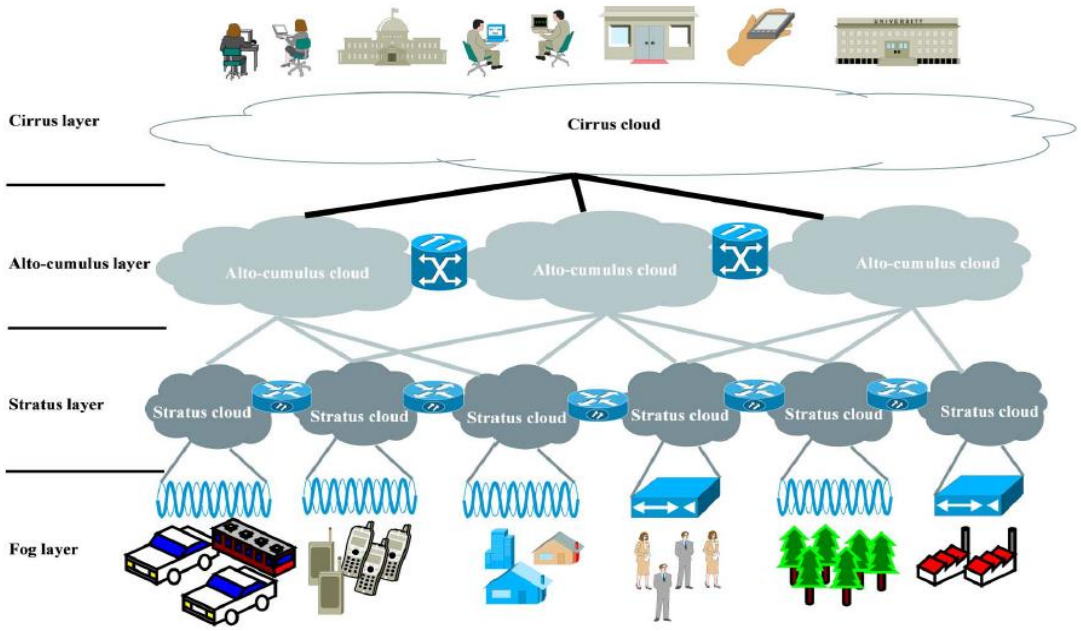


Figure (5) CARS Fourth Layers Architecture [55]

3.1.1.3 Internet of People

Javier Miranda et al [27] proposed a smart architecture that is based on smartphones as a way to interact with people that involved Internet of Things applications. The new elements in this paradigm include the consideration of interacting and the adaptively between people and smart things in every day live by context of Internet of Things, This is an important idea that extends the use of Internet of Things applications and makes them smarter with people in everyday life activity.

Moreover, they discuss the related social issues of the impact on people to accommodate this transformation, i.e., from real life to smart life. Finally, they design a middleware architecture that depends on this discussion and considers People as a Service (PeaaS) [56], and Social Devices. This layer has many components such as an action repository, application repository, and device registry and application manager. Figure (6) shows middleware architecture.

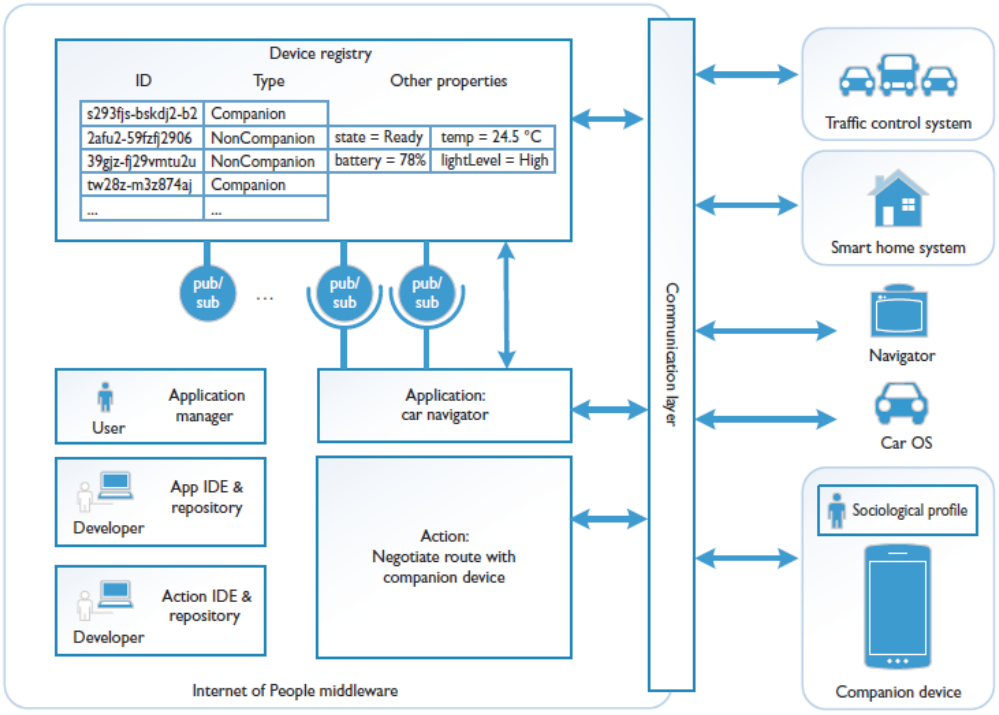


Figure (6) IoP Middleware Architecture [27]

This model gives users the ability to build social profiles in their own devices and shear these profiles with the middleware layer, which will enable the adaptive reaction between things, some weaknesses in this project include issues that are outside the scope of the technology framework and assume the end-user interference as a part of this model.

3.1.2 Sensor Cloud Paradigm

While the Internet of Things combines things and services in the context of the cloud, the sensor cloud takes a different approach, namely to attempt to build a virtual sensor on top of the existing physical sensors. Many studies have been carried out to support this paradigm.

3.1.2.1 Virtualized Sensors on Cloud Computing

IBM Japan, Ltd., Shimotsuruma et al [3], at the 2010 IBM Research office/Tokyo with contraptions of others researchers, introduced approaches to represent a physical sensor in cloud computing. This approach enabled the physical sensor to be accessible from anywhere. Moreover, they addressed the challenges of future work in these approaches, the actor's role in the sensor cloud, and compared the proposed architecture with current studies regarding sensor networks. The main benefits of this architecture was hiding the technical details from the consumer, the end user having the ability to control his own virtual sensors. Figure (7) shows the proposed architecture. The main disadvantages of this architecture were that the system administrator should prepare a virtual sensor for each physical sensor in addition to the cost needed to prepare the ICT infrastructure.

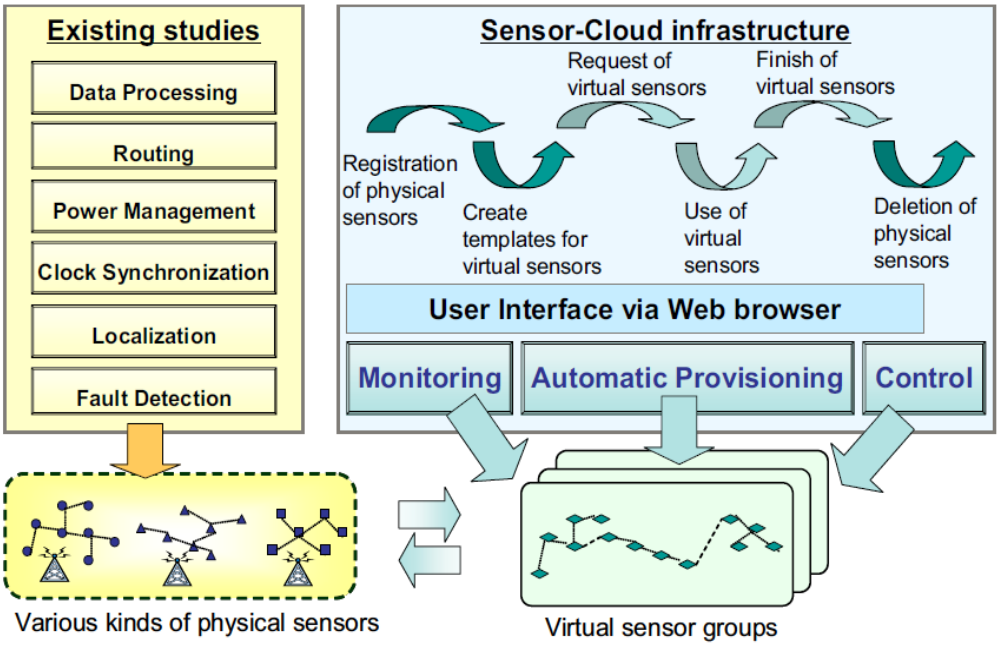


Figure (7) Sensor Virtualization Proposed Architecture [3]

3.1.2.2 Virtual Cloud Sensor

Sanjay Madria et al [20] proposed a new architecture for building a virtual sensor on top of a physical one. They discuss many components of this design. The architectures form an intermediate layer between a sensor device in the real world and consumers. The designed architecture includes three layers: a sensor-centric layer to deal with physical sensors; a middleware layer, an intermediate layer; and a client-centric layer to handle applications. In this design, it is not clearly shown how these layers can build a standard virtual sensor template on top of the physical one so as to handle different sensor types. These came from different vendors and work using diverse technology. Figure (8) shows the proposed design architecture.

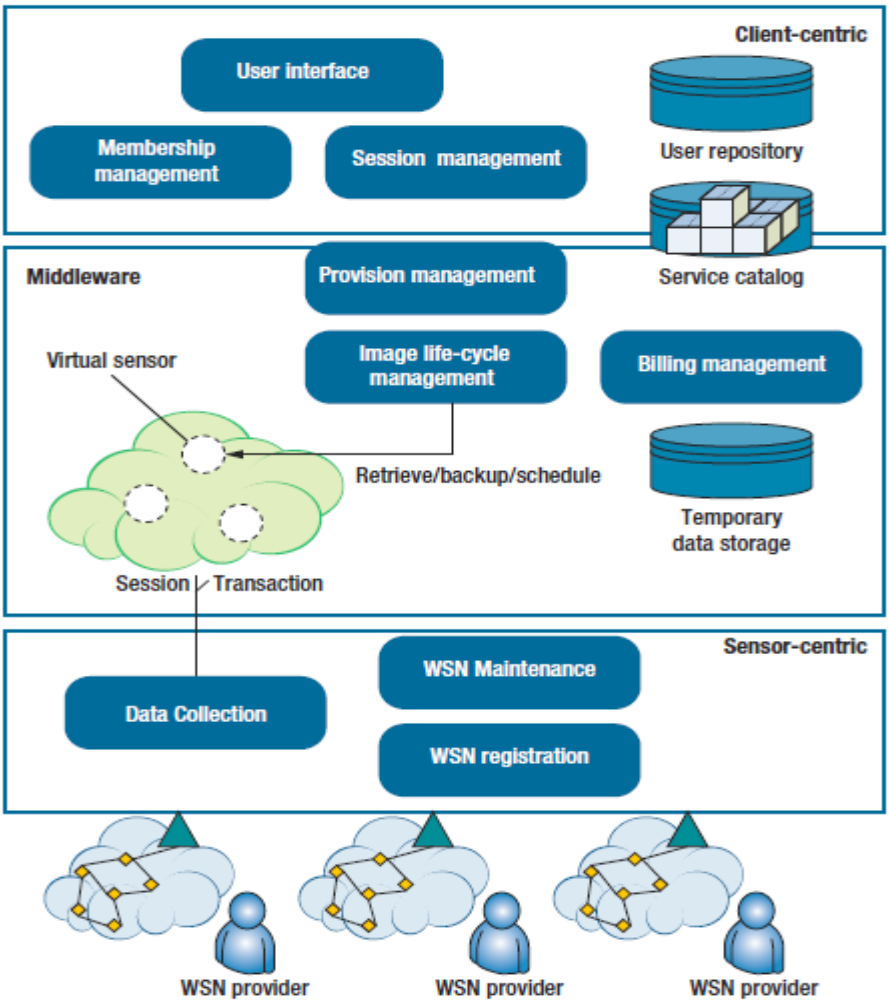


Figure (8) Sensor Cloud Proposed Architecture [20]

3.1.2.3 Cloud for Sensing

Maria Fazio and Antonio Puliafito [57] proposed a new sensor control architecture the main objective of which is to control and manage sensor recourses in the context of cloud computing and to provide sensors as a service. This project considers the use of available sensor standards to enable this feature in a sensor device, such as OGC-SWE specifications, a things that distinguishes this project was, providing the sensor as services in terms of the data-centric model (consumers have the ability to know the data has been measured and processed) and the device-centric model (consumers have the ability to customized a virtual sensor build on top of the physical one), while most of the architectures in the sensor cloud provide only a device-centric model. Figure (9) shows cloud for sensing architecture.

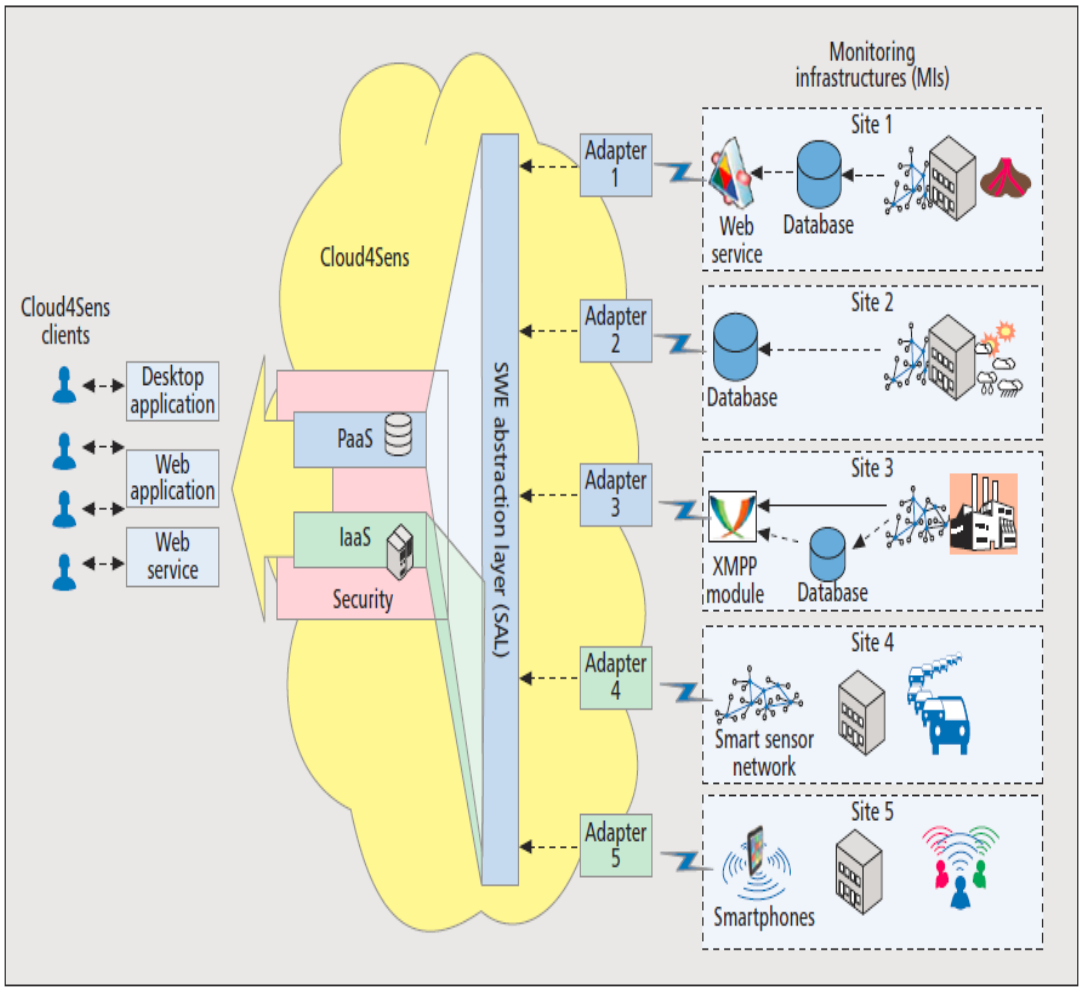


Figure (9) Cloud for Sensing Architecture [57]

3.1.3 The Web of Things Paradigm

The Web of Things paradigm is an active research area that practices a World Wide Web (WWW) podium and its related technologies as based on the structure to extend the concept of the Internet of Things. Many studies have been carried out to support this paradigm.

3.1.3.1 Web of Things Framework

Federica Paganelli et al [58] proposed a structure model dedicated to developers. This model allowed developers to demonstrate things in the real world and modeled them to smart things by using web resources. The model essentially was built by linking the relations between aggregation and reference. Basically this model has three components, the first being a general-purpose layer that is concerned with web resources, while the middleware layer attempts to implement these services through open standards. The third component is a set of tools for developers to allow them to represent physical things as virtual things. The main benefit of this project was a numerical representation of physical sensors, approaches to interlinked between object/things and the Web, and publishing new objects represented as web services. On the other hand, this project did not show how to interact with adaptive components in the context of the Web of Things. Figure (10) shows the proposed architecture.

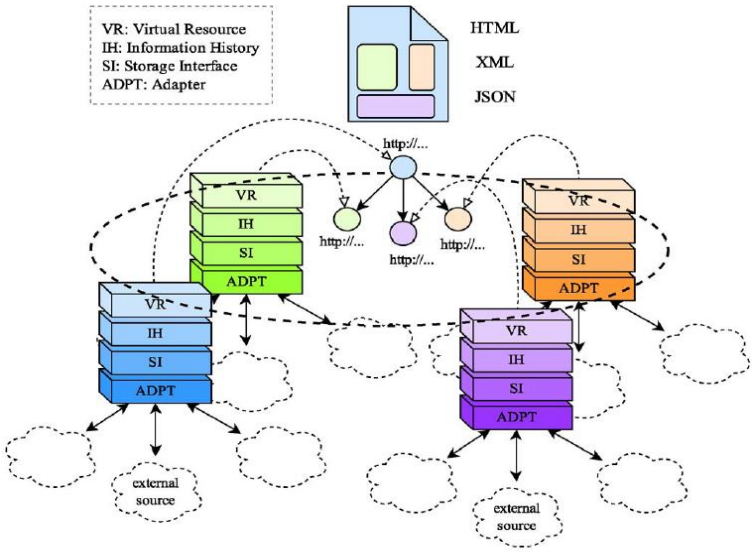


Figure (10) WoT Proposed Architecture [58]

3.1.3.2 The Virtual Environment of Things

Jih-Wei et al [59] introduced a new paradigm called "*The Virtual Environment of Things (VEoT).*" This paradigm aims to assimilate smart things in the real world with a virtual environment in the context of the Web of Things. In this project, they confirm the effectiveness of the model by designing a smart gateway and a core resource exchange. This core included a resource manager, an event manager and a smart object manager. The proposed model shows how the objects/things interacting with each other use real-time applications in the Web of Things environment. This project lacks standardization in the proposed design and they focused on software technologies instead of creating applications to serve the Web of Things.

3.1.3.3 Social web of Things

Hoon-Ki Lee, et al [60] proposed a new paradigm that enables the concept of a Social Web of Things (SoT). This paradigm is based on machine to machine talking in context of the Web of Things. They implemented a social sensor network and enabled the information associations in the context of web and social networks. The main component of this model included the service domain, social relationships, and user information. The main objective benefit of this model was finding a relationship between users, things and social networks and providing a dynamic service that has the ability to be reconfigured according user needs and activities in social networks around the world. Figure (11) shows SoT architecture. On the other hand, no security or privacy issues were discussed as a consequence of this wide sharing of information related to sensitive data, such as sensor networks.

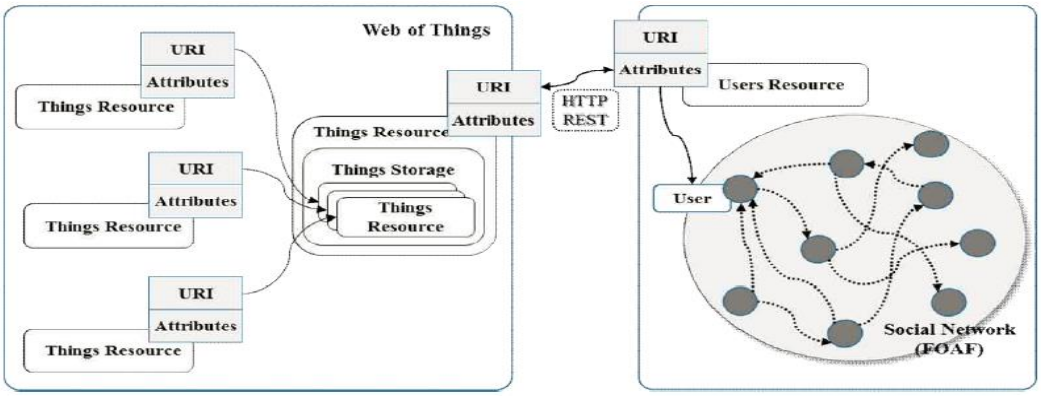


Figure (11) SoT Structure [60]

3.2 Security and Privacy Requirements

Security and Privacy requirements in sensor networks are many-faceted in wireless sensor networks and normal networks. In the context of the Internet of Things, Sensor Cloud and Web of Things, this section provides a brief discussion of these requirements.

3.2.1 Data Confidentiality

Confidentiality means the capability of hiding messages to protect data from a potential attacker. Confidentiality is considered to be a significant subject in network security. A sensor security designer should focus on addressing these tricky issues. Confidentiality in the context of sensor networks can be related to the following:

- The designer should establish an encrypted channel.
- No leakage to sensors neighborhoods
- Data encryption and multimedia security mechanisms should be applied.

3.2.2 Availability

It is of great value to security when we have a mechanism to confirm whether network resources, nodes and communication links are available and ready to forward a packet.

3.2.3 Data Freshness

Because of the nature of the data sent by the sensors, designers need to be certain about the data freshness, especially in real-time applications. Data freshness proposes that data be fresh and guarantees that no new message data has been repeated or replayed. This mechanism important when a shared-key technique is used and needs to be changed in a timely manner.

3.2.4 Data Integrity and Authentication

Integrity means the ability to guarantee that network packets have not been modified while they travel through the network. An attacker may completely change data packets, control the packet stream or even attempt to inject additional information into the packets and resend them.
Security administrators/designers need to secure this process and verification such that a stream of packets has been certainly sent by the r dispatcher. Authentication symmetric mechanisms and embedded security information in the packet header may help in these cases.

3.2.5 Time Synchronization

In business sensor network applications, each sensor has its own clock, timer and external or internal sources for time synchronization, which are essential to recognize the relations among measured phenomena in the real world. Moreover, time synchronization can increase the use of redundant data and give measured data a time stamp, which helps sensor applications to analyze these data in a more advanced manner. Time synchronization in wireless sensor networks faces many issues, including the large scale of nodes and the need for robustness.

3.2.6 Self-Management

Wireless sensor networks basically operate in an ad-hoc network topology and should be prepared to work in remote areas and in different environmental situations with a minimum possibility of technical support, maintenance and re-configuration. Consequently, sensor network nodes need a self-management capability. These nodes should be adapted to the reform of failures, environmental changes and interaction with other nodes without the need for human involvement.

3.2.7 Secure Localization

Sensor nodes in the real world usually deal with natural phenomena such as temperature, light, soil, water, wind, etc., and monitor the relationships among these elements and other objects, measurements and events in the real world. These items of information are vital components in sensor networks. Without expressive sensor node locations, this information drives only a portion of the story.

3.3 Research challenges

The Internet of Things, the Sensor Cloud and the Web of Things paradigm currently reflect a new revolution in ICT business and centrally this will improve your lifestyle. To reach this point, many challenging issues should be addressed, some of which are briefly discussed below.

3.3.1 Big Data

The Internet of things and Big Data are two different faces on the same coin. The Internet of Things has been designed to gather data from a huge number of objects and this number is rapidly increasing on a daily basis. Dealing with this amount of data, the cost of storage in addition to managing and extracting useful information from this Big Data is a great challenge in the Internet of Things.

3.3.2 Lack of Standardization

Sensor nodes, objects or any other devices that can be connected to Internet of Things platforms build from numerous vendors and use varying technology, protocols, services and different topologies. As a result of this diversity, bringing all these things to work in the same standardization will not be an easy task.

3.3.3 Identity Management

Billions of things are planned to be linked in the context of Internet of Things platforms as discussed previously. These objects should serve to meet the needs of numerous applications. As a result, identity management for these objects takes place as a valuable issue. In this regard, using the IPv6 protocol may be part of the solution to this challenge.

3.3.4 Connectivity Robustness

In the Internet of things, objects, nodes and human connectivity and ensuring this connectivity of links are a vast challenge. Currently, a new project gives us hope. This project was founded by Facebook, a giant leader in social networking sites. The project, namely “internet.org”, aims to provide Internet access to everyone around the globe free of charge. This expansion is the vision of the Internet of Things.

3.3.5 Security and Privacy

Things in context of the Internet of Things have sensitive data, private style, multiple dimension nature, are scattered in different locations, belong to diverse network types and use different communication standards. As a result of the above, providing a security mechanism and ensuring consumers’ privacy are complex and compound challenges in the Internet of Things.

CHAPTER 4

DESIGN AND IMPLEMENTATION

4.1 Web-based Internet of Things (Web IoT)

In contrast to the Internet of Things and the Sensor Cloud, we proposed a secure and scalable Web-based Internet of Things architecture called Web IoT. This architecture can be considered a system integrated model of interconnected sensors, smart devices, social networks, objects, actuators or things. Furthermore, it can provide support for machine-to-machine collaboration from network-enabled devices to network-enabled lives. Moreover, it can be used to serve the Internet of Everything (Io-E) and the Social Web of Things in the future. In this section, we will overview and discuss a conceptual model for our proposed design.

4.1.1 Proposed Reference Architecture

The proposed reference architecture model of our Web IoT consists typically of four layers that operate in different network zones: the Application Layer, the Middleware layer, the Network Layer and the Physical layer. Each layer has a specific role and serves other layers in the system model. A cloud service structure model was used to distribute the facilities of shared services in which consumers take advantage of accessing our system from anywhere by using these services. Moreover, end users will not be worried about detailed implementation of this service. Our proposed design provides a high level of transparency and scalability. Web IoT layers can be classified in the following descriptions. Figure (12) shows Web IoT abstract layer architecture.

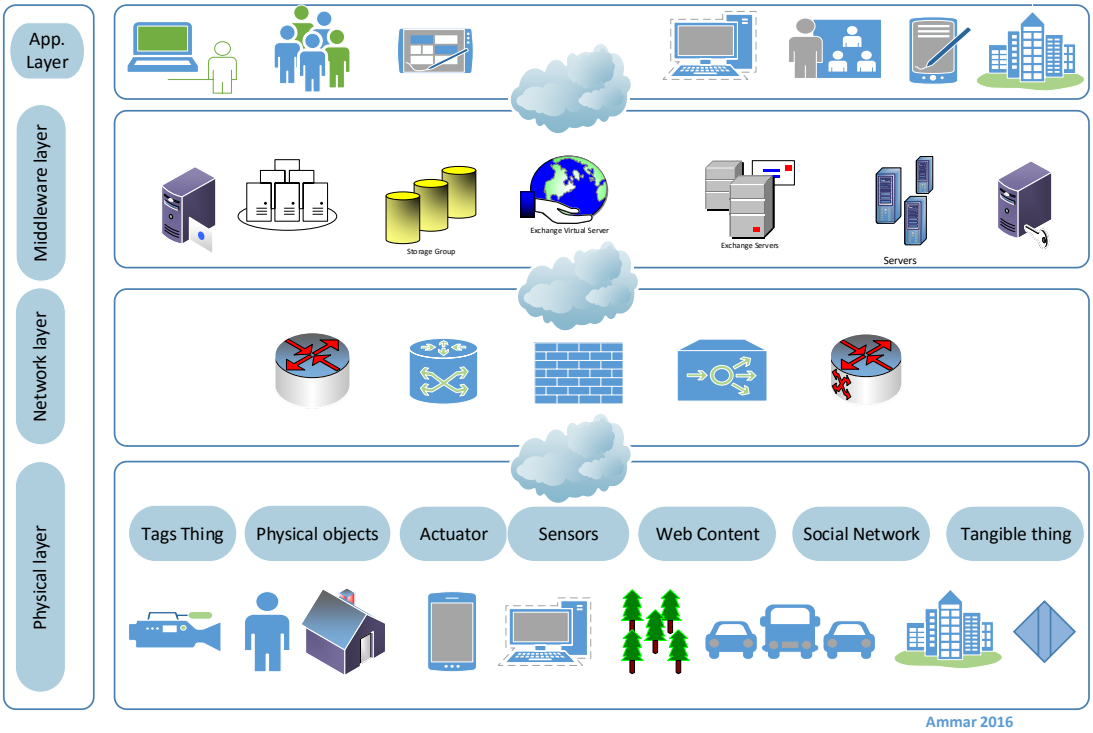


Figure (12) Web IoT Abstract layer Architecture

4.1.1.1 Application Layer

This layer is a highest layer in our proposed design and corresponds to the end users and their viable requests with the fact that we have numerous consumers needing to stay connected with valued collected data from different kinds of environment using different types of applications. This gives us an idea of why we need this layer. The main functions of this layer include being a stand-in as the stakeholders' entry point, allowing end users to set up their look and feel of their web site and providing them many tools to set up any kind of web content such as blogs, forms, personal information, schedule tasks, calendars, etc. Moreover, it can provide other requirements to consumers such as creating a public or private web site and sharing their own content with others' web sites and social media. The output from this layer can also serve out-of-the-box applications such as Data Mining, decision maker applications and other science and research fields.

4.1.1.2 Middleware Layer

The middleware layer is an abstraction of the physical world to the ICT world. It is the more important layer in our proposed design and cannot be accessed directly by stockholders or end users. However, it will serve them over the concept of request and response of up-down layer operations. The main functions of this layer are abstracting physical objects to be Web-accessible objects, managing the operations of virtual instances, managing the customer Service Level Agreement (SLA) and providing scalable web applications for data exploration that can be used by stockholders or end users to visualize their data in real-time. This layer communicates with a wide range of things and attempts to place them into one classified group. In addition, the layer allows these things to be managed remotely without concern for the real physical object or location thereof. Our reference model for this layer consists of portal servers with failover and load balancing considerations, application servers with failover and load balancing considerations, database servers with clustering database functionality, storage devices with clustering functionality, backup devices, an authentication server, a monitor server and a mail server, Figure (13) shows the Middleware Layer Reference Architecture.

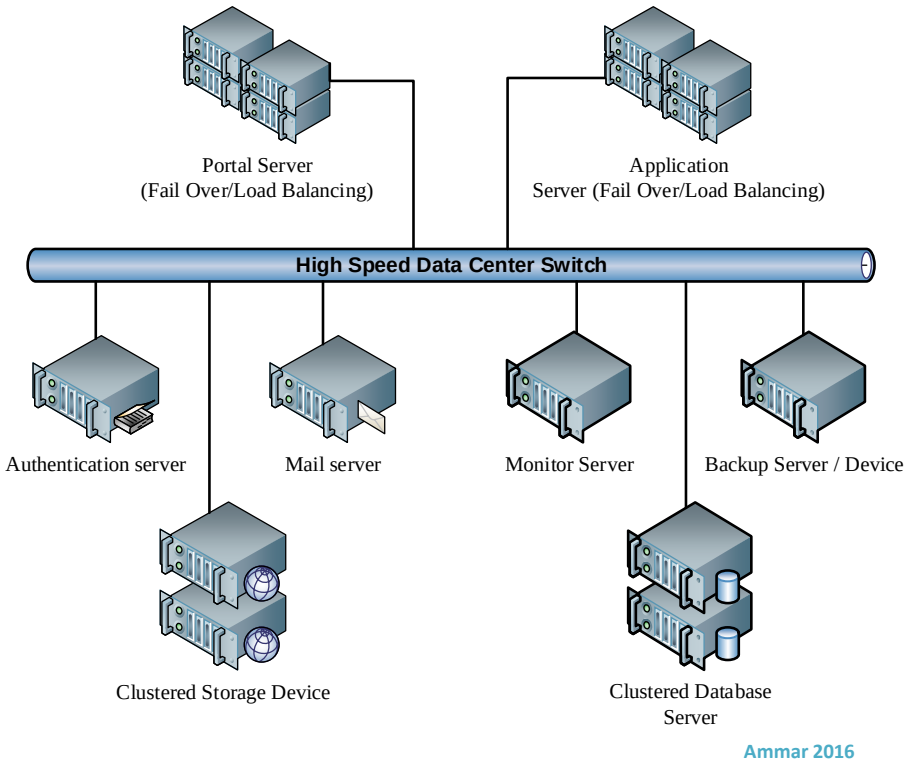


Figure (13) Web IoT Middleware Layer Reference Architecture

4.1.1.3 Network Layer

This layer is responsible for network functionality and the communication line. The main functions of this layer are identification of all things through the Internet by using IPv6 and/or IPv4 providing a heterogeneous communication infrastructure, securing the network communication line and data to allow the secure connection of billions of things around the world. In our reference model, we suggested three types of network zone: Internal, External, and DMZ zones. The Internal zone, which includes our Application servers, Authentication server, Storage devices, Database servers, Mail server, Backup Devices and Monitor Server, can be accessed only from the DMZ zone and blocked from direct access from the External zone. The External zone, which includes users, services, network devices and communication lines from outside the boundary of our network (including third-party servers and services such as third party mail systems, physical or virtual sensors, social networks, Google App., etc.) or any other ICT equipment, has the ability to access our DMZ zone only. Figure (14) shows the Network Zone Layers in our proposed design.

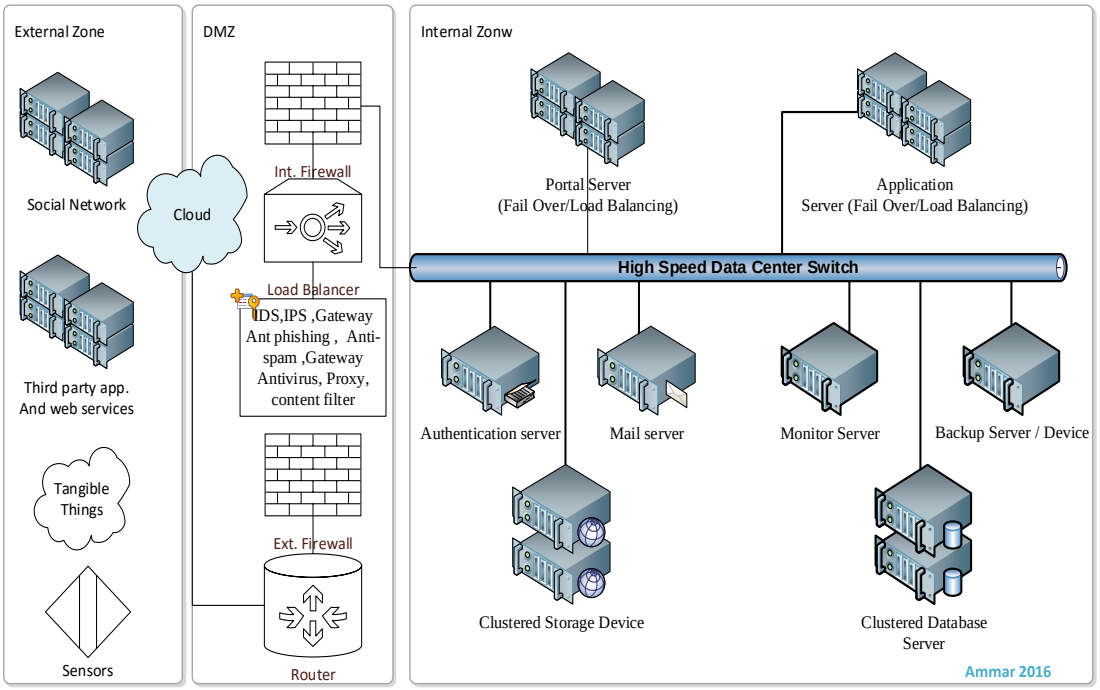


Figure (14) Web IoT Net Work Zone Layers

The DMZ zone consists of a two-sided and an in-between server and services. The external side of the DMZ zone includes a router, firewall, an Intrusion Detection System (IDS), an Intrusion Prevention System (IPS), a Gateway anti-phishing server, Mail Anti-spam and Gateway Antivirus, which provides the first level our defense, while the internal side of the DMZ zone includes a second firewall and load balancer, which provides a second level of defense. Between these two sides, we place a Web proxy, a web server, a content filter and VPN servers. The DMZ plays the role of interconnecting both the Internal and External zones with restricted roles to enhance our security policy.

4.1.1.4 Physical Layer

This layer is responsible for physical objects, sensing devices, actuating resources and any other things that can be part of the communication line. This layer contracts with the preparation of the service template construction and provision standard definition in addition to defining the physical object as XML, a web service or a web-enabled device. This layer allows consumers to access physical objects and develop them on several platforms without concern for the integration with a number of application platforms.

4.2 Experiment Workbench

Our experiment lab included three main parts: the components and the backend and frontend implementations. First, we will explain the lab components and the interconnection in backend and frontend. The main goal of the lab tests was to discuss the scalability, performance and security of our referenced model. We reduced the number of servers required in order to optimize the use of available resources in our lab.

4.2.1 Lab Components

The references model has many components, such as application servers, an authentication server, storage devices, database servers, a router, a firewall, an IDS, an IPS system, etc., Moreover, we may need more than one application server, database server, storage devices and a firewall to achieve high availability and security in order to implement all these servers in a real test environment. We need at least eight physical servers or two high-level servers with virtualization capability along with other ICT resources. In our workbench, we emulated the references model to the minimum required recourse to build applications that are based on an open source platform so as to demonstrate a smart and secure Web IoT. The emulated test system was built in a multi Linux environment system and run on Oracle VM Virtual Box. The test system included four main virtual machines, Universal Thread Management (UTM), Applications server, a storage device, and Host machines (also acting as clients), Figure (15) shows the Test Lab Components.

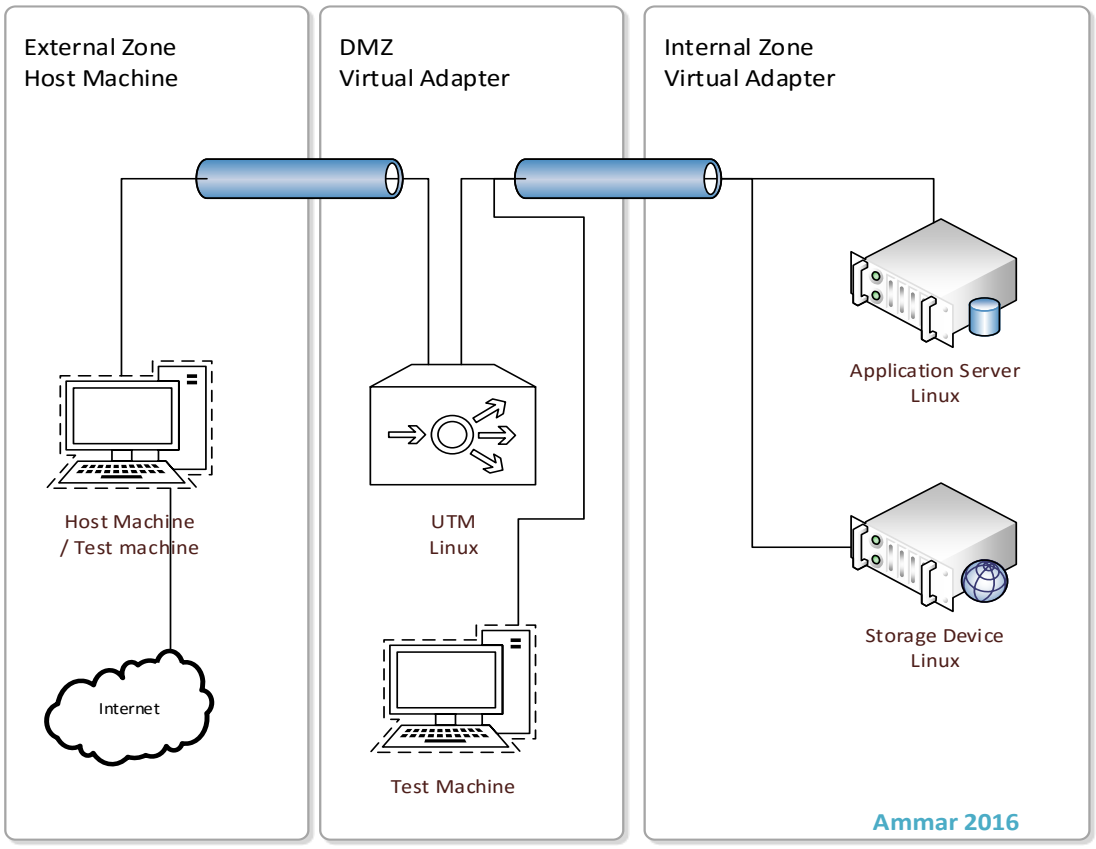


Figure (15) Test Lab Components

4.2.2 Lab Environment

In our lab, we built an optimal emulation system for our reference model by using the following devices and environment: Universal thread management was deployed on a virtual machine instance running a 64-bit Red Hat Linux-based system UTM Community Edition, 2 GB of memory, a dual-core CPU with a total of 4 CPUs and 20 GB of storage with moderate I/O performance, while the application server was deployed on a virtual machine instance running 64-bit Linux Ubuntu 14.04 LTS, Portal Server Community Edition, 4 GB of memory, a dual-core CPU with a total of 4 CPUs and 20 GB of storage with moderate I/O performance. The storage devices were deployed on a virtual machine instance running 64-bit Linux Ubuntu 14.04 LTS, Cloud Storage Community Edition, 2 GB of memory, a dual-core CPU with a total of 4 CPUs and 20 GB of storage with moderate I/O performance. The test database was MySQL version 5.1.73. The sensor that was used was from Ptolemy II simulation version 10.0.

4.2.3 Backend Implementation

Through the conception above, we deployed three virtual machines in a Linux environment, two of these were Ubuntu Linux, and the other Red Hat Linux. Java Runtime Environment (JRE) was installed on the host operating system to support the Java Virtual Machine (JVM). Apache Tomcat was also installed. This was required to contain the portal server instance. The server delivered the connectivity and inter-operability by using the Enterprise Service Bus. A Model Driven Development approach was used to deploy the services. Administration tools were provided by the server, which was used for integration and support for every module. Administration included wizards, runtime configuration parameters, service providers, a web site builder and listeners to tug our application server in runtime mode. Network configuration and server integration were deployed in each individual server in our lab to put them online in both the Internal and DMZ zones. Dynamically generated portlets (plug-in) were used as a bridge to the end users as well as to enhance system integration.

4.2.4 Frontend Implementation

The implementation of the frontend is such that it is placed on top of our model and connected with the interface available to all consumers. It should be available from the external zone. We provided a scalable web interface for the end user that offers a wide range of facilities such as Single Sign-On (SSO), Portlet Management, Content Management, Web Content Management, Document Management and Site Management. All of these features are protected by our security model and allow all end users with the appropriate permission to be part of our DMZ zone, and can be involved in building a personal public and private site more effectively. This may include attaching their own things to these sites, collaboration, personalization, social networking, virtualization, personal storage quota management, and integrating dynamic web content in addition to many other things.

4.2.5 Overall Workbench Structure

In the previous sections, we covered the lab component and the back and front end implementations to come out with the substance of this workbench for all of these components that are linked together, Figure (16) shows Overall Workbench Structure.

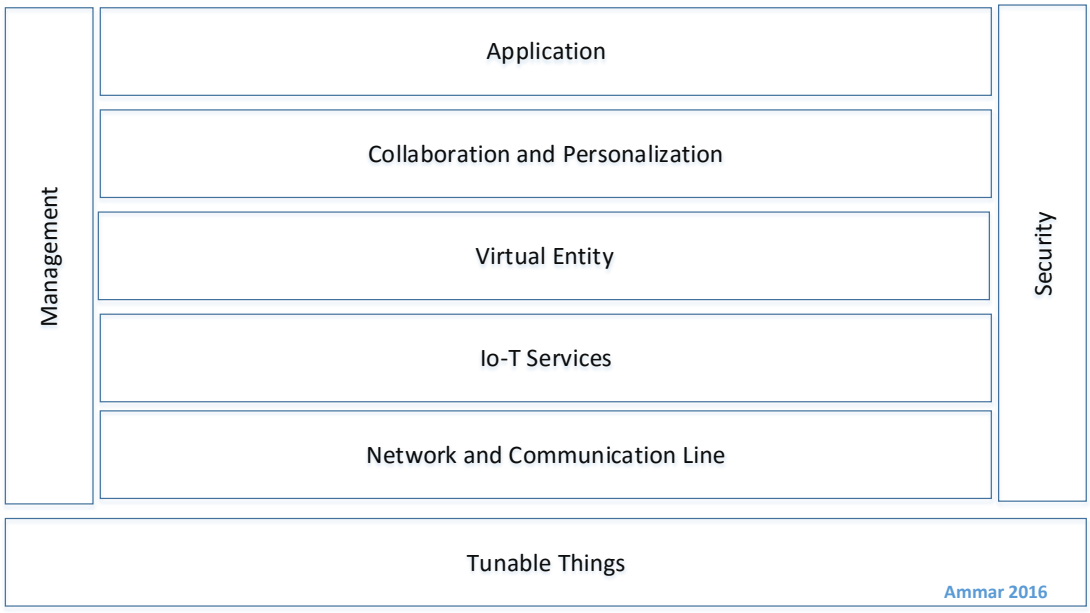


Figure (16) Web IoT Overall Workbench Structure

CHAPTER 5

RESULTS AND DISCUSSION

5.1 Web IoT Features

Our Web IoT model provides a scalable web application to visualize data that have been collected by IoT devices in a closely real-time manner. The mechanism of work can be as follows: IoT devices, or things, can be deployed anywhere; these devices collect data such as sensing data (such as movement, humidity, pressure, temperature, etc.) or multimedia data such as video, audio, and images; or it can collect any type of web content or data from third-party applications or data repositories. Our Web IoT design provides end users with the ability to manage and control data collected in a visual manner from a single point. Moreover, it provides corresponding dynamic data updates for live notification. Additionally, our design can be extended to integrate with third-party applications such as Google App., social networks, etc. The main features of our proposed design will be demonstrated in the following sections.

5.1.1 Web Content Management

Our Web IoT includes a web Content Management System (CMS) that allows end users to create rich web content by using this facility. End users will be able to create websites, public and private web pages. Furthermore, they will be able to use predefined templates that are included in our application. Additionally, they will be able to control the schedule time for publishing, use Portlet (Plug-In) inside a web page and give permission to specific users, groups or organizations. Moreover, a new feature called an asset publisher was added to our application.

This feature allows end-users to add any web content from other resources and display it within the user's webpages in one place. Finally, it offers Office integration, activity tracking, and abuse reporting and dynamic data listing.

Figures 17, 18 and 19 show our Web IoT Interface.

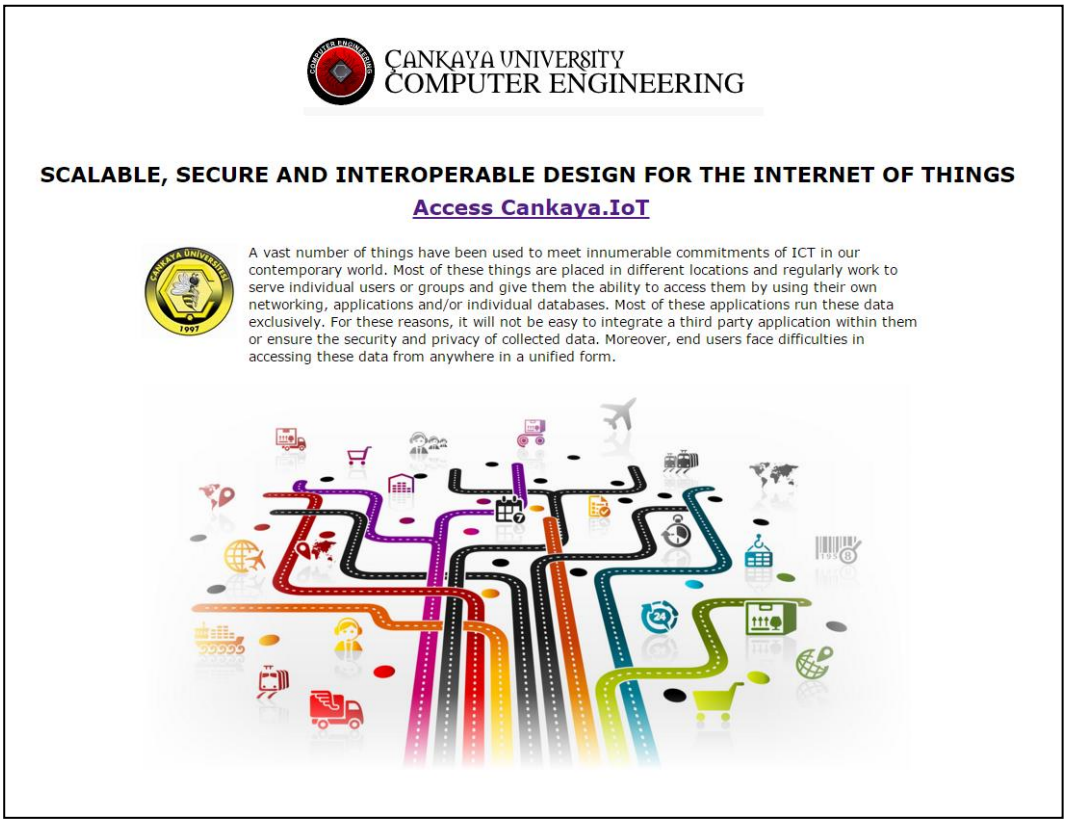


Figure (17) Web IoT Main Page

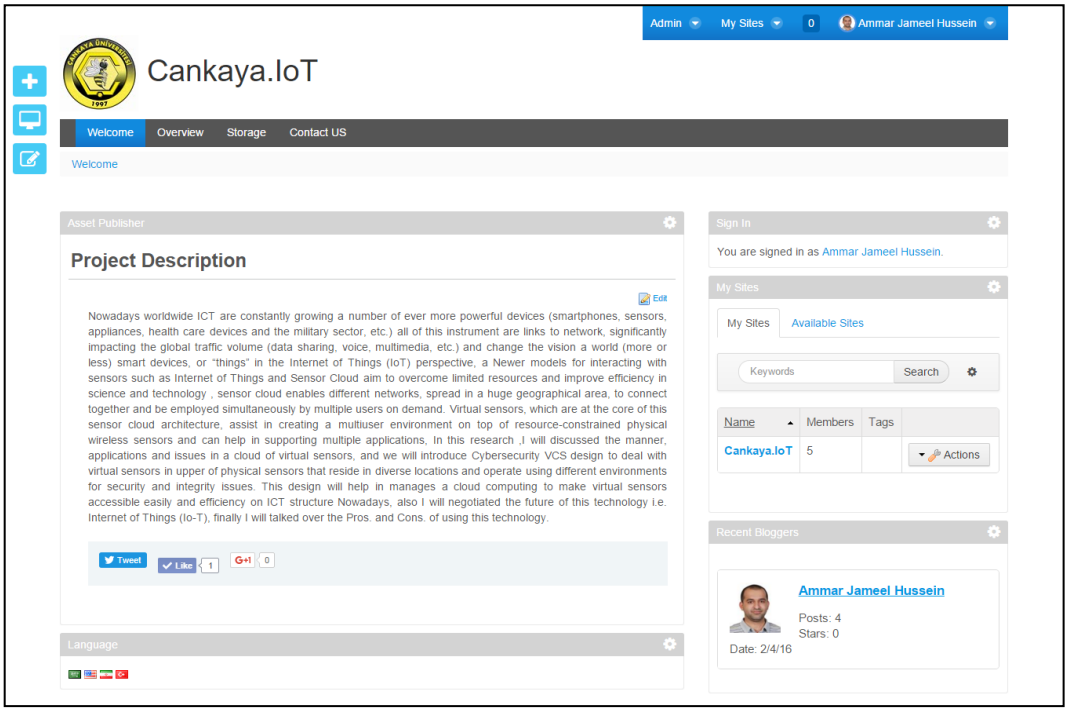


Figure (18) Web IoT Welcome Page

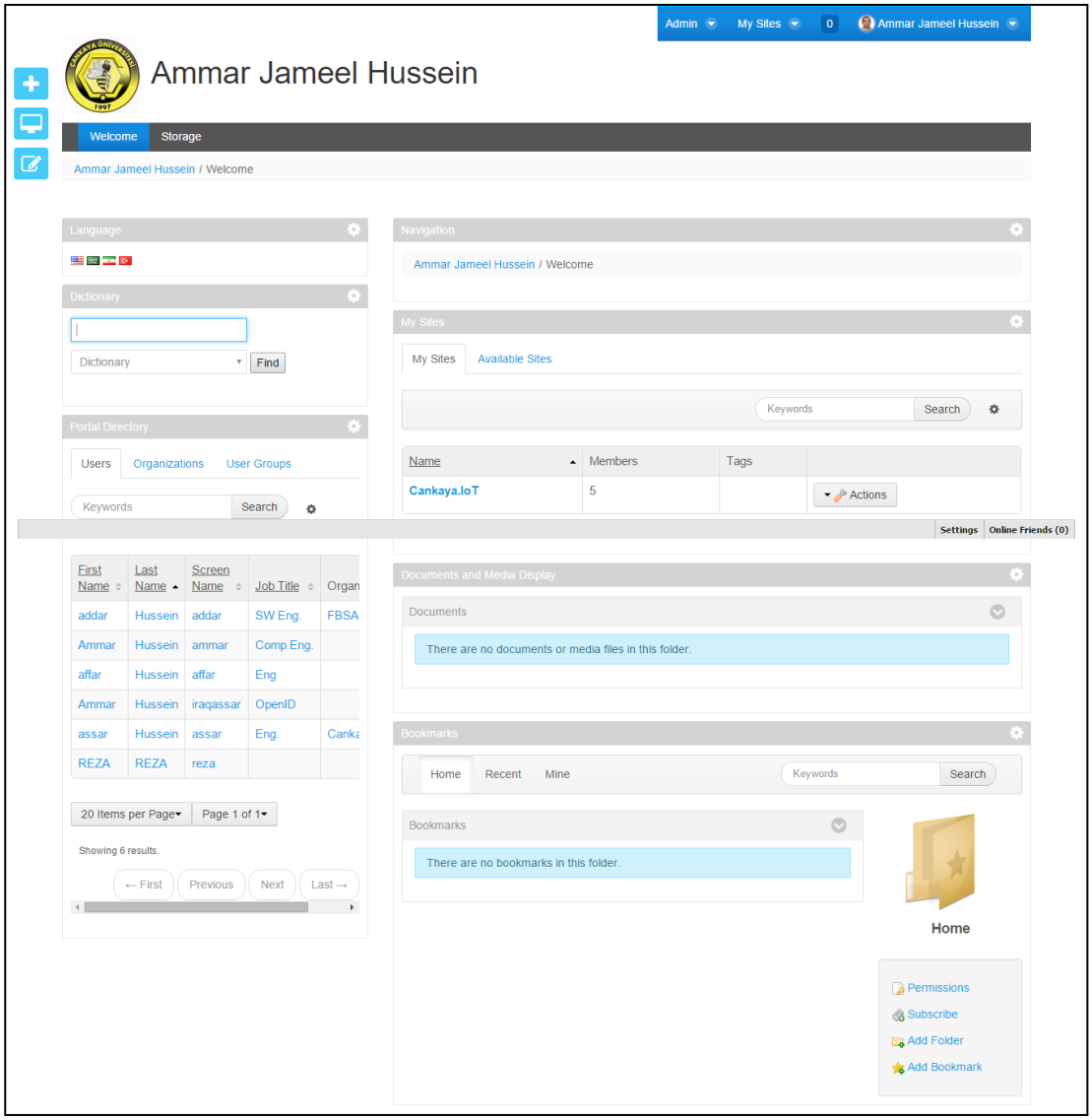


Figure (19) Web IoT Admin Page

5.1.2 Flexibility

Our Web IoT provides powerful collaboration tools in one single package along with the ability to manage and control roles, permissions, and policy development in addition to the flexible management of resources, flexible management of users and groups and pages. Moreover, it supports Social/Web 2.0 features, which include, but are not limited to, Tagging, Comments, Ratings, Blogs, Message Boards, Shared Calendars and Web-Mail. Furthermore, our design is a risk-free, open source license which can be operated in a flexible ICT infrastructure to reduce the Total Cost of Ownership (TOC) of customization and integration. Figures 20, 21 and 22 show Some Web IoT User Homepages.

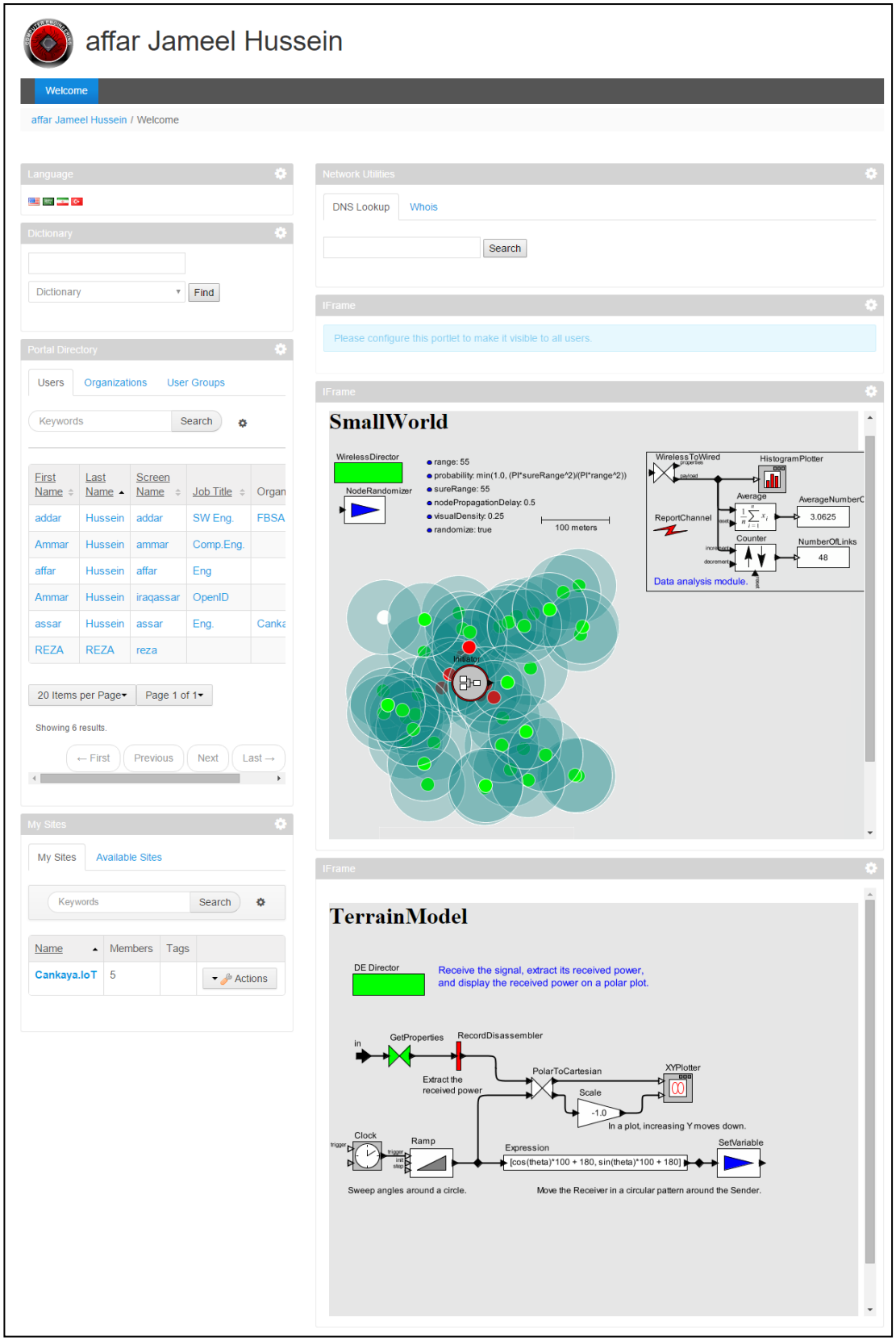


Figure (20) Web IoT User 1 Home Page

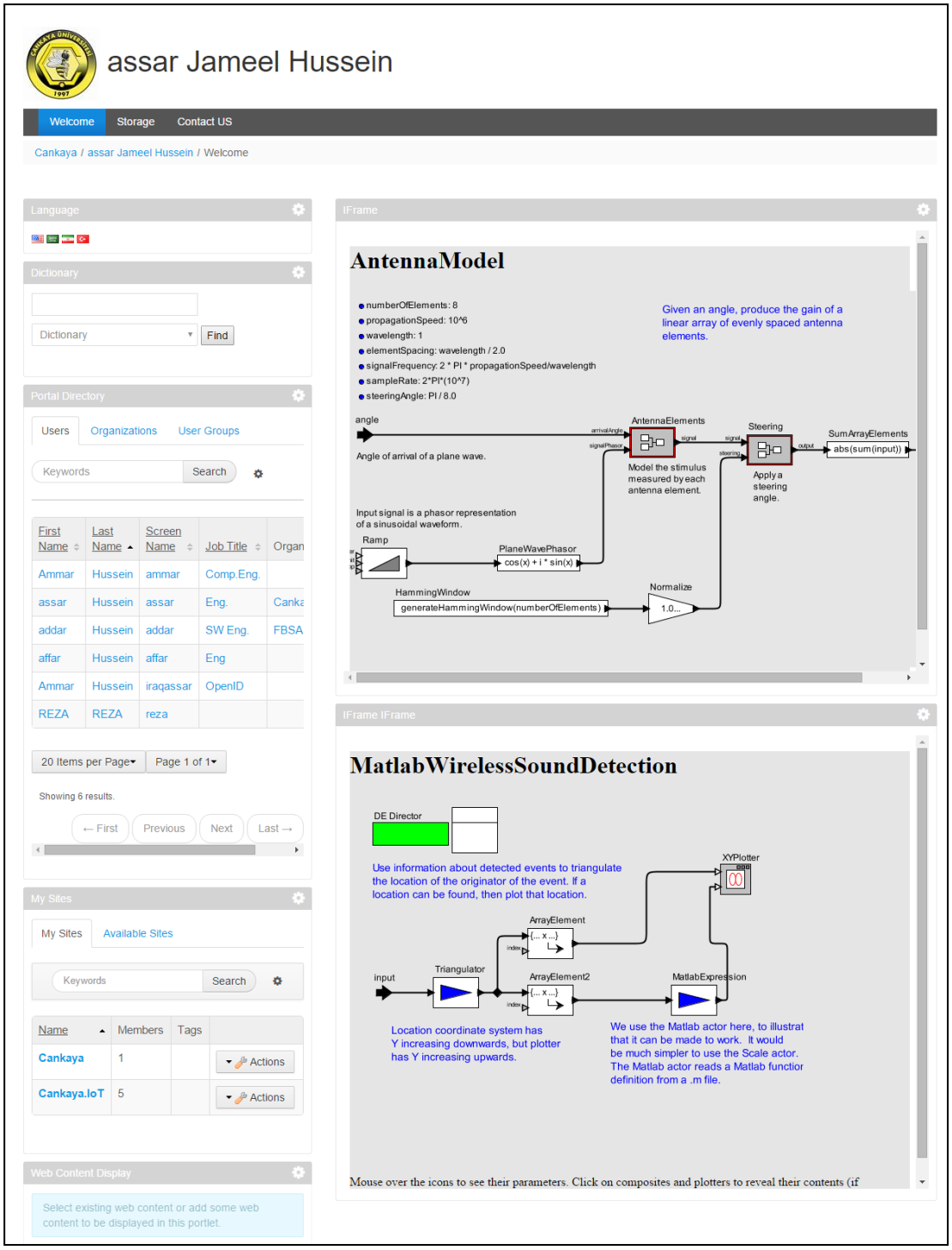


Figure (21) Web IoT User 2 Home Page

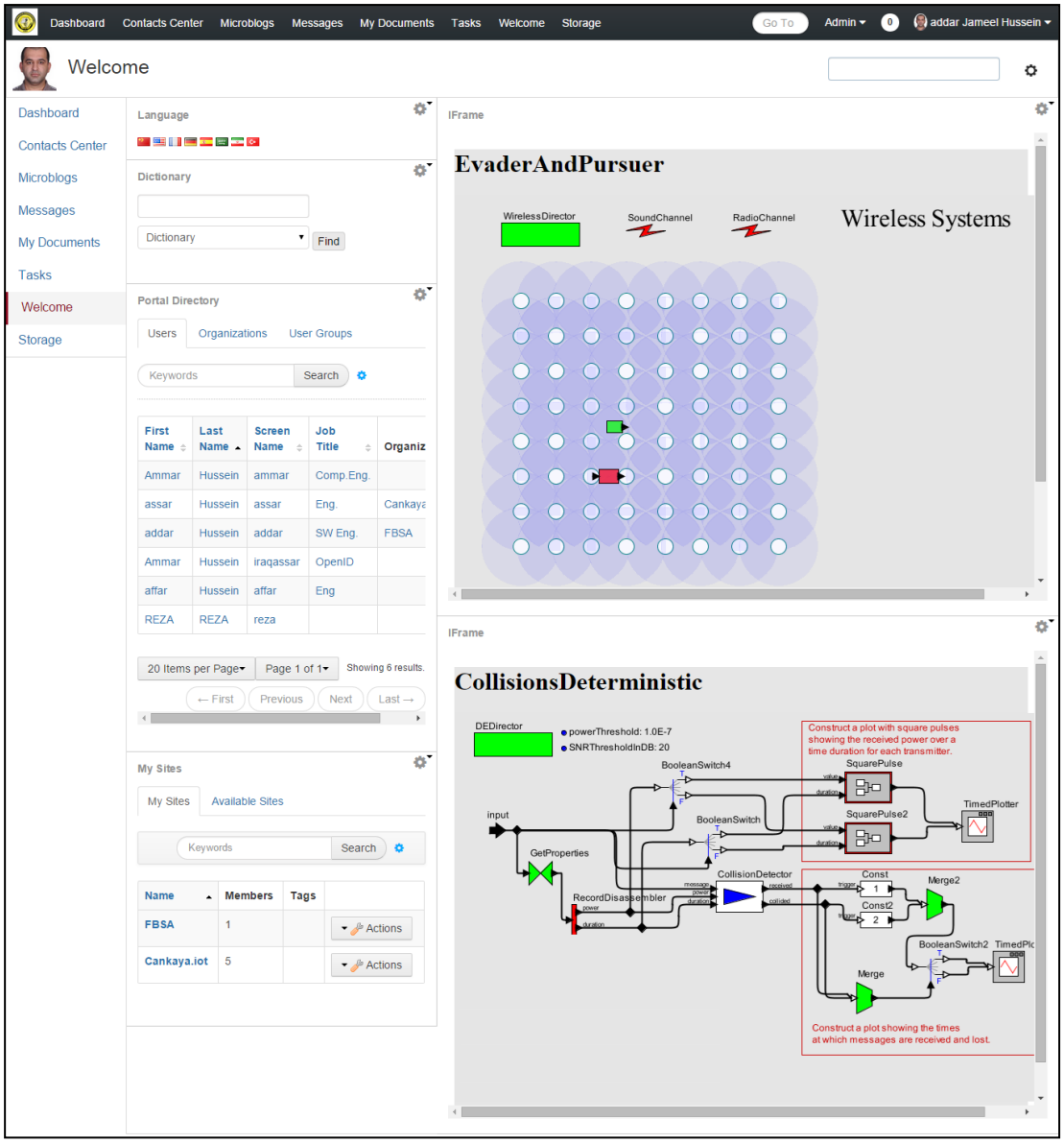


Figure (22) Web IoT User 3 Home Page

5.1.3 Scalability

Our Web IoT has a scalable web interface that allows developers, stakeholders and authorized users to have control over their own entire website, including the look and feel, styling and layout. Additionally, they can use out-of-the-box tools and external plugins to take advantage of more facilities such as layout template plugins, web plugins, Portlet plugins and theme plugins. Moreover, it supports web services by using built-in Service Oriented Architecture (SOA), which includes HTTP, JSON and SOAP. It also can be integrated with Java ME and Java SE.

Additionally, our application offers many drag-and-drop Portlets and a scalable configuration wizard for live Page Editing. All these tools can be flexibly extended and updated. Figure 23 shows Web IoT available tools.

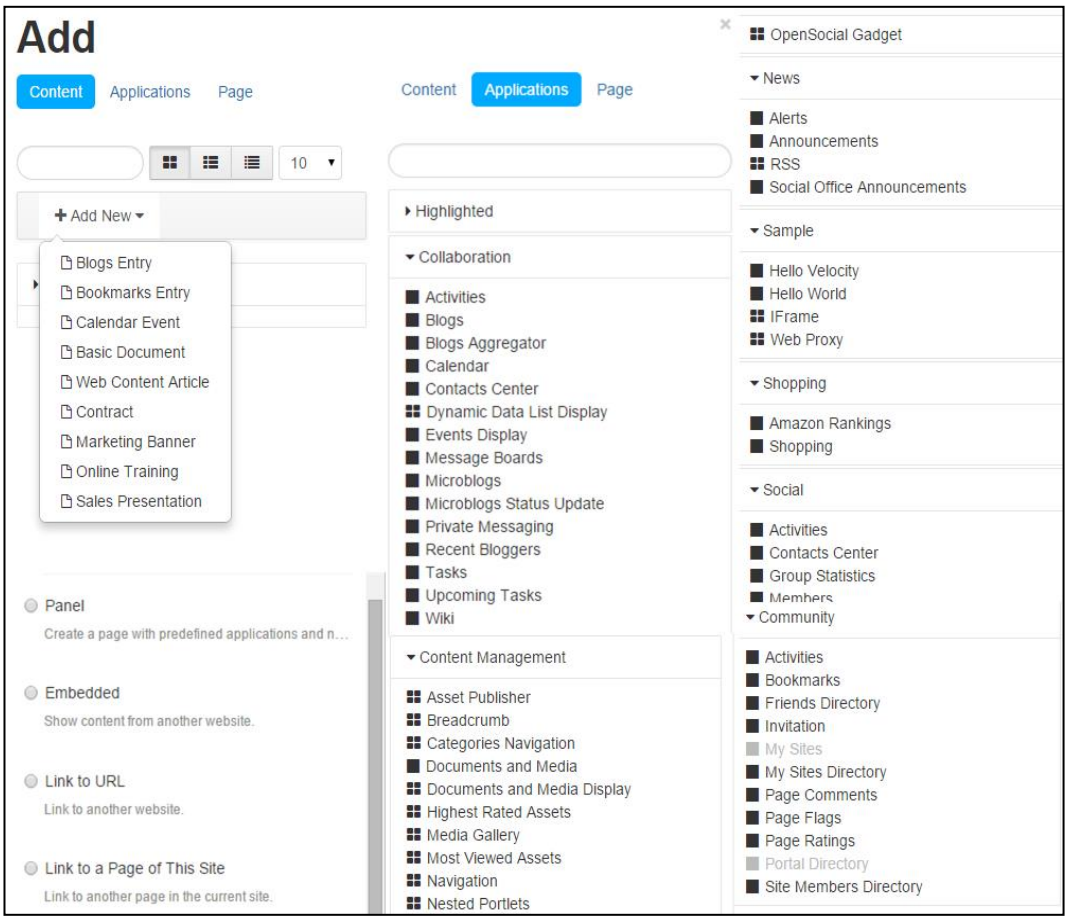


Figure (23) Web IoT Available Tools

5.1.4 Reliability

High availability was considered in our referenced model by using clustering data base servers with the capability of handling failover, load distribution, and load balancing. In addition, we used two application servers, two portal servers and backup storage with consideration given to a backup communication line and multi security level so as to increase reliability, achieve high rating throughput traffic, and a reduction of the responses latency under multiple operational conditions. High availability will insure high performance of our suggested model; however, it will affect also the total cost of ownership.

5.1.5 Security and Privacy

To enhance the security and privacy of our design, three different network zones had been deployed to isolate our design components, namely Internal, External and DMZ zones. A comprehensive security model, a number of techniques and mechanisms were deployed to achieve the security objective of our design and to secure the communications line. This included, but was not limited to, the following: a Multi-layer firewall, an Intrusion Detection and Prevention system, Getaway Antivirus, Anti-spam, Gateway Anti-phishing, Virtual Private Networking (to encrypt communication lines), Content filters, a web proxy and Secure SSO. Figure 24 shows our UTM dashboard.

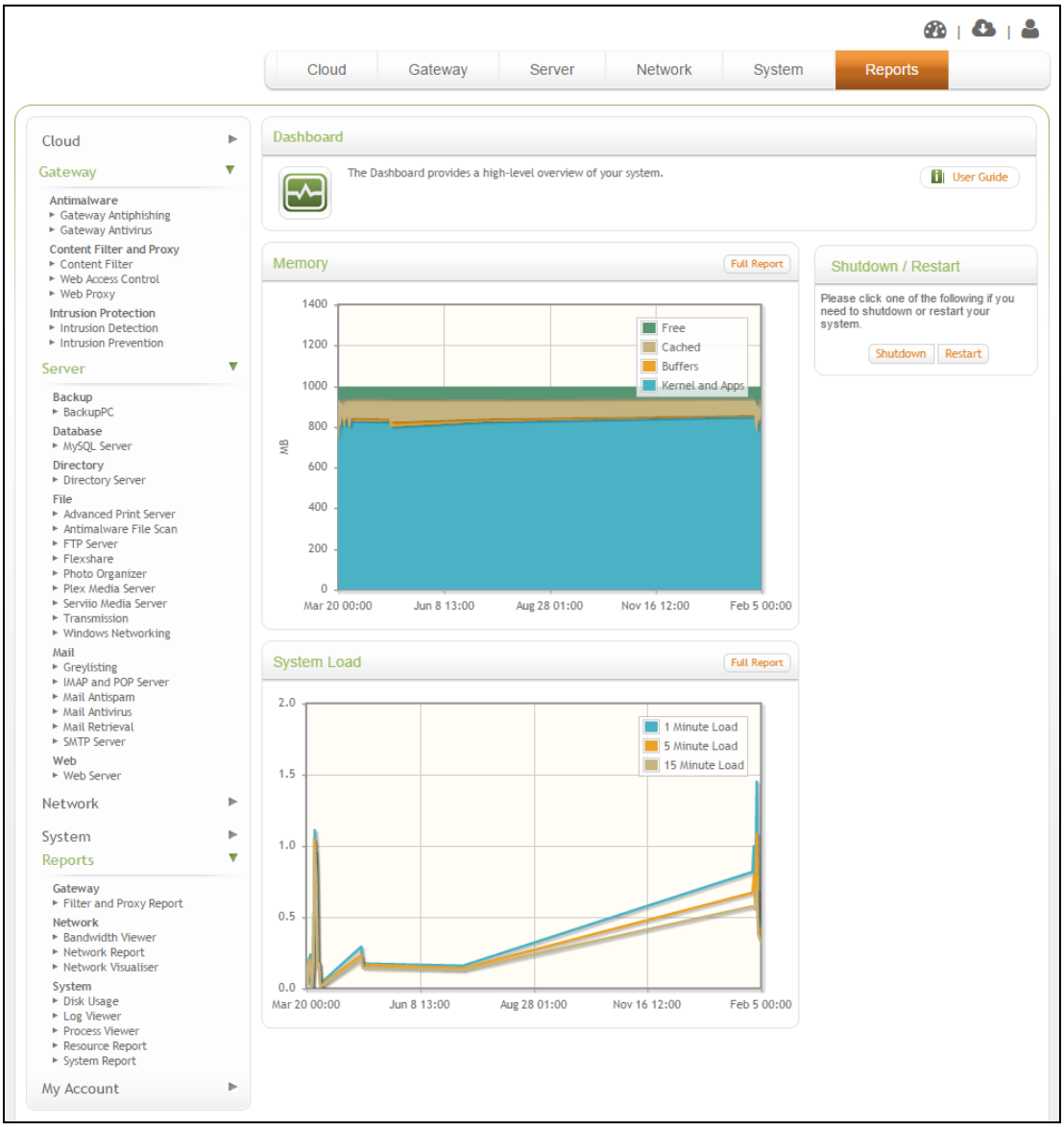


Figure (24) Web IoT UTM Dashboard

5.1.6 Documents and Media Repository

The Web IoT includes a document repository that can host a wide variety of videos, documents, images, audio files in one place. Moreover, it can share these resources with a specific user or group and it can collaborate in open social networks. Figures 25, 26 and 27 show our storage repository Interface.

Figure (25) Web IoT Storage Repositories Login Page

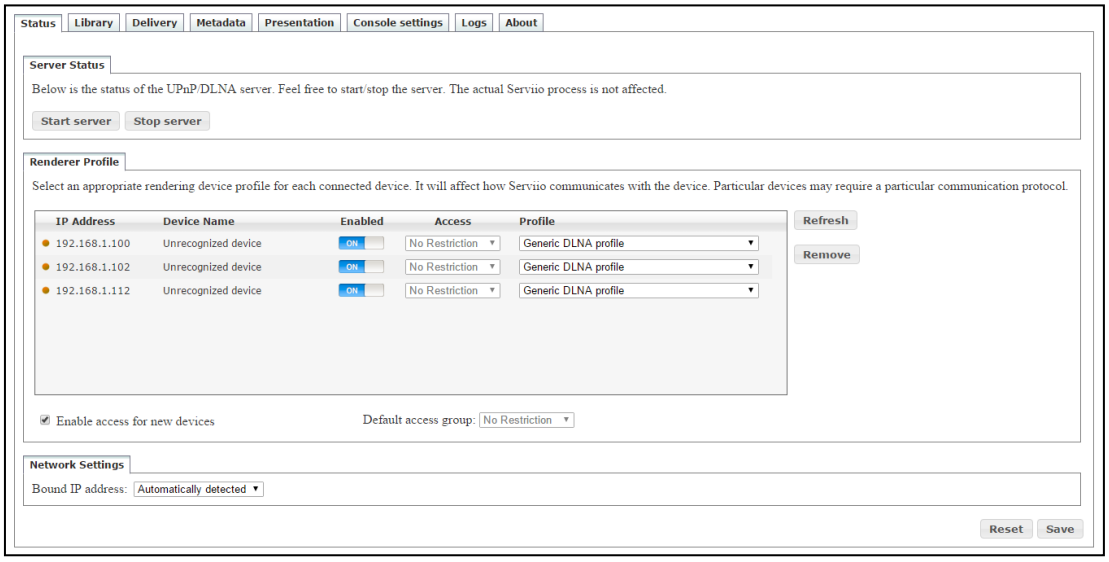


Figure (26) Web IoT Medea Stream Repositories

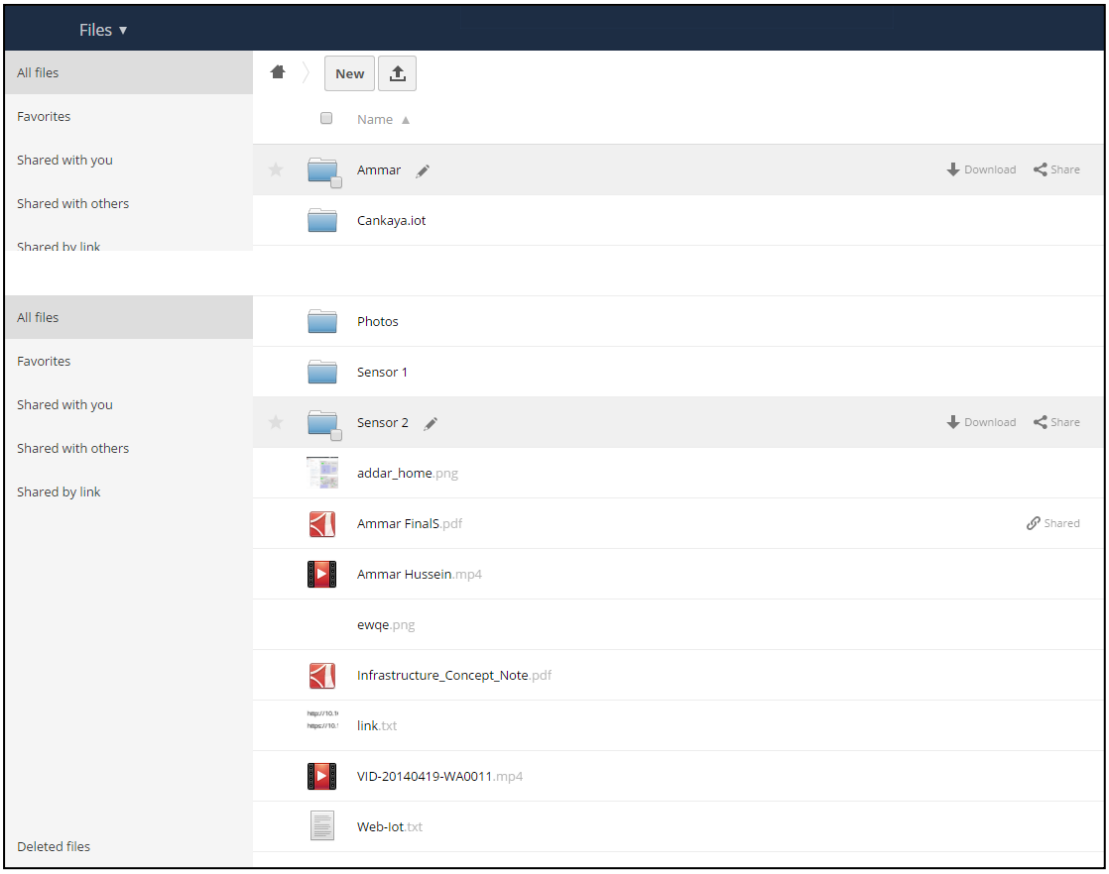


Figure (27) Web IoT File Storage Repositories

5.1.7 Unified Access

Different web content and applications can be put together in one place via logging with a secure Single Sign on (SSO). This can be integrated with an LDAP server and can be configured with customizable authentications, i.e., each user can have his own customizable web interface in accordance with his own rights and permissions.

5.2 Comparative Related Paradigms

In the previous chapters, we overviewed three suggested architecture-related works, and we classified them according to the established paradigms, namely the Internet of Things (IoT), the Sensor Cloud (SC) and the Web of Things (WoT). Table 1 below shows the most important features from the related work paradigms comparing them with our Web IoT paradigm.

Service and Technology used	WoT Paradigm	SC Paradigm	IoT Paradigm	Web IoT Paradigm
Portal	Yes	No	Partially Yes	Yes
Flexibility Sharing	No	No	No	Yes
Reliability	No	No	Yes	High Reliability
Scalability	Partially	Partially	Highly Scalable	Highly Scalable
Actors (Things)	No	No	Yes	Yes
Actors (Sensors)	Yes	Yes	Yes	Yes
Content Shearing	Yes	Yes	Yes	Yes
Cloud Services	Yes	Yes	Yes	Yes
Communication Line Protocols	Wifi, WiMaxetc, Zigbee, 3G, 4G, EDGE	Wifi, WiMaxetc, Zigbee, 3G, 4G, EDGE	Wifi, WiMaxetc, RFID, Zigbee, 3G, 4G, EDGE	Wifi, WiMaxetc, RFID, Zigbee, 3G, 4G, EDGE
Customizable	Yes	No	Partially Yes	Fully
Social Network	Yes	No	No	Yes
Calibrations	Partially Yes	No	Partially Yes	Yes
Web 2.0	Yes	No	Yes	Yes
Interoperability	Yes	No	Yes	Yes
Security and Privacy	High	High	Very High	Very High
CMS	No	No	No	Yes
Real Time Manner	Yes	Yes	Yes	Yes
Unified Accessing	Yes	No	Yes	Yes
Complexity	Yes	Yes	Yes	No
Look and Fell	Low	Low	Good	Very Good
Heterogeneity	Partially	Yes	Yes	Yes
Automation	No	Partially	Yes	Yes
Big Data	Medium	Medium	High	High
TCO	High	High	Very Hugh	Low

Tables [1] Related Work Paradigms Comparison

5.3 Performance Evaluation

In our lab, the test plan was performed to test our Web IoT performance. Web IoT offers services to huge numbers of end users. The dominant factors in such scenarios are the number of data packets exchanged per second, latency and throughput per server.

For this purpose, we use open source Apache JMeter to perform stress load testing on our application. Our lab components specification described in Chapter 4 and our test plan parameters included tuning the JVM parameters, tuning the server properties and tuning our application (to achieve high performance). We built our test plan with Apache JMeter as follows: Create a Thread Group, Create an HTTP Request to test (Login, logout , private load page, all web sites and Portlet login), Add HTTP Cookie Manager under Thread Group (control the cookie), Add Once Only Controller (control login request), add HTTP Proxy Server, Add Regular Expression Extractor, add Logic Controller (Recording Controller), and finally, adding a Listener, such as the Summary Report, a response graph (to view the result). Figure 28 shows our test plan implementation.

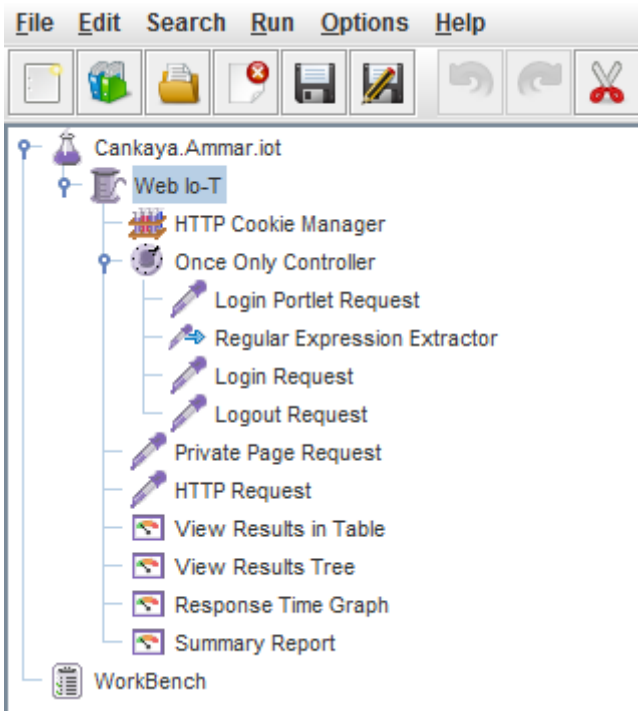


Figure (28) Test Plan Implementation

The test was performed many times to test the stress load on our application. The test included five elements (login, logout, private load age, all web site and Portlet logins). The test was carried out by accessing multiple users that generate multiple threads and samplers simultaneously. Each test was run with 100, 150, 200, 250 and 300 threads respectively and each thread was run 100 times. Tables 2, 3, 4, 5 and 6 show the results that were collected respectively, while Figures 29, 30, 31, 32 and 33 show the chart performance for each test respectively.

Label	Samples	Av.(ms)	Min	Max	Std. Dev.	Throug.	KB/sec	Avg.Byt.
Login Portlet Req	100	1.671	6	563	2062.04	14.8	337.1	23359
Login Request	100	1.034	35	259	793.77	13.4	331.6	25424
Logout Request	100	0.728	130	210	624.13	11.3	12.54	1134
Private Page Req.	10000	1.562	47	444	690.57	48.5	2313	48796
HTTP Request	10000	0.168	5	246	193.71	49.4	2289	47489
TOTAL	20300	0.884	5	563	910.97	103.6	4647	45944

Tables [2] Test 1-100 Threads Run 100 Times Results

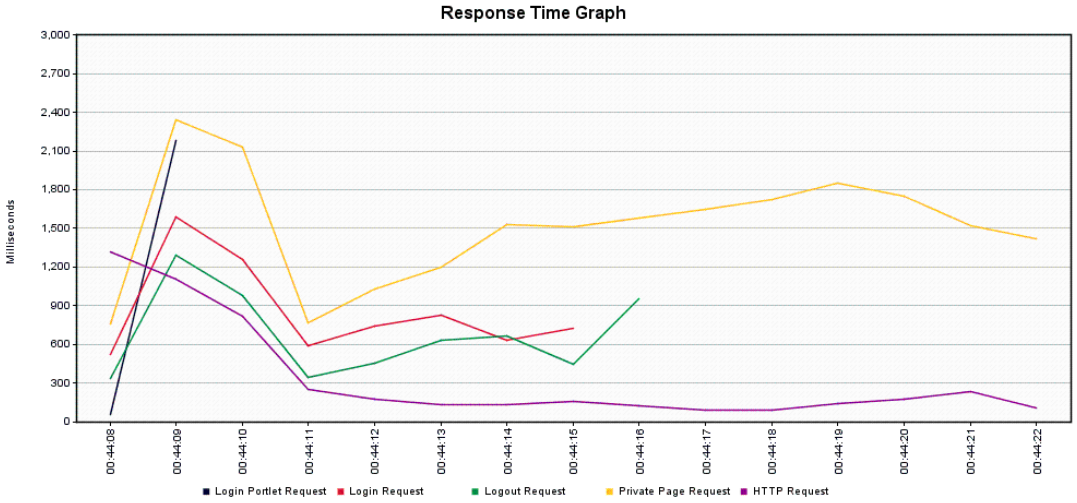


Figure (29) 100 Threads Run 100 Times Results

Label	Samples	Av.(ms)	Min	Max	Std. Dev.	Throug.	KB/sec	Avg. Byt.
Login Portlet Req	150	2.211	83	633	2536.48	19.7	450.3	23362
Login Request	150	1.001	15	201	357.6	16.6	412.5	25422.4
Logout Request	150	0.645	51	145	329.11	16.3	18.04	1134
Private Page Req.	15000	2.178	26	583	874.91	53.9	2570	48787.1
HTTP Request	15000	0.293	5	245	332.1	55.5	2573	47489
TOTAL	30450	1.239	5	633	1191.67	112.1	5031	45940.5

Tables [3] Test 2 -150 Threads Run 100 Times Results

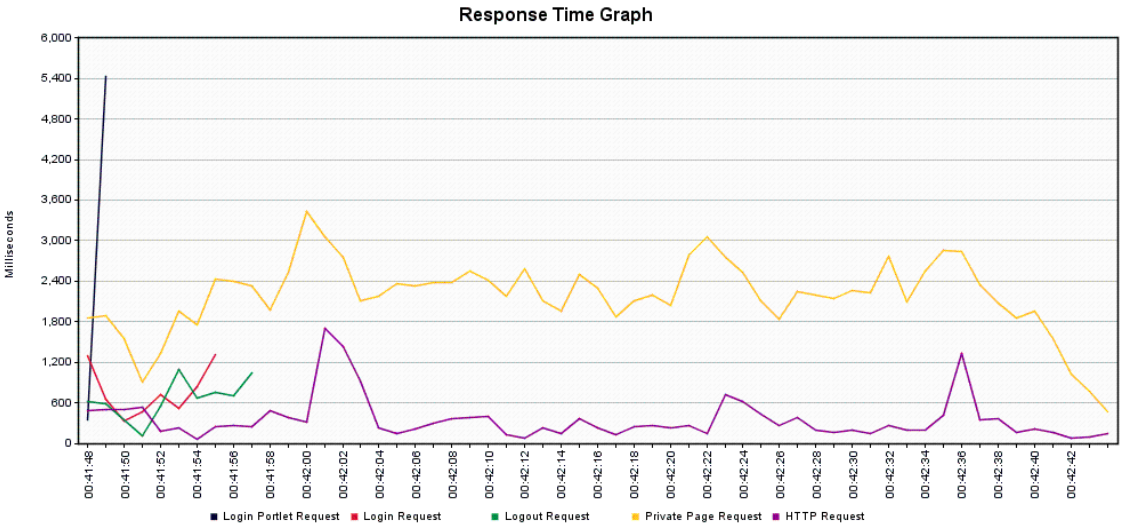


Figure (30) 150 Threads Run 100 Times Results

Label	Samples	Av.(ms)	Min	Max	Std. Dev.	Throug.	KB/sec	Avg. Byt.
Login Portlet Req	200	3.965	6	8818	3133.59	19.6	447.6	23359
Login Request	200	1.246	19	4214	671.35	14.4	358.6	25424
Logout Request	200	1.044	15	6452	946.65	10.8	11.99	1134
Private Page Req.	20000	3.158	96	1119	1504.55	49.4	2354	48795.7
HTTP Request	20000	0.274	6	3131	222.63	49.6	2301	47489
TOTAL	40600	1.742	6	1119	1844.75	104	4667	45944.4

Tables [4] Test 3- 200 Threads Run 100 Times Results

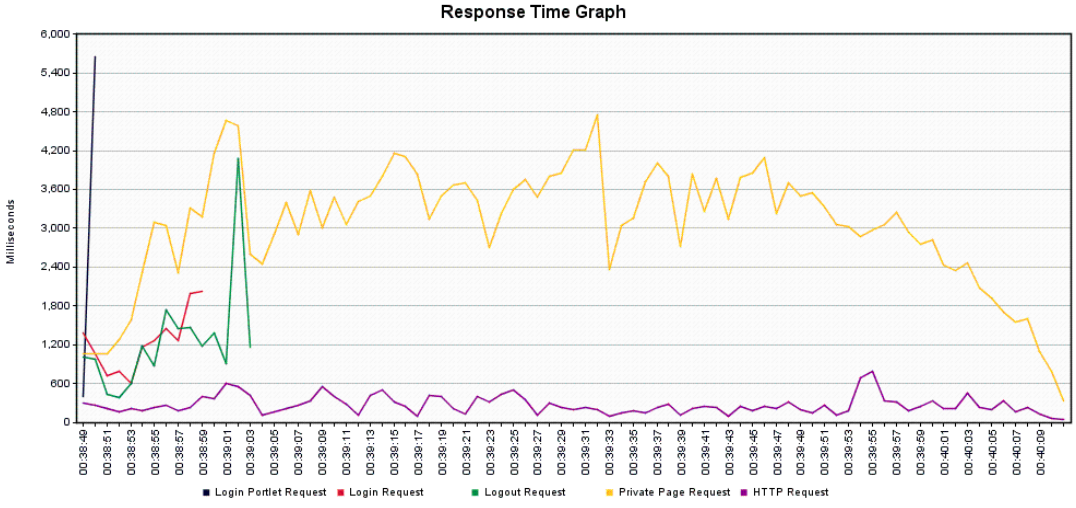


Figure (31) 200 Threads Run 100 Times Results

Label	Sample	Av.(ms)	Min	Max	Std. Dev.	Throug.	KB/sec	Avg. Byt
Login Portlet Req	250	6.308	6	1236	4046.58	18.1	412.3	23359
Login Request	250	1.721	12	7778	1025.92	11.6	288.7	25424
Logout Request	250	1.076	30	3395	698.22	10.7	11.89	1134
Private Page Req.	25000	3.556	56	2444	1733.12	52.1	2484	48796
HTTP Request	25000	0.412	5	3403	400.54	52.4	2429	47489
TOTAL	50750	2.057	5	2444	2153.34	109.9	4930	45944

Tables [5] Test 250 Threads Run 100 Times Results

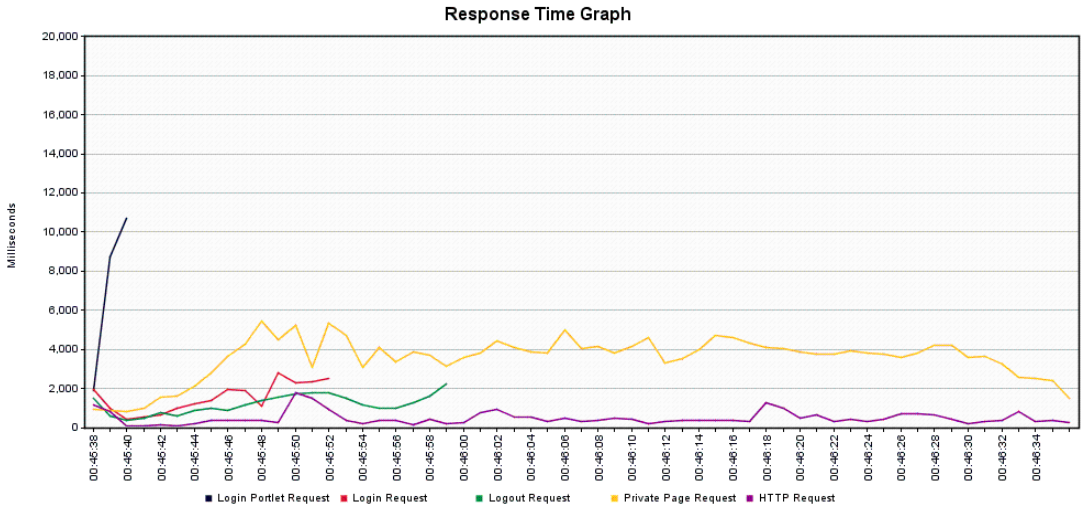


Figure (32) 250 Threads Run 100 Times Results

Label	Samples	Av.(ms)	Min	Max	Std. Dev.	Throug.	KB/sec	Avg. Byt
Login Portlet Req	300	13.963	6	8634	28778	19.6	77.05	23359
Login Request	300	2.109	17	7286	1014.96	11.4	81.82	25424
Logout Request	300	1.306	12	3504	619.38	12.1	3.6	1134
Private Page Req.	30000	3.489	48	2382	1817.21	52.7	2514	48796
HTTP Request	30000	0.394	6	1537	471.66	53.6	2488	47489
TOTAL	60900	2.21	6	8634	5143.72	149.4	5018	45944

Tables [6] Test 300 Threads Run 100 Times Results

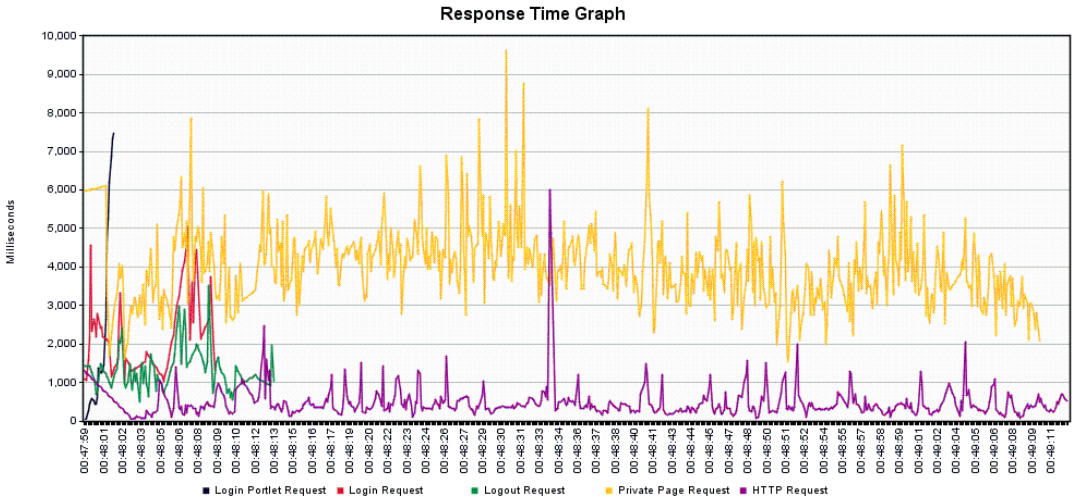


Figure (33) 300 Threads Run 100 Times Results

5.4 Compare System Performance

To achieve a fair comparison, we need to consider the following: the platform used in the system, lab test hardware and the test plan applied. Table 7 shows some results obtained from a test carried out in an online project that used the same relative test plan and a different methodology available at [61]. Our test showed better performance in average time response per millisecond and better throughput in Kb/sec.

Model	On line Project Test			Wob IoT Test		
Term	Request	Ave.(ms)	Throug.	Request	Ave.(ms)	Throu g
Private Page Req.	30,000	4,524	30.6	30,000	3.489	52.7
Login	30,000	5,100	30.6	300	2.109	11.4
Logout	30,000	22	31.5	300	1.306	12.1
HTTP Request	N/A	N/A	N/A	30,000	0.394	53.6
Login Portlet Req.	N/A	N/A	N/A	300	13.963	19.6
Total	90,000	3,215	91.7	60,900	2.21	149.4

Tables [7] Comparing System Performance

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

The Internet of Things in business and industry is facing many problems and there are many modern studies that attempt to overcome these problems. This research successfully introduced a risk-free paradigm for the Internet of Things, which provides support for HTTP, JSON, CoAP and SOAP. Furthermore, it can be integrated with Java ME and Java SE. This thesis has addressed the objective of this research and has overcome the problems of heterogeneity. The results show high performance and high throughput that was achieved under applied stress load tests. The research results proved that we can use the proposed model to reduce the total cost of ownership and produce a high scalable solution for the Internet of Things. Moreover, it can involve people in its life cycles.

Our results show high flexibility when accessing resources by giving stockholders and end users the authority to control and manage a wide range of customization tools of their own things and share these things on social networks or with individual users. Moreover, high reliability, security and privacy were achieved in our referenced architecture. The proposed architecture may be considered to be a step towards enabling the Internet of Everything (Io-E) in the future. A comparative study was applied in this research to show the proposed Web IoT paradigm feature compared with related work paradigms such as WoT, SC and IoT. The comparative results show many new features that can be added to our new paradigm.

6.2 Future Works

The big question of this industry is the future of the Internet of Things in a world that rapidly needs increasingly more connecting devices. Furthermore, there are billions of unconnected devices and dealing with these billions of prospective connectable things in the context of Big Data, security and privacy, and how to connect these unconnected devices using standard forms will remain open research issues in the next few years, also some recommendations of future works are listed below:

- Produce new communication protocols or develop existing ones to insure the reliability of communication lines in a real-time manner and to use a high rate of data transfer taking into consideration low power operation, heterogeneity and the Interoperability of Things.
- Develop a robust security mechanism to deal with things in a more efficient and reliable way taking into consideration the non-exhaustion of resources.
- Analyzing data collected and reused in other forms to serve other fields of science such as data mining and data warehouses.
- Develop new methodologies and embedded systems to connect unconnected things in a standard form. The embedded system should consider self-operation, self-management and efficient use of available resources.
- Suggestion of new business models for both stakeholders and end users
- Developing new applications giving people more opportunities to contribute to Internet of Things life cycles and more openness with social networks.

REFERENCES

1. **Charith P., Chi H., Srima J., and Min C., (2014*),*** *"A Survey on Internet of Things from Industrial Market Perspective"*, IEEE and ACCESS, IEEE Journals & Magazines Vol. 2 pp.1660 – 1679.

2. **Jayavardhana G., and Rajkumar B., Slaven M., and Marimuthu P., (2013),** "Internet of Things (IoT): A vision, architectural elements, and future directions", Elsevier, Future Generation Computer Systems 29 1645–1660.

3. **Madoka Y., and Takayuki K., (2010*),*** *" Sensor-Cloud Infrastructure Physical Sensor Management with Virtualized Sensors on Cloud Computing",* IBM Research/Tokyo IBM Japan, Network-Based Information Systems (NBiS), 13th International IEEE Conference, pp. 1 – 8.

4. **Irena B., George H.,and Jeffrey V., (2014),***"Imagineering an Internet of Anything",* IEEE Journals & Magazines Vol.: 47, Iss.:6, pp. 72 – 77.

5. **V. Çag G.,and Gerhard P.,(2013),***" Industrial Wireless Sensor Networks: Applications, Protocols, and Standards",* CRC Press, Series Industrial Electronics, USA ISBN: 978-1-4665-0051-8, pp.2-18.

6. **Tein-Yaw., Ibrahim M., Osama A., Van H., Wen-Hsing K., and Dharma P. (2013*),*** *" Social Web of Things: A Survey"*, IEEE International Conference on Parallel and Distributed Systems, pp. 570 – 575.

7. **Su L., Yan T. , and Yonghua L.,(2012),** *"A survey of transport protocol for Wireless sensor networks",* IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 2338 - 2341.

8. **Raghunandan G. , and Lakshmi B.,(2011) ,***"A comparative analysis of Routing techniques for wireless sensor networks",* IEEE National Conference on Innovations in Emerging Technology (NCOIET), pp. 17 - 22.

9. **Waltenegus D., Christian P., (2010),** *"Fundamentals of wireless sensor networks: theory and practice",* Wiley ISBN 978-0-470-99765-9, pp. 115-125.

10. **Gajjar, S.H., Dasgupta, K.S., Pradhan, S.N., Shingala, K.V., Zinzuwadia, and K.P.,(2011),** *"Comparative analysis of medium access control protocols for wireless sensor networks" ,* IEEE India Conference (INDICON) ,pp. 1-4.

11. **Alessandro S., Laurent G., Konrad W., and Lorenzo O., (2007),** *"Secure and trusted in-network data processing in wireless sensor networks: a survey",* Journal of Information Assurance and Security, Vol. 2, pp. 188-198.

12. **Ridong B.,(2011),** *"Topological optimization based on small world network Model in wireless sensor network", 2nd* International Conference on Control Instrumentation and Automation (ICCIA), pp. 253-256.

13. **Jiu-qiang X., Hong-chuan W., Feng-gao L., Ping W., and Zhen-peng H., (2011),** *"Study on WSN topology division and lifetime"*, IEEE International Conference, (CSAE), pp. 380-384.

14. **Bin W., Dongliang X., Canfeng C., Jian M., and Shiduan C., (2008***),"Employing mobile sink in event-driven wireless sensor networks",* IEEE Vehicular Technology Conference, 2008, pp. 188-192.

15. **D. Boyle, and T. Newe, (2007),** *"Security Protocols for use with Wireless Sensor Networks a Survey of Security Architectures ",* IEEE Third International Conference, (ICWMC'07), pp. 54 – 54.

16. **Jennifer Y., Biswanath M., and Dipak G., (2008),** *"Wireless Sensor Network Survey"*, Elsevier Computer Networks 52, pp.2292–2330.

17. **H.Dinh, C. Lee, D. Niyato, and P. Wang, (2011),** *"A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches",* Wireless Communications and Mobile Computing, Wiley Online Library.

18. **M. Zhou, R. Zhang, D. Zeng, and W. Qian, (2010),** *"Services in the cloud Computing era: A survey",* 4th International in Universal Communication Symposium (IUCS), pp. 40 –46.

19. **Sehgal, V.K., Patrick, A., Rajpoot, and L. A, (2014),** *"Comparative Study of Cyber Physical Cloud, Cloud of Sensors and Internet of Things: Their Ideology, Similarities and Differences",* Advance Computing Conference (IACC), 2014 IEEE International, pp. 708 – 716.

20. **Sanjay M., Vimal K., and Rashmi D., (2014),***" Sensor Cloud: A Cloud of Virtual Sensors",* IEEE Journals & Magazines Vol.: 31, Iss: 2, pp. 70 – 77.

21. **Miao W., Ting-Jie L., Fei-Yang L., Jing S., and Hui-Ying D. , (2010),** *"Research on the architecture of Internet of Things",* IEEE 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol.5, pp. v5-484 - v5-487.

22. **Gerd K., Fahim K., Daniel F., and Vasughi S., (2010),** *"Smart Objects and Building Blocks of Internet of Things"*, IEEE Internet Computing Journal, Vol. 14, Iss.:1, pp. 44-51.

23. **Rafiullah K, Sarmad U., Rifaqat Z., and Shahid K., (2012),***"Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges"*, proceedings of 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan.

24. **Miao W. ET. al., (2012),***"Research on the architecture of Internet of things",* proceedings of 3rd International Conference on Advanced Computer theory and Engineering, Beijing, China.

25. **Dieter U., Mark H., and Florian M., (2011),** *"Architecting the Internet of Things",* Springer, Verlag Berlin Heidelberg, ISBN: 978-3-642-19156-5, pp. 97-120.

26. **Roel P., (2012),** *"Security Architecture for Things That Think",* PhD Thesis Arenberg Doctoral School of Science, Engineering & Technology Faculty of Engineering Department of Electrical Engineering (ESAT).

27. **Miranda, J., Makitalo, N., Garcia-Alonso, J., Berrocal, J.; Mikkonen, T., Canal, C., Murillo, and J.M.,(2015),** *"From the Internet of Things to the Internet of People",*IEEE Journals & Magazines Vol.: 19, Iss.: 2,pp. 40 – 47.

28. **Dominique G. , and Vlad T.,(2009)**,"*Towards the web of things: Web mashups for embedded devices"*, Second Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 09).

29. **Erik W.,(2007),***" Putting things to REST",* Technical Report UCB iSchool Report 2007-015,School of Information, UC Berkeley.

30. **Markus W., Adrian M., Thorsten S., and Elgar F.,(2010),** *"Towards a PowerPedia A Collaborative Energy Encyclopedia",* Workshop of Ubiquitous Computing forSustainable Energy (UCSE), at UbiComp, Copenhagen, Denmark.

31. **OGC, (2014),** *"Sensor Web Enablement (SWE) standards"* **,** [Online]. Avalibal : http://www.opengeospatial.org/ , [accessed 17 Oct 2015].

32. **Mike B.,and Alexandre R., (2007),** *"OpenGIS Sensor Model Language (SensorML) Implementation Specification"*, Open Geospatial Consortium, Inc.

33. **IoT European Research Cluster, (2015),** *"Internet of Things Strategic Research Agenda (SRA)"* **,** [Online]. Avalibal : http://www.internet-of-things-research.eu/sra.htm [accessed 20 Oct 2015].

34. **Ian G., Ovidiu V., Peter F., and Anthony F., (2012),** *"Internet of. Things. 2012",*New Horizons, Halifax, UK, ISBN: 978 - 0 - 9553707 - 9 – 3

35. **Rohan N., Geoffrey M., Ian R., et..al , (2008),** *"CitySense: an urban-scale wireless sensor network and testbed",* School of Engineering and Applied Sciences, Harvard University BBN Technologies.

36. **Ron J., Davide C., Umberto C.,et..al , (2012),***"Smart Environmental Measurement &Analysis Technologies (SEMAT): Wireless sensor networks in the marine environment",* Centre for Marine Studies, The University of Queensland, St Lucia, 4072, Australia.

37. **S. Bainbridge, C. Steinberg, M. Furnas, *(2008),*** *" GBROOS—an ocean observing system for the Great Barrier Reef, in: International Coral Reef",* 11th International Coral reef Symposium, Ft. Lauderdale, Florida, pp.529–533.

38. **Min Z.,Tao Y., and Guo Fang Z., (2011),** *"Smart Transport System Based on The Internet of Things",* Applied Mechanics and Materials Vol. 48-49, pp. 1073-1076.

39. **Hong-En L. and Rocco Z., (2005),** *"A review of travel-time prediction in transport and logistics",* Proceedings of the Eastern Asia Society for Transportation Studies, Vol. 5, pp. 1433 – 1448.

40. **Chee-Yee C., and Kumar, S., (2003),** *"Sensor Networks: Evolution, Opportunities, and Challenges",* Proceedings of the IEEE, Vol. 91, no. 8, IEEE, 1247-1256.

41. **Bharathidasan, A., Anand, V., Ponduru, and S., (2001),** "Sensor Networks: An Overview", Department of Computer Science, University of California, Davis, Technical Report.

42. **Manoj K., (2011)***," Wireless Sensor Networks: Security Issues and Challenges",* IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224, Vol. 02, Iss. 01, code: 110746.

43. **HBE-Zigbex, Ubiquitous sensor network, Zigbex Manual,** [Online]. Available: http://www.hanback.co.kr. [Accessed 20 Oct 2015].

44. **Gartner , (2013),** [Online]. Available: http://www.gartner.com/technology/home.jsp [Accessed 20 Oct 2015].

45. **Gartner , (2014**), *"Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020"*, a research made in 2013 and republish in 2014[Online]. Available: http://www.gartner.com/newsroom/id/2636073 [Accessed 20 Oct 2015].

46. **ABI Research,** [Online]. Available: https://www.abiresearch.com/ [Accessed 20 Oct 2015].

47. **ABI Research, (2014**), *"More than 30 billion devices will be wirelessly connected to the Internet of Things by 2020",* [Online]., Available: https://www.abiresearch.com/press/ more-than-30-billion-devices-will-wirelessly-conne/ [Accessed 20 Oct 2015].

48. **Cisco,(2015) ,** *"Internet of every things (Io-E)",* tocnology accomplishment by Cisco ,[Online]. Available: http://www.cisco.com/c/r/en/uk/internet-of-everything-ioe/tomorrow-starts-here/ [Accessed 22 Oct 2015].

49. **The Internet Engineering Task Force (IETF)**, [Online]. Available: https://www.ietf.org/rfc.html [Accessed 25 Oct 2015].

50. **N. Kushalnagar , G. Montenegro, and C. Schumacher , (2007) ,** *"IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals",* RFC 4919, [Online]. Available: https://tools.ietf.org/html/rfc4919 [Accessed 25 Nov.2015].

51. **W3C, (2001),** *"Web Services Description Language (WSDL)",* [Online]. Available: http://www.w3.org/TR/wsdl [Accessed 29Oct 2015].

52. **W3C, (2007),** *"Simple Object Access Protocol (SOAP)",* [Online]. Available: http://www.w3.org/TR/soap12/ [Accessed 20 Oct 2015].

53. **Jun L., Yan S., John-Austen F., Richard P., and Dipankar R.,(2012),** *"Enabling Internet-of-Things Services in the MobilityFirst Future Internet Architecture",* World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE International Symposium .pp. 1 – 6.

54. **Raychaudhuri , Wade T., Roy Y.,et.al, (2010) ,** *"Mobility First Future Internet Architecture"*, funding from the National Science Foundation's Future Internet Architecture (FIA) program, [Online]. Available: http://mobilityfirst.winlab.rutgers.edu/ [Accessed 5 Dec. 2015].

55. **Sherif A., Bechir H., Mohsen G. and Ammar R.,(2014),** *"Enabling Smart Cloud Services Through Remote Sensing: An Internet of Everything Enabler"* , Internet of Things Journal, IEEE, Vol. 1, no. 3, pp. 276 – 288.

56. **Guillen, J., Miranda, J., Berrocal, J., Garcia-Alonso, J.,Murillo, J.M., and Canal, C., (2014),** *"People as a Service: A Mobile-centric Model for Providing Collective Sociological Profiles",* IEEE Journals & Magazines, Vol.: 31, Iss.: 2,pp. 48 – 53.

57. **Fazio, M.; Puliafito, and A.,(2015),***" Cloud4sens: a cloud-based architecture for sensor controlling and monitoring",* Communications Magazine, IEEE, Vol.: 53, Iss.: 3,pp. 41 – 47.

58. **Paganelli, F.; Turchi, S.; and Giuli, D.,(2014),***" A Web of Things Framework for RESTful Applications and Its Experimentation in a Smart City",* Systems Journal, IEEE, Vol.: PP, Iss.: 99,pp. 1 – 12.

59. **Jih-Wei W.,Ding-Wei C.,and Jehn-Ruey J,(2014),** *"The Virtual Environment of Things (VEoT): A Framework for Integrating Smart Things into Networked Virtual Environments",* Internet of Things (iThings), IEEE International Conference , pp. 456 – 459.

60. **Hoon-Ki L., Jong-Hyun J.,and Hyeon-Soo K.,(2014),** *"Provision of the Social web of Things",* Consumer Electronics ,Berlin (ICCE-Berlin), IEEE Fourth International Conference ,pp. 404 – 407.

61. **Simon S.,(2015),** *"Quick Wins in Liferay Performance: Testing and Tuning Liferay Portals"*, [Online]. Available: https://www.firelay.com/resources/blog/-/blogs/liferay-performance-testing-and-tuning [Accessed 28 Dec. 2015].

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Ammar Jameel Hussein Albayati

Date and Place of Birth: 28 November 1983, Iraq/ Kirkuk

Marital Status: Married

Phone: +9647808667758

Email: ammar.jameel.ict@gmail.com

EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Çankaya University, Computer Engineering dept., Ankara, Turkey.	2016
PGD	Iraqi Commission for Computers and Informatics- Informatics Institute for Postgraduate Studies , Baghdad , Iraq	2010
B.Sc.	Control and Systems Engineering University of Technology, Baghdad, Iraq.	2005
High School	Central High School Baghdad, Iraq.	2001

WORK EXPERIENCE

Year	Place	Enrollment
2005- Present	Iraqi Federal Board of Supreme Audit	ICT Specialist
2006-2012	Digital Pioneer Magazine / Part Time	Managing Editor

LANGUAGES

Language	Speaking	Reading	Writing
Arabic	Native	Native	Native
English	V.Good	V.Good	V.Good
Turkish	fair	Work on the development	Work on the development

PUBLICATIONS

- Digital Pioneer Magazine " Iraq Local ICT magazine " Thirteen edition Arabic-language at a rate of 5 thousand copies for each edition.

- Ammar Jameel , Seda Yuksel, Ersin Elbasi, " Dynamic Binary Location based Multi-watermark Embedding Algorithm in DWT " , iscturkey, ITU, Istanbul Conference 10 / 2014.

- Ammar Jameel , Seda Yuksel, Ersin Elbasi, " Dynamic Binary Location based Multi-watermark Embedding Algorithm in DWT " (Improved) , Journal of Theoretical and Applied Information Technology 20th August 2015 -- Vol. 78. No. 2 – 2015.

- Ammar Jameel Hussein, Ammar Riadh, Mohammed Alsultan, and Abd Al-razak Tareq, " Applications and Design for a Cloud of Virtual Sensors", 8th International Conference on Information Security and Cryptology,ISCTurkey 2015, METU, Ankara 10 / 2015.

- Ammar AL Bayati, Aws Nazar,Ammar Riadh, and SinanMajeed ," Examination a Wireless Sensor Data founded Using a Traditional Data Mining Algorithms", 3rd GLOBAL CONFERENCE ON COMPUTER SCIENCE, SOFTWARE, NETWORKS AND ENGINEERING, Istanbul Aydin University, Istanbul, Turkey, November 2015.

MEMBERSHIP AND PROFESSIONAL ASSOCIATION

- Microsoft certified professional ISA (2004)

- ORACLE DBA (Oracle 10 & 11 Database Administrator).

    - Oracle 11 DBA 1 & 2
    - Oracle 10g. Backup and Recovery
    - Oracle 10g. Performance Tuning
    - Oracle 10g Application server 1 & 2

- IBM Rational (Software Eng.)

    - Mastering requirements management with (Use Case)
    - Essential of Rational Clear Case UCM for windows 7.0
    - Essential of Rational Requisite Pro V7

- DELL- Enterprise Server Specialist (Technical)

    - Enterprise Service Force 1 (ESF1)
    - Dell Power Edge Servers and Dell Power Vault Storage
    - Dell Blade Server Solutions and Dell Equal Logic

- EMC's Velocity SE Development

    - Systems Engineer for the Consolidate & SE Accreditation for Governance and Archive

- CCSP Cisco Security Professional (course)

    - SNRS : Securing network with routing & switching
    - SNPA : Securing Networks with PIX and ASA
    - CSVPN: Implementing Cisco virtual private network
    - MARS: Implementing Cisco Security Monitoring, Analysis and Response System

- CCNSP : Cyberoam Certified Network & Security Professional (course)

- Iraqi Engineers Union Since 2006

- Federation of Arab Engineers Since 2010

HOBBIES

Reading, Photography, Community, Model building, and Traveling.