4-14-2017

Security Management for The Internet of Things

Long Chen
University of Windsor

Security Management for The Internet of Things

By

Long Chen

A Thesis
Submitted to the Faculty of Graduate Studies
through the Department of **Electrical & Computer Engineering**
in Partial Fulfillment of the Requirements for
the Degree of **Master of Applied Science**
at the University of Windsor

Windsor, Ontario, Canada

2017

Security Management for The Internet of Things

by

Long Chen

APPROVED BY:

_____

M. Kargar
Computer Science

_____

H. Wu
Electrical and Computer Engineering

_____

S. Erfani, Advisor
Electrical and Computer Engineering

14 February 2017

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

The expansion of Internet connected automation provides a number of opportunities and applications that were not imaginable before. A prominent example is the Internet of things (IoT). IoT is a network system that consists of many wired or wireless smart sensors and applications. The development of IoT has been taking decades. However, cyberattacks threat the IoT since the day it was born; different threats and attacks may cause serious disasters to the network system without the essential security protection. Thus, the security and the management of the IoT security system become quite significant.

This research work into security management of IoT involves five sections. We first point out the conception and background of the IoT. Then, the security requirements for the IoT have been discussed intensively. Next a proposed layered-security management architecture has been outlined and described. An example of how conveniently this proposed architecture can be used to come up with the security management for a network of the IoT is explained in detail. Finally, summarise the results of implementing the proposed security functions architecture to obtain the efficient and strong security in an IoT environment.

Keywords: Internet of things (IoT), architecture and layers, threats and attacks, security and management.

ACKNOWLEDGEMENTS

I would like to give my gratitude to the University of Windsor and the Faculty of Engineering to give me such a wonderful opportunity.

I want to thank my advisor professor Shervin Erfani, internal department reader professor Huapeng Wu and outside department reader professor Mehdi Kargar for their patiently guiding my studies and thesis.

Finally, I want to thank my parents, who gave me so much love and supports and my friends, who gave me so many encouragement and confidence during my entire studies.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS/SYMBOLS

AES	Advanced Encryption Standard
AMPQ	Advanced Message Queuing Protocol
API	Application Programming Interface
CA	Certification Authority
CRC	Cyclic Redundancy Check
CoAP	Constrained Application Protocol
CSA	Composite Services Architecture
DDoS	Distributed-denial-of-services Attack
DES	Data Encryption Standard
DLNA	Digital Living Network Alliance
DoS	Denial-of-service Attack
ID	Identification
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IDtrust	Identity and Trusted Infrastructure
IETF	Internet Engineering Task Force
IoT	Internet of Things
IoTSMS	Internet of Things Security Management System
IP	Internet Protocol
ISO	The International Organization for Standard
ITU-T	The International Telecommunication Union
MAC	Media Access Control
MD	Message Digest
MEMS	Micro-electromechanical System

MQTT	Message Queue Telemetry Transport protocol
M2M	Machine to Machine
NIDS	Network Intrusion Detection System
OASIS	Advancing Open Standards for the Information Society
OIC	Open Interconnect Consortium
PHY	Physical Layer
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RFID	Radio-frequency identification
SHA	Security Hash Algorithm
SKC	Secret Key Cryptography
SMIB	Security Management Information Base
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play Forum
WS-I	Web Services Interoperability
WPAN	Wireless Personal Area Network

CHAPTER 1

INTRODUCTION

"The IoT is the infrastructure of the information society." *

1.1 Internet of Things

IoT is a network system in both wired and wireless connection that consists of many software and hardware entities such as manufacturing management, energy management, agriculture irrigation, electronic commerce, logistic management, medical and healthcare system, aerospace survey, building and home automation, infrastructure management, large scale deployments and transportation. [1]

The purpose of IoT is to turn traditional products into connected products by taking advantage of exchanging data and communicating with each other in order to monitor and control the objectives. Figure 1 shows the conception of IoT.

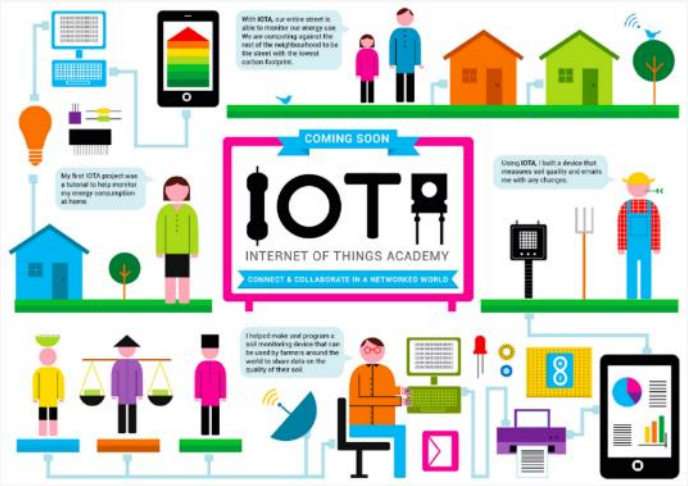

Figure 1. Conception of IoT. (*Taken from* [1])

*ITU, "Internet of Things Global Standards Initiative," Recommendation ITU-T Y. 2060, June 2012.

The advantage of the IoT is obvious: it is efficient data collection and exchange. In addition, IoT provides cost-effective ways for saving energy and contributing to environment protection. In other words, IoT enables advanced security by interconnecting physical and virtual devices based on existing and evolving interoperable information and communication technologies [*]. It involves a variety of protocols, domains and applications.

1.2 A Bit of History

As early as 1982, in the Carnegie Mellon University, a modified Coke machine was made which could report the temperature as well as the inventory. It is commonly believed this is the first internet connected appliance. The term IoT was coined by Peter T. Lewis in one of his 1985 speeches given at U.S Federal Communication Commission (FCC). In 1991, Mark Weiser, a chief scientist in the United States and the father of *ubiquitous computing* wrote a seminal paper on ubiquitous computing as well as the academic venues produced the conception of IoT. In 1994, Reza Raji an engineer of Echelon company in Palo Alto, California defined the IoT as "moving small packets of data to a large set of nodes, to integrate and automate everything from home appliances to entire factories". [1] From 1994 to 1996, companies like Microsoft, Novell, NEST provide some network solutions for the IoT. In 1999. Kevin Ashton, a British technology pioneer cofounded the Auto-ID Center at MIT. In his option, radio-frequency identification (RFID) made the IoT popular.

In 2013, the IoT evolved into multiple technologies, such as wireless communication, micro-electromechanical system (MEMS), and embedded systems. These realms working together to make a contribute to the IoT.

By the year 2020, it is expected that the IoT will surpass 50 billion objects. [1]

Figure 2 shows the increasing number of Internet connected devices of the IoT.

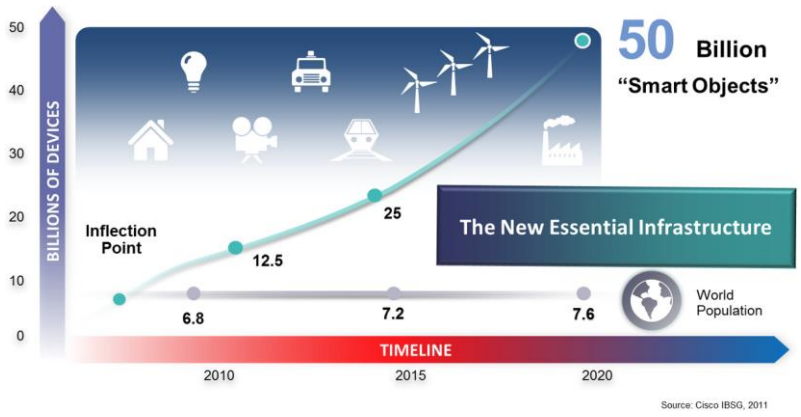

Figure 2. Internet Connected Devices of The IoT. (*Taken from* [1])

1.3 Applications of IoT

It is expected that IoT will

• Improve the intelligence of interconnected physical and virtual objects.

• Promote the interaction among people and their environment.

• Enhance reliability, operational efficiency and security.

• Reduce cost and energy consumption.

It is impossible to demonstrate all potential IoT applications in this study. fortunately, we mention a few applications, which represent the advancing trend of the future of IoT.

By the time of this writing, it becomes clear that the IoT will consist a large number of systems being connected to the Internet using IP addresses as unique identifiers. Interconnected systems in the IoT environment are using IPv6 to accommodate the extremely large address space requirement. The objects are having an IP address or uniform resource identifier (URI).

1.3.1 Smart Mobility

The conception of the Internet vehicles give rise to an easier and safer transportation method for the city residents, communicators as well as travellers. This is the core

Figure 3. The Conception of The Internet of Vehicles. (*Taken from* [1])

conception of the smart mobility as well as smart transport, security, mobility and convenience are three elements that Internet vehicles should be concerned with.

Safety and security should be the priority objectives for all the features. It involves network security, vehicle-to-vehicle communication security, and vehicle-to-infrastructure communication. The smart sensors guarantee the eco-friendly driving. Another objective is the automatic monitoring and identifying the critical systems and dangers in the road warning. Figure 3 shows the conception of the Internet of vehicles.

1.3.2 Smart Home

Nowadays, many families have WIFI devices at home, from the iPhone to the smart TV. The home IP network plays a significant role in the smart home, the conception of smart home focuses on the comfort, convenience, assisted living, and environmental monitoring.

There are sensors employed to collect the environment data like temperature, lighting, humidity, noises and atmospheric pressure. The smart-home application using this data to control the air conditioning, lighting, heating, ventilation and security at home. Users can modify the details of the smart-home application through some access like mobile phone, tablet, laptop or even use the voice control. Figure 4 shows the conception of the smart home.

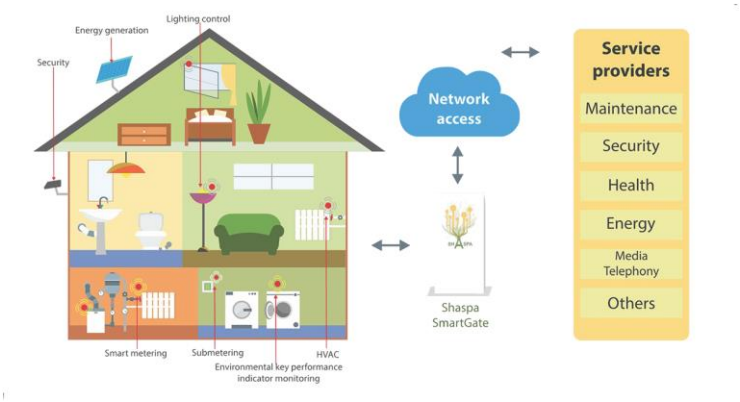

Figure 4. The Conception of the Smart Home. (*Taken from* [1])

1.3.3 Smart Health

The IoT devices can enable remote health monitoring. Nowadays, not only the conventional smart-health devices become popular in the market, but there are also the wearable technology devices, such as smart watches, healthcare devices, fitness tracking devices, baby and pregnancy wearable and even pet wearable. These smart health devices have the capability to obtain data from the sensors. Some other devices support the user interface or have displays and the wireless network connectivity such as Bluetooth or mobile network. The wearable technology devices required features like low power consumption, robustness, durability, accuracy, reliability and security to protect the personal privacy. Figure 5 shows the conception of the smart health.

Figure 5. The Conception of the Smart Health. (Taken *from* [1])

1.4 Problem of The IoT Security

The security issues descent the pace of the development of IoT. The attackers may use different techniques in different layers to attack the IoT network. As the IoT evolves, cyberattacks are more becoming physical threats. Data security has become the priority consideration for the designing of every IoT network systems. Some manufactures do not have any security standard for their products; some devices use its own de facto standard of security that do not compatible with other manufactures products; some old versions of devices do not have any security measure at all. Computer-controlled devices in automobiles such as breakers, engines, locks and dashboards have been shown to the vulnerable to attackers who have access to the network. Because the IoT is a rich source of data it will always be vulnerable to sophisticated attacks. In summary, there are number of security concerns from the end-user point-of-view as listed below:

i) Inadequate physical security for interconnected devices

ii) Insecure Web interfaces

iii) Insecure software/firmware

iv) Insecure mobile interfaces

v) Insecure network services

vi) Insecure transport and transmission

vii) Inefficient authorization and authentication

viii) Privacy and confidentiality concerns

ix) Data integrity concerns

x) Distributed denial-of-service (DDoS) threats *

* In 2016, a distributed denial-of-service (DDoS) attack used the IoT devices and caused a malware known as Mirai to take domain a DNS provider and major websites.

The security management of the IoT network system is very important to the potential end-users as well as network providers.

1.5 Purpose of The Study

The main purpose of this study is to provide a background of the IoT security and then propose a robust security management structure for the IoT.

There have been research works published on the IoT security management requirements. [2] [3] However, there is *lack of a unified approach* to systematically address the challenges arising from the integration and convergence of IoT into the existing network environment.

In order to provide a more cost-effective and efficient computer-controlled environment. ** There is a robust IoT security management system (IoTSMS) needed that enables the seamless integration of new applications that typically require installation of relevant devices, sensors and software. The IoTSMS must be able to handle a large number of devices, interconnected systems, transmission and processing of the pertaining security data.

There is no proposed IoTSMS for developing integrated solutions and incorporating new applications to cast an efficient, strong and sustainable security in the IoT environment. To fill this gap, we proposed a layered security functional structure for a robust IoTSMS in this study.

** As a response to increasing concerns over security, the Internet of Things Security Foundation (IoTSF) was launched on September 23, 2015. Its mission is to promote knowledge and test practices for security of the IoT.

1.6 Research Hypothesis

The existing and future IoT protocols and applications in practice are a variety of different technologies to support sophisticated automation. With that, it brings about an enormous challenge for security management of devices deployed in real environments. The essence of this study is to consider and analyze security services in IoT first and then outline a comprehensive IoT security management system. This research is needed as a response to increasing concerns over the security in the IoT environment.

1.7 Theoretical Framework

The functional architecture of IoT has been divided into four distinct layers, as we will describe in chapter 2. From the bottom to top are element layer, network layer, service layer and application layer. *

Each layer has its own components such as smart sensors and RFID in the element layer, IEEE 802.15.4 and 6LoWPAN protocols in the network layer, software applications in service layer and the application layer. The existence of the service layer is since a more extensive infrastructure will be needed on the network and on background services in order to manage the smart objects and provide services to support them. Different layers have different security issues such as element layer which consists of the smart devices requiring low-power and low-computing sensors. Smart devices are vulnerable to unauthorized access, eavesdropping and spoofing attacks. [3]

Thus, different layers need different mechanisms to ensure the overall security for the IoT. In addition to the security and protection aspects of the Internet such as the confidentiality, integrity and nonrepudiation, other security requirements in an IoTSMS

*ITU, “Internet of Things Global Standards Initiative,” Recommendation ITU-T Y. 2060, June 2012.

such as authorization, authentication, access control, availability and prevention of denial-of-service attacks.

1.8 Importance of the Study

The billions of smart devices will create huge amounts of data every day. These data can be used to deliver a better the users experience, improving the products services and benefit the development of other data-based search such as health and fitness, automatic driving and business management. [4]

Internet has changed our lives. The IoT has already assimilating into our daily lives, however, much of the public debate on whether to accept or reject the IoT involves security concerns.

The important of this study is to deliver a security functional architecture as well as easy security management methods for the IoT to meet the requirements of the end-users and network providers. The security management of IoT could provide protection of the data from the bottom to the top layers of the IoT; useful data and privacy information are firmly protected by the different security polices, services, mechanisms, as will be discussed in chapter IV.

1.9 Scope and Limitations of the Study

This study of security and management of IoT is a qualitative research. Every conception has its own limitations and boundaries. In the IoT, each layer has its own security challenges and issues. Different threats may cause different consequences for each layer. Different security services and different security mechanisms needed to be implemented in different layers to counter the corresponding security threats. However, different suppliers and network providers and manufactures may use different security standards and

mechanisms for their own IoT products. Thus, make the IoTSMS inefficient and impractical to implement.

1.10. Complexity and Compatibility

The IoT system has an architecture consists of four layers. Under different circumstances, such as multi-users and multi-tasks, working load of the IoTSMS may become complicated. A little bug in hardware or software may cause serious system failure or even worse. Thus, a common standard for IoT in both hardware and software at each layer should be employed in the design. The hardware and software manufactures should take care of the compatibility issues of IoT.

CHAPTER 2

IOT LAYERED ARCHITECTURE

> "As the IoT becomes a reality, networking will become even more complex, with virtually every computing element or household object becoming part of a large interconnected system."

As Mr. Pete Lewis said "The IoT is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices." * Today computers and computing capabilities is incorporated into almost every industrial product. So, the IoT reference model has been partitioned into four main layers. The layers from bottom up are element layer, network layer, service layer and application layer, as shown in Fig 6. **

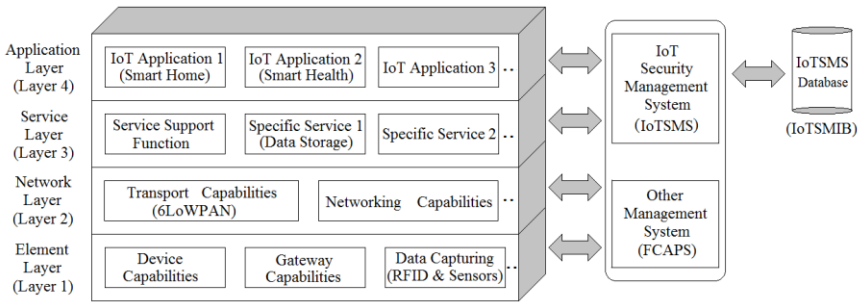

Figure 6. The IoT Layered Reference Model.

*ITU Internet Reports, "The Internet of Things," Geneva, Switzerland, November 2005, (retrieved on Dec. 19, 2016).

**ITU, "Internet of Things Global Standards Initiative," Recommendation ITU-T Y. 2060, June 2012.

Each layer has its own components, communication standards and protocols. The advantages of layered architecture are:

• Providing modular management of the IoT. We can implement different security protocols, security services and security mechanisms at each layer to enhance the overall protection of the IoT network system.

• The layered structure is easily expandable, and the lower layers are providing services to upper layers.

• Allowing the new technologies for both hardware and software to be incorporated into the existing IoT network system, and the layered structure is easy to manage as well as configure in a practical implementation.

2.1 Element Layer

Element layer is the lowest layer of the four layers of the IoT. It is in fact the device layer and consists of various kinds of nodes and sensors such as RFID, barcode labels, actuators and intelligent detection devices. These sensors are used to identify the objects as well as transport the obtained data to the next layer. Devices gather and upload data to the network layer either directly or indirectly. It is expected that all devices will be IPv6-capable in the future.

2.1.1 Radio-frequency Identification

Initially, RFID-equipped devices can be used for monitoring and status and access control in the IoT. Radios-frequency identification (RFID) is a wireless device using electromagnetic fields to transfer the data. The purpose of RFID is identifying and tracking tags attached on the objects. [5] The tag stores the electronic information. Some tags are battery powered, others are powered by the electromagnetic induction from a magnetic

Figure 7. The RFID Tags Used in the Libraries. (Taken *from* [5])

field from a tag reader. The RFID tag can be attached to an object and used to manage and track. RFID is widely used in many applications. It offers many advantages over the barcode, the tag can be read even covered by other objects, it can read hundreds at a time and the cost of a passive tag start at USD 0.09 each. [5] RFID is one method for automatic identification and data capture. Figure 7 shows the RFID tags used in the libraries. RFID can be implanted as microchips. The ISO/IEC 18000 and ISO/IEC 29167 provide the use of on-chip cryptography for untracebility, authentication and privacy.

2.1.2 IEEE 802.15.4 Standard Protocol

The IEEE 802.15.4 is a standard that specifies the requirements for physical layer and the media access control (MAC) for the low-power wireless personal area networks, which was defined in 2003. It is focuses on low-speed low-cost communication between devices. The IEEE 802.15.4 can be exclusively used with the IPv6-based Low Power Wireless Personal Area Network (6LoWPAN) to build a wireless embedded network for the IoT. The basic framework communication range is 10 meter with a transfer rate of 250 Kbit/s. [6] The higher layers are not defined in the standard. The architecture of the basic IEEE 802.15.4 is shown in Figure 8.

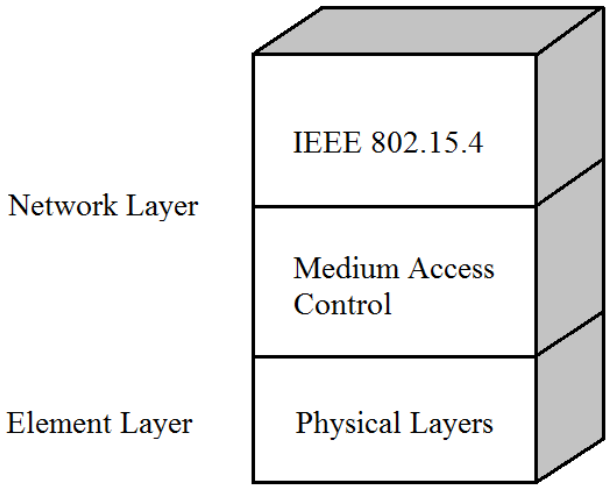

Figure 8. The Architecture of the IEEE 802.15.4.

2.2 Network Layer

The network layer transmits the data obtained from the element layer to the upper layer. The network layer transmits the information through the existing communication methods either wired or wireless network, Internet, cloud, mobile network, satellite network or military network. The IoT requires scalability in networking of a large numbers of devices. More than a billion devices will be added to the system annually. For this reason, IPv6 will play a major role in handling the network layer scalability.

2.2.1 6LoWPAN Protocol

The IPv6 Low Power Wireless Personal Area Network (6LoWPAN), which is named by the Internet Engineering Task Force (IETF) meets the requirements of the low-power consumption devices as well as the weak computing capabilities nodes and sensors which are the basic elements that constitute the IoT. 6LoWPAN allow packets to be received as well as send over the IEEE 802.15.4-based networks. [7]

2.3 Service Layer

The service layer consists of functionalities that processing the collected data and provide the links to the storage for the obtained data from the element layer. This layer of IoT serves as an interface between the different devices of IoT and provides communication methods between the elements. The service layer on top of the network layer provides connectivity between the sensors and application layer. It also provides services to ensure the effective functional communications between application and devices. The Figure 9 shows the data go through the service layer as an integration layer.

For an RFID system, as an example of a service-layer implementation, we can mention the "Open Remote," such as a middleware solution for residential and commercial buildings and automation.

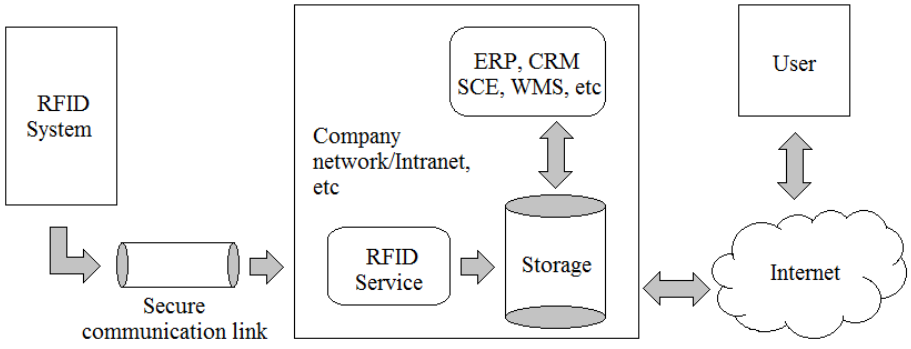

Figure 9. Data Go Through the service Layer. *

* ITU Internet Report, the Internet of Things, November 2005.

2.4 Application Layer

The application layer consists of a variety of practical applications of IoT based on the requirements of the users. The application layer uses various numbers of different protocols, such as the constrained application protocol (CoAP), the message queue telemetry transport (MQTT) protocol, the advanced message queuing protocol (AMQP), and extensible messaging and presence protocol (XMPP).

2.4.1 Constrained Application Protocol

The constrained application protocol (CoAP) is a synchronous request/response protocol designed by the Internet Engineering Task Force (IETF). [8] It was designed by using a subset of the HTTP schemes making it interoperable with HTTP. The CoAP runs over the UDP. The UDP-based application layer protocols reduce the bandwidth requirements and support multicast and unicast, not like the TCP, which does not support multicast. The target of the CoAP is the resource-constrained devices like the mobile phone, tablet, laptop, and low-power consumption devices.

2.4.2 Message Queue Telemetry Transport Protocol

The message queue telemetry transport (MQTT) is an application layer protocol, MQTT was powered by IBM as a lightweight machine-to-machine (M2M) communication protocol. [8] The MQTT runs on top of the TCP. It is an asynchronous publish/subscribe protocol that decreasing the network bandwidth and dropping the requirements for the computation. The MQTT is designed to meet the requirements of low-bandwidth and battery usage. The Facebook messenger uses the MQTT protocol. MQTT may has lower delays but CoAP gets low package losses and more reliability by providing the option of using quality of service (QoS). The MQTT protocol takes advantage of security features of

transport layer security (TLS)/ secure sockets layer (SSL) the same as HTTP transaction over the Internet.

2.4.3 Advanced Message Queuing Protocol

The Advanced Message Queuing Protocol (AMQP) is mostly used in financial industry. JPMorgan use AMQP sends 1 billion messages per day. [8] AMQP has an underlying reliability when runs over the TCP protocol. It provides asynchronous publish/subscribe messaging system. Research shows that the success rate increases as the bandwidth increases and compare with other rivals the AMQP can send a larger amount of message per second. [8] It ensures reliability with message-delivery guarantees. The security in AMQP is handed by using of the TLS/SSL.

In IoT network environment, everything designed by the various network suppliers and manufactures needs to be connected to the Internet; various forums and organizations are getting involved in the IoT network environment.

2.4.4 Extensible Messaging and Presence Protocol

The extensible messaging and presence protocol (XMPP) was standardized by the IETF, and it is designed for near real-time communications and runs over TCP. The XMPP protocol has TLS/SSL security built into its core specifications. [9] However, it does not support QoS options that makes it impractical for M2M communications. Although, XMPP has its own shortcomings, but lately has regained importance as a suitable protocol for the IoT.

2.5 Data Flow Between Layers

The data flow of the IoT can be divided into four phases, data collection, data transmission, data storage, and data analysis. The figure 10 shows the data flow of the IoT.

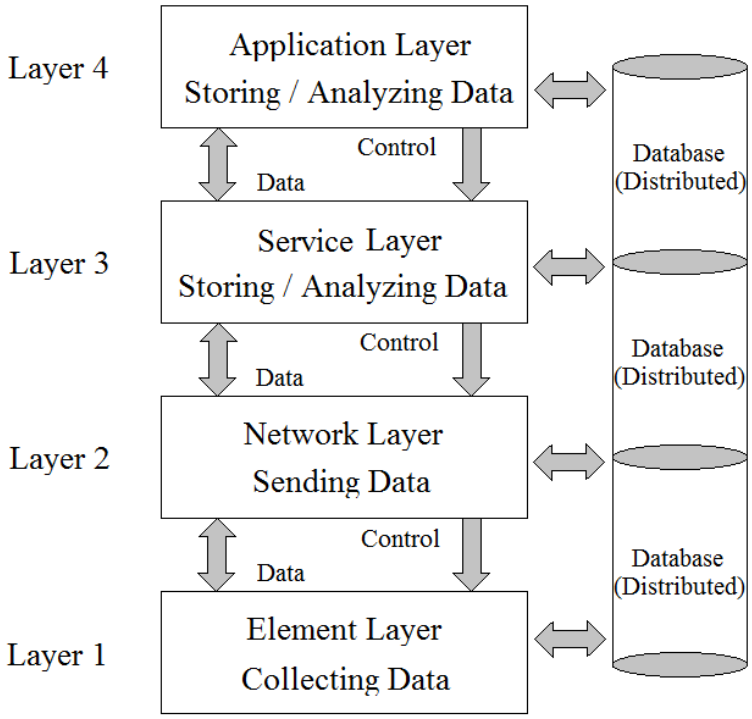

Figure 10. Data Flow Between Layers.

The data collection and storage are needed to perform the so-called five known network management (FCAPS) functions: fault, configuration, accounting, performance and security management.

2.5.1 Data Collection

The devices of the element layer collecting data from the environment; the data come from the various smart devices such as RFID, barcode labels, actuators and intelligent detection devices. These data will be sent to the upper layer in secure methods. The data content type can be XML on JSON (Java script object notation) and depends on the HTTP serve and its configuration.

2.5.2 Data Transmission

The data collected by the smart devices from the element layer will be sent in a secure method to guarantee the authentication, integrity and availability through the network layer.

Some standards should be implemented to ensure the data security such as IEEE 802.15.4 standard and the 6LoWPAN protocol.

2.5.3 Data Storage

To guarantee the reliability and data availability, the data storage needs backup and redundancy. This provides the required data duplication in case of system failure and in case of critical conditions.

2.5.4 Data Analysis

The service layer provides connectivity between the element layer and the application layer; it also provides the required software to the upper layers. The data transmitted through the network layer should be analyzed and implemented by the application layer software.

2.6 Summary

The IoT is defined as a network of intelligent systems for a more connected world. In fact, it is a network of physical objects that can interact with each other, share information, and take actions. IoT uses the RFID and sensors technologies, wireline and wireless communications, low-energy consumption technologies, cloud computing, and advanced Internet protocols. The IoT reference model is arranged as a four-layer functional architecture: (i) element layer, (ii) network layer, (iii) service layer, (iv) application layer.

The element layer is the lowest layer, which incorporates sensors, actuators, devices, etc, and collects the real-time information data. The network layer is the communication network infrastructure and supports the bandwidth and security requirements. It allows multiple organizations to share and use the same network environment independently. The service layer captures and analyzes periodic security data, ensures security and extracts relevant information from massive amount of raw data. The application layer provides a

user interface for using IoT. It supports different applications such as healthcare, transportation, supply chains, smart cities, etc. The major challenge for the IoT is huge data, large number of devices and physical components, power efficiency, advanced Internet protocols, and security management.

Our focus is mainly on the security management for the IoT. In the chapter 3, we will discuss security issues in the IoT environment in details.

CHAPTER 3

SECURITY REQUIREMENTS

3.1 Security Requirements

The basic security issues of IoT requires the identity authentication mechanisms and protection of the confidentiality of the data. The three basic areas are data confidentiality, data integrity and data availability. Breaching any one of these three basic security areas may cause security damages to the IoT system. Thus, each of the four layers of the IoT network system should meets these minimum requirements. Figure 11 shows the basic security requirements for the IoT.

3.1.1 Data Confidentiality

The goal of Data confidentiality is protecting the privacy of sensitive information by using some mechanisms and preventing the unauthorized access. [10] For the IoT devices such as the sensors and nodes, data confidentiality means the data collected by the sensors and nodes should not be transmitted to an unauthorized party. Data encryption is a mechanism to ensure the data confidentiality. The encrypted data convert into cipher text; thus, unauthorized users cannot easily access the data. The two-step verification is another method to ensure the data confidentiality. In this method, the user can only access to the data by passing two dependent authentication tests.

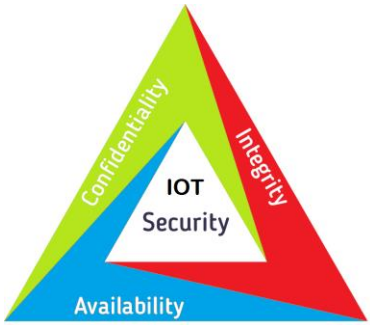

Figure 11. Basic Security Requirement for The IoT.

3.1.2 Data Integrity

Data Integrity protect the useful information from tempering by the cybercriminals, during the communication. There are variety of cases such as crash of servers or power disturbance that may affect the data integrity. One method to ensure the data integrity at the first-level is the cyclic redundancy check (CRC): CRC is a simple error detector mechanism to encode the message by adding a fixed-length check value for the error detection in IoT communication networks, the data integrity can be ensured by checking the check value. [11] Other method like Version control can syncing and backup the data to keep the file changes in the system, thus ensure the data integrity by restore the changing data in case of deletion or lost.

3.1.3 Data Availability

Data availability is very important to the security of IoT, data availability ensure the users can access to the information resources in both normal and disastrous situations, and data availability also ensure the consequent flowing of the information. To guarantee the data availability and reliability, IoT system needs the backup and redundant techniques to provide the duplication of the important information and prevent the data lose in system failure or system confliction conditions. Denial-of-service (DoS) and distributed-denial-of-services (DDoS) attacks cause the security issues of data availability, router filtering can countermeasure the issue and ensure the data availability of the IoT system.

3.2 Security Mechanisms

The security mechanisms of IoT is based on the restricted devices such as the low-power wireless sensors and battery powered network devices. Thus, efficient security mechanisms for security of the IoT needs to be considered in any design. Since the nodes and sensors

are low-power consumption and low-computing capabilities devices, the security mechanisms for the IoT devices should be as lightweight as possible. Without the efficient security, the data collected by the nodes may be captured by the intruders or be used to destroy the network system. Thus, several basic security mechanisms at all levels should be involved to protect the system.

3.3 Threats and Attacks on Element Layer

Element layer consists of different nodes and sensors to collect the data from connected network environment. The nodes and sensors are exposed to different threats such as unauthorized access, eavesdropping, spoofing, etc.

3.3.1 Unauthorized Access

The Element layer used nodes and sensors like RFID, tags, barcode labels, actuators and intelligent detection devices to collect the data from the environment; due to the absence of authentication services, unauthorized parties can get access to the data and modify it, or even delete the data. [12]

3.3.2 Eavesdropping

The information collected by the wireless components like RFID and tags are easy to be read by the attackers as has been mentioned in reference. [13] The data may be used by the attackers to hack any IoT system or sniff out the important information such as password or confidential information of the users.

3.3.3 Spoofing

Spoofing is the attackers send some fake information to the nodes and sensors pretend to act like the original failure, then the attackers may have the full access to the system. [14]

3.4 Element Layer Security

Element layer is the lowest layer of the four layers of an IoT system environment. Element layer consists of sensors and nodes, these devices are exposed to threats such as unauthorized access, eavesdropping and spoofing.

3.4.1 Element Layer Security Services

Authentication services are protecting the element layer from the unauthorized access attacks. Access control services can protect the element layer from the eavesdropping attacks. Confidentiality services are required to protect the element layer from the spoofing attacks. Thus, the authentication, access control and confidentiality services protect the element layer from attacks such as unauthorized access, eavesdropping and spoofing.

3.4.2 Element Layer Security Mechanisms

The element layer authentication services are using hash algorithms to provide a digital signature to counter the unauthorized access attacks, the access control table mechanism counter the eavesdropping attacks and the public key infrastructure (PKI) provide the confidentiality of the data collected by the sensors and smart devices.

3.5 Threats and Attacks on Network Layer

Network layer transmit the data which collected by the nodes and sensors to the terminal, wireless sensor network has been used to transmit the data, there are several security concerns at the network layer such as denial of services (DoS) attacks, man-in-the-middle attacks and malicious code injection.

3.5.1 Denial-of-Service (DoS)

DoS attack is when the attackers send lots of useless data to make the network traffic flooded. [15] By the huge consumption of the system resources, the IoT system will be blocked for the access of the authorised users.

3.5.2 Man-in-the-Middle Attack

This attack is a kind of eavesdropping that the unauthorized attackers can control the communication between the two parties. [16] The attacker can get the useful information through the communication channels.

3.5.3 Malicious Code Injection

In this case, the attacker compromises the vulnerable nodes and sensors by injection of malicious codes and attacks the IoT system. [17] The result may cause the network shutdown and the attackers could get the control of the system.

3.6 Network Layer Security

Network layer transmits the data which collected by the nodes and sensors to the upper layer, which is the service layer. There are several security concerns to be addressed at the network layer, such as denial of services attacks (DoS), man-in-the-middle attacks and malicious code injection.

3.6.1 Network Layer Security Services

Availability and non-denial of service protect the network layer from the denial of service attacks, the integrity and protection service protect the network layer from the man-in-the-middle attacks, the anti-virus services protect the network layer from the malicious code injection attacks.

3.6.2 Network Layer Security Mechanisms

The availability and non-denial of services are used through the router filtering to counter the network layer denial of service attacks. The data encryption needed to counter the man-in-the-middle attacks and the anti-virus security mechanism needed to counter the malicious code injection attacks.

3.7 Threats and Attacks on Service Layer

The service layer is processing the data and providing the links to the storage for the collected data from the element layer. The service layer security should prevent attacks like DoS attack, unauthorized access and malicious insider.

3.7.1 DoS Attack

The DoS attack in the service layer is similar to the network layer, that the attackers send lots of useless data to make the network traffic flooded, thus the huge consumption of the system resources exhausts the IoT system and cause the users unable to access the system.

3.7.2 Unauthorized Access

The unauthorized attackers could access to the service layer that provides the interface to the data and storage services; thus, the attackers may modify or delete the important data and cause fatal problems to the IoT system.

3.7.3 Malicious Insider

The malicious insider attack happens from the inside of an IoT environment, which uses the data for personal use. These data are very easy to access from the inside and only the authorized users can do it. [18] This is a different threat than unauthorised access and requires different mechanisms to counter the threat.

3.8 Service Layer Security

The service layer is processing data and provide the links to the storage for the collected data from the element layer. The service layer deals with security issues like DoS attack, unauthorized access and malicious insiders.

3.8.1 Service Layer Security Services

Availability and non-denial of service protect the service layer from the denial of service attacks. Access control and authorization service protect the service layer from the unauthorized access attacks, and the auditing log service we can protect the service layer from the malicious insider attacks.

3.8.2 Service Layer Security Mechanisms

The availability and non-denial of service via using intrusion detection system [19] (IDS) can counter the denial of service attacks. The access control mechanism is used to counter the unauthorized access attacks, and the event monitoring is needed to counter the malicious insider attacks.

3.9 Threats and Attacks on Application Layer

The application layer consists of a variety applications of IoT. The application layer security concerns such as DDoS attack, malicious code injection attack and phishing attack need to be addressed.

3.9.1 DDoS Attack

Distributed denial of services (DDoS) attack in the application layer is sophisticated nowadays. For the non-encrypted devices, an attacker can easily breach the system and cause data privacy issues for the users. The victims have no access to the services of the system and hardly noticed that the DDoS attacks occurred in the IoT system. [20]

DDoS attacks are different from the DoS attacks. Distributed denial of services (DDoS) attacks are launched from the many different connected devices; these connected devices are distributed across the IoT environment.

3.9.2 Malicious Code Injection

Malicious code injection is when attackers hacking the system and inject certain malicious code to get the access of the administration and control the IoT system. Attackers can get the confidential data or delete the important data of the system. This attack at the application layer requires different mechanism than when the malicious attacks occur at lower layers.

3.9.3 Phishing Attack

The phishing attack is a kind of email attack; the authorized users lured to open the email and the attacker is hacking into the system to get the access control of the IoT system. The attackers may get the sensitive messages or confidential data to get control of the whole system. [21]

3.10 Application Layer Security

There are several security breaches can happen at this layer such as DDoS attack, malicious code injection attack and phishing attack.

3.10.1 Application Layer Security Services

The availability and non-denial of service protect the application layer from the distributed denial of service attacks. The anti-virus services protect the application layer from the malicious code injection attacks, and the anti-phishing services protect the application layer from the phishing attacks.

3.10.2 Application Layer Security Mechanisms

The availability and non-denial of service using IDS are needed at this layer to counter the distributed denial of service attacks. The anti-virus mechanism is required to counter the malicious code injection attacks, and the spam filtering mechanism [22] can counter the phishing attacks. In this chapter, we used the conception of security services and mechanisms as defined in ITU-T (X.800). ITU-T X.800 commends some security mechanisms to provide the security services defined in standards.

Table 1 and Fig 12 shows the security services as well as mechanisms at each layer.

Table. 1 Security Services and Mechanisms at Each Layer.

Layers	Threats Attacks	Security Services	Security Mechanisms
Element	• Unauthorized Access • Eavesdropping • Spoofing	• Authentication • Access Control • Confidentiality	• Digital Signature • Access Control Table • PKI*
Network	• Denial of Services • Man-in-the-middle • Malicious Code Injection	• Availability • Integrity • Anti-virus	• Router Filtering • Data Encryption • Anti-virus
Service	• Denial of Services • Unauthorized Access • Malicious Insider	• Availability • Access Control • Auditing Log	• IDS* • Access Control Table • Event Monitoring
Application	• DDoS • Malicious Code Injection • Phishing	• Availability • Anti-virus • Anti-phishing	• IDS* • Anti-virus • Spam Filtering

*PKI: A framework provides data privacy in communications by using encryption and authentication.

*IDS: A security system to monitor the traffic of the network to detect the DoS attacks.

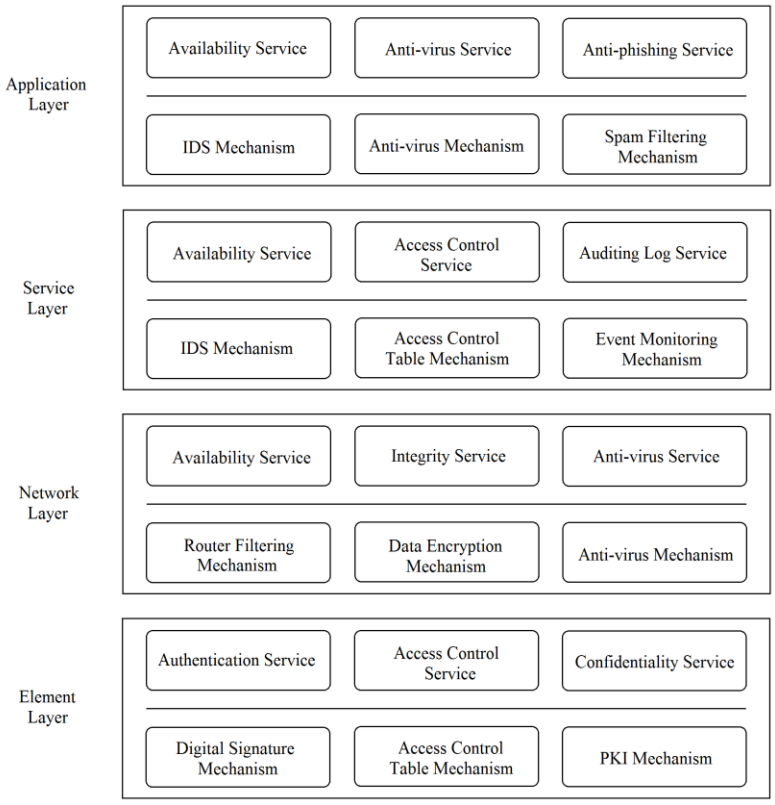

Figure 12. Security Services and Mechanisms at Each Layer.

3.11 Standards and Protocols for IoT at Each Layer

Due to the existence of a variety of networks, devices and applications in an IoT environment, a number of standards are used and various organizations are getting involved. This adds to the complexity of design as well as implementation of a reliable IoT network.

In the early 2013, standards for the IoT has been only concern of IT industry. As standards were developed later, and their implementation were concerned, IoT encountered lots of security challenges and still have a long way to go from the universal IoT standard. More specifically, IoT standards are not like a “one fits all” standard. It is more like a pacemaker that fix the security problems and protect the IoT system from the attacker’s threats. Figure 13 shows the organizations and various protocols at use today for IoT at each layer.

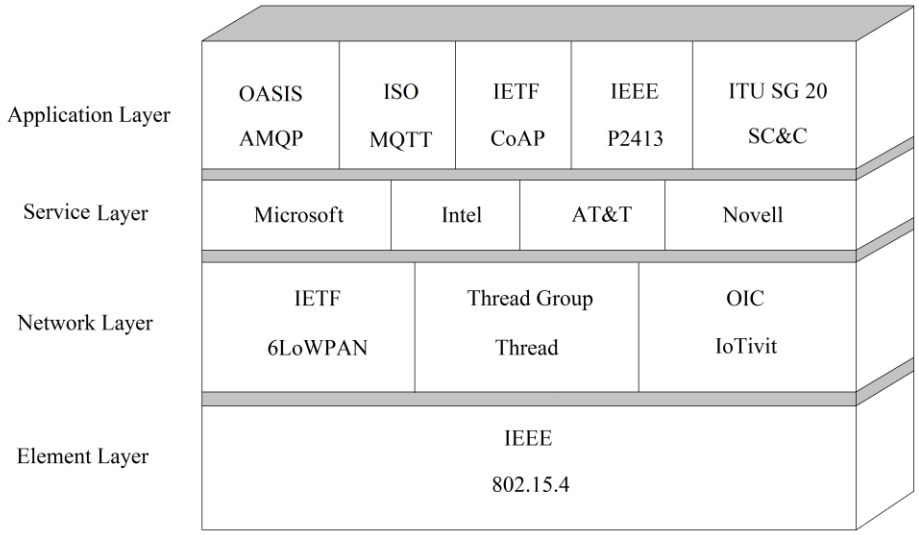

Figure 13. Organization and Protocols for IoT at Each Layer.

3.11.1 IEEE 802.15.4 at Element Layer

IEEE 802.15.4 is a standard that specifies the physical layer (PHY) and the media access control (MAC) communication for the low-speed low-cost communication between devices in wireless personal area networks. IEEE 802.15.4 implements the advanced encryption standard (AES) symmetric cryptography mechanism and support several security modes; [23] these security modes provide security services such as confidentiality, authentication, and integrity. Table 2 shows the security services and the security modes of the IEEE 802.15.4.

Table 2. Security Services and the Security Modes of the IEEE 802.15.4

Security Service	Security Mode	Security Mechanism
Confidentiality	AES-CTR	Data is encrypted using AES in the counter mode with 128-bit keys
Authentication Integrity	AES-CBC-MAC/MIC-32	Data is encrypted using AES in the cypher block chaining mode with message authentication code and message integrity code in 32/64/128-bit keys
	AES-CBC-MAC/MIC-64	
	AES-CBC-MAC/MIC-128	
Confidentiality Authentication Integrity	AES-CCM-32	Data is encrypted using AES in the counter and cypher block chaining mode with message authentication code and message integrity code in 32/64/128-bit keys
	AES-CCM-64	
	AES-CCM-128	

3.11.2 6LoWPAN at Network Layer

6LoWPAN is a network protocol that transport IPv6 packets through the low-powered IEEE802.15.4 wireless communication network environment. The 6LoWPAN implements the routing protocol (RPL) for low-power and lossy networks (LLNs) routing mechanism and has three security modes. The RPL implements the AES with 128-bit keys for MAC and supporting RSA with SHA-256 for the digital signatures to provide confidentiality, and integrity. [23] The security modes are described below:

• Unsecured: In this secure mode, the RPL sending the data without using any additional security and this is the default security mode in RPL protocol.

• Preinstalled: The symmetric keys will give to the nodes by join the RPL.

• Authenticated: When there is, a new device join the network, the key authority will authenticate and authorize the new device.

3.11.3 CoAP at Application Layer

The CoAP runs over the UDP. The UDP-based application layer reduces the bandwidth requirements and support multicast and unicast, the target of the CoAP is on the resource constrained devices like the mobile phone, tablet, laptop, and low-power consumption devices.

The CoAP protocol provides a "request and response" communication model between the end-points and adopts the AES as the cryptographic algorithm to provide the security services such as confidentiality, authentication and integrity. [23]

Figure 14 shows the format of the CoAP message header.

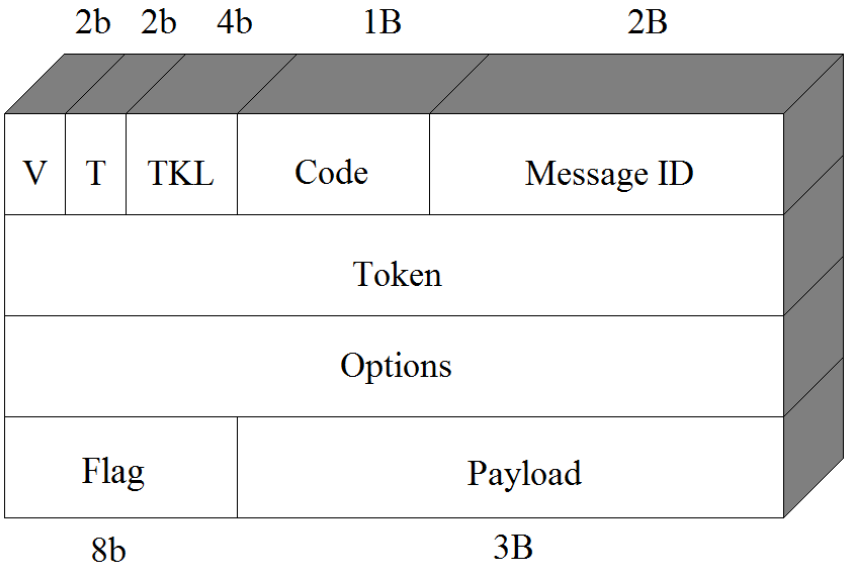

Figure 14. CoAP Message Header.

The header of the CoAP has 4 bytes which are: version field with 2 bits, the message type with 2 bits, the token length with 4 bits, the code field with 8 bits and the message ID with 16 bits. The token enabled the CoAP to perform a matching of the request and replies, the options define the length value format by specifying the option number following its length and value.

The standards and protocols show above will be sued in the IoTSMS smart home scenario at the next chapter.

CHAPTER 4

IOT SECURITY LAYERED ARCHITECTURE

> "A comprehensive system and method for managing security in an electronic network."

4.1 IoT Security Management System

The IoT security management system (IoTSMS) should be based on the architecture of the IoT network system. There are five basic security problems in the IoT network system; each of them should be considered before the design in the security management system. These security issues are that smart sensors are easy to attack, security management should support low-power smart devices, privacy issues of the element layer devices, different Layers confront with similar threats, and system complexity and compatibility issues. *

These requirements imply that we need to develop a security management system for the IoT environment that counters all perceived threats and be compatible with the IoT network architecture. In other words, since the IoT network environment is designed as a four-layer system architecture, it is quite appropriate that the security management of the network be organized along the same lines as a layered architecture. To implement this concept, we propose a four-layer security management system for the IoT environment as shown in Fig 15, similar to that used for the IPSec functional architecture. [24]

The proposed IoT security management system (IoTSMS) has four functional layers. The principles that were applied to arrive at four layers are as follows:

(i) A layer of functionality is created where a different type of security functions on different level is needed.

* S. Erfani, "Security management system and method," Patent US 6542993B1, April 1, 2003, Lucent Technologies Inc.

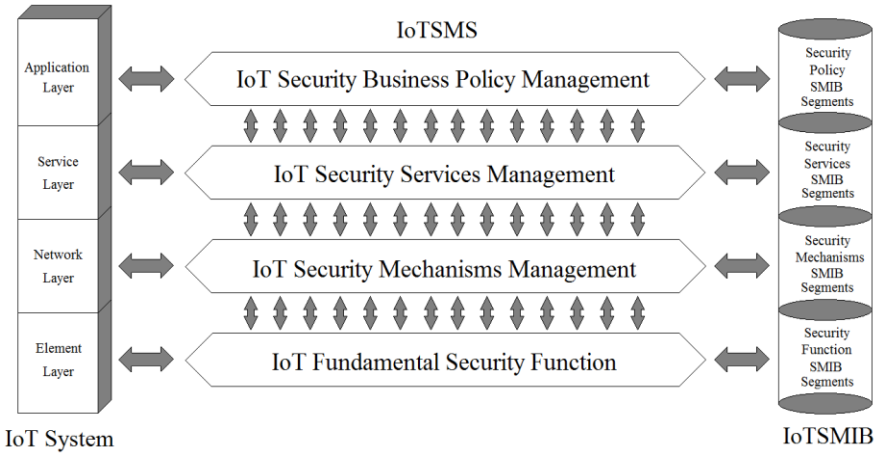

Figure 15. Security Management System for IoT.

(ii) Each layer performs a well-defined security function.

(iii) The functionality of each layer is chosen with consideration toward already existing standardized protocols.

(iv) The layer boundaries are chosen to minimized the data flow across the system interfaces.

(v) The number of layers are compatible with the IoT system layers in such a way that distinct security functions need not be through in the same layer.

The shown security management system has three parts; on the left, we have shown the architecture of the IoT network system which consists of four layers. In the middle part is the IoTSMS, which has the four-layer as the security business policy management, IoT security services management, IoT security mechanisms management and IoT fundamental security function. Such as pseudorandom generator, multiplicative inverse, modular arithmetic function, etc.

Each layer has its corresponding security management functionality to provide the data confidentiality, data integrity and data availability. On the right-side of this diagram is the IoT security management information base (SMIB), the SMIB implement the X.509

version 3 recommendation authentication, among other things, to provide the conceptual data need segments of IDs of smart sensors, user profiles, access control list and security logs.

4.2 Functional layers of Security Management for IoT

There are four layers of security management for IoT, as mentioned before. They are IoT security business policy management layer, IoT security service management layer, IoT security mechanisms management layer and IoT fundamental security function layer. Each layer has its own function to provide the protection for the IoT security management system.

4.2.1 IoT Security Business Policy Management Requirements

The security business policy management layer is concerned with the business user requirements such as prevention and detection of all attacks from different point of attacks, protecting the privacy of all smart devices and protecting the IoT system from attacks and forestall the system failure. Figure 16 shows the IoT security business policy management at minimum requirements.

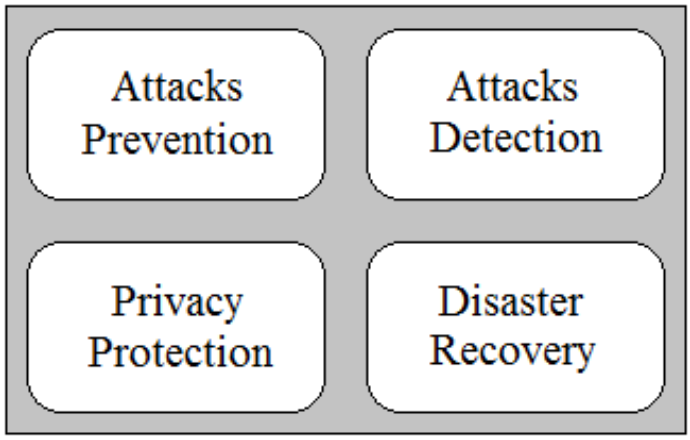

Figure 16. IoT Security Business Policy Management Requirements.

4.2.2 IoT Security Services Function

The IoT security services functional layer section provides the most common security services such as authentication service including peer-entity authentication and data-origin authentication, confidentiality is probably the most common aspect of IoT security including connection confidentiality, connectionless confidentiality, selective field confidentiality and traffic flow confidentiality. Information in the IoT environment is changing constantly. Integrity service in this environment means that changes need to be done only by authorized entities and through authorized mechanisms. Integrity services including connection integrity, connectionless integrity and selective field integrity; nonrepudiation services including origin nonrepudiation and destination nonrepudiation and the access control service are essential for security of the IoT system.

Figure 17 shows the section of IoT security services functionality layer.

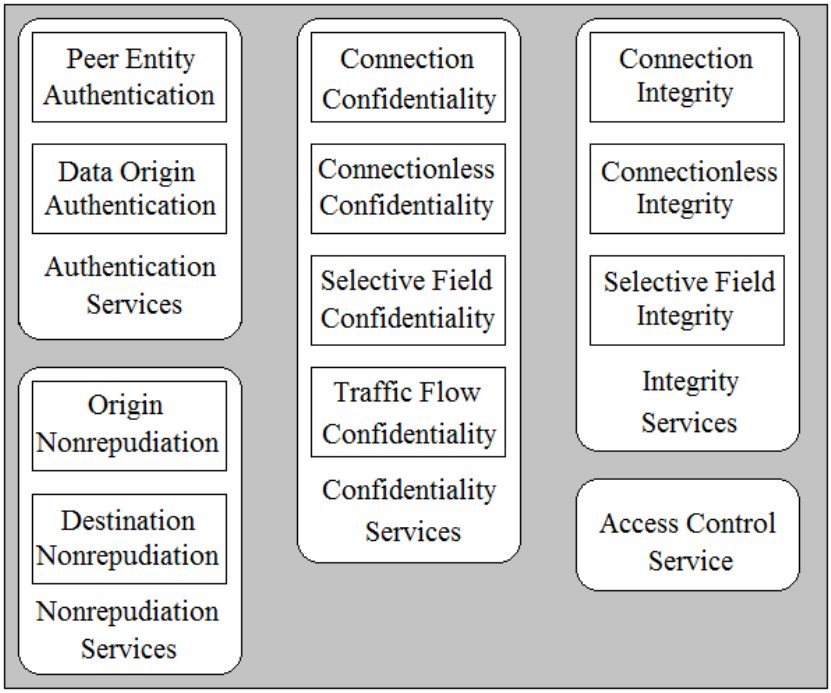

Figure 17. IoT Security Services Functionality Layer.

4.2.3 IoT Security Mechanism Function

Security mechanisms provide techniques, algorithm and schemes needed to support specified security services defined in the security services layer. The IoT security mechanism functionality layer provides the security mechanisms as either specific mechanisms or pervasive mechanisms. The specific security mechanisms include encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control and notarization security mechanisms. Pervasive security mechanisms include trusted functionality, security label, even detection, security audit trail, security recovery, network and host IDS and anti-virus security mechanisms.

Figure 18 shows the modules of IoT security mechanism functionality layer.

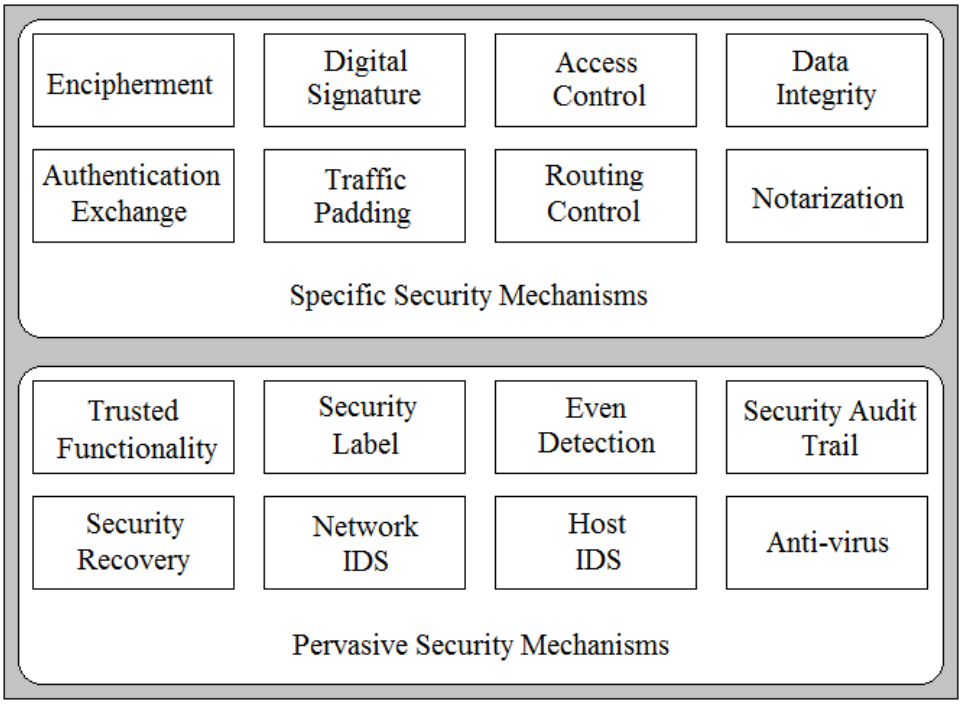

Figure 18. IoT Security Mechanisms Functionality Layer.

4.2.4 IoT Fundamental Security Function

A fundamental property of the IoT SMS is to be used as a comprehensive autonomous security server, as it may provide security to multiple applications at the same time. Thus, the lowest layer of functionality is considered to include various generic arithmetic and encryption modules. The IoT fundamental security function provides the basic security functions such as one-way hash, message digest, and secure hash algorithms. Key exchange security functions including Diffie Hellman, elliptic curve and RSA algorithms are including in this layer. Digital signature standard and elliptic curve algorithms, message authentication, authentication code, time stamping and certificates including X.509 certificate standard can be included in this layer. This layer encompasses the all required cryptographic elementary functions for the IoT SMS to operate.

Figure 19 shows the modules of IoT security fundamental security functionality layer.

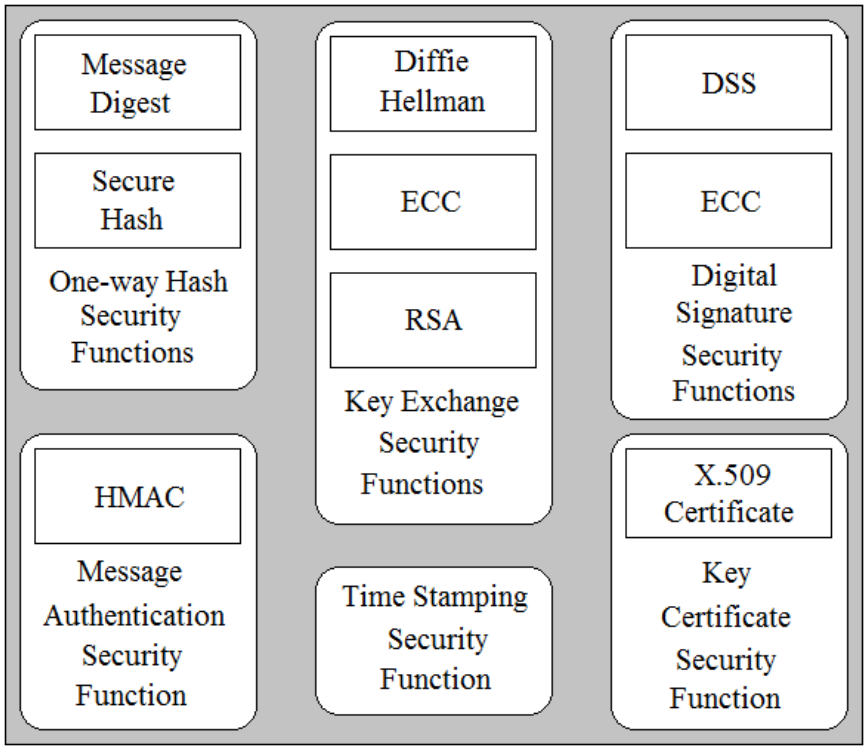

Figure 19. IoT Fundamental Security Functionality Layer.

4.3 IoT Security Management Information Base

The IoT SMIB is an important component of the IoT SMS. This information database must be structured to support implementation of all IoT security services in a computing environment or communication environment. The IoT security management information base is the conceptual segments of IDs of smart sensors, user profiles, access control list and security logs. Note that this concept does not suggest any content or form for the storage of information. [25] Figure 20 shows the IoT SMIB segment.

As shown, the IoT SMIB is a repository of all content information and parameters necessary for normal functioning of the IoT system. There are interactions within and amongst the IoT SMS layers and the IoT SMIB.

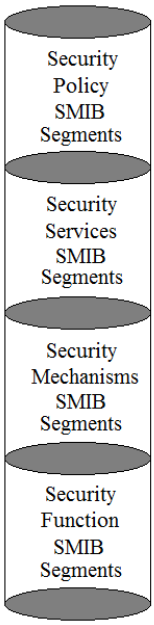

Figure 20. The IoT SMIB segments.

4.4 PKI for the IoT Security

The Internet Engineering Task Force (IETF) has created the Public-key Infrastructure (PKI) to provide several and a trust model. The important functions of PKI as far as the security of the IoT system is concerned are issuing X.509 certificates, key storage and update, providing services to a number of protocols, and providing access control.

PKI provides basic framework for information security in communications by using encryption and authentication. With having PKI in place, the IoT system is not vulnerable to the brute-force and malicious attacks. PKI secures the integrity of the data collected by the sensors and smart devices and provides the availability as well as access to the protocol and application configuration. Also, PKI ensuring the confidentiality of the element layer in IoT system.

In the IoT system, the data is encrypted by the Wireless Sensor Network (WSN) nodes and transmitting to the gateway. The gateway decrypts the data and then encrypted the aggregated data before transmitting to the upper layers. According to the conventional approaches, a key is sheared among all the sensors while encrypting the collected data. If the key is compromised the whole system is compromised.

PKI provides a pair of public-private keys mathematically related. If one key is used to encrypt the data, only the other related key can decrypt the data. In the case of the element layer in IoT system, the data collected by the sensors and smart devices is encrypted using a public key and then using the private key to decrypt.

4.5 Advantages of The Modular Security Management System for The IoT

The security management system for the IoT providing a modular structure that provide a plurality of security services and a plurality of security mechanisms. Thus, it implementing

the security requirements for the suppliers, network providers and the device manufactures. The different security service management module can invoke different security mechanisms module by implementing the efficient fundamental security function to establish the optimal requirements for security and management of the IoT network system.

Based on the security requirements of the users, the modular security management system IoTSMS implements efficient security methods and schemes in the IoT network system. The proposed IoTSMS can accommodate new security as well as new techniques and technologies. It provides a common platform for security in an IoT system environment.

4.6 An IoT Security Management Scenario

Let us look at a smart home security management scenario. The owner of the house wants to monitor the comfort level in his house. However, the owner of the house is at his/her workplace and wants to use his/her smart phone to monitor the temperature, humidity as well as illumination in his house.

Figure 21 shows a possible communication scenario for this smart home concept.

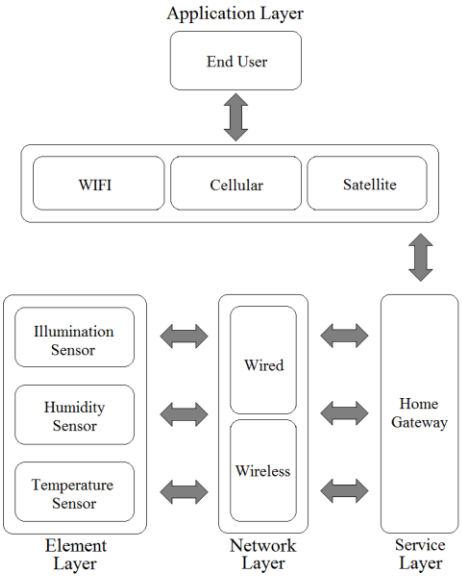

Figure 21. Concept of The Smart Home Scenario.

4.7 Protocols Used In The IoTSMS Scenario

To illustrate the complexity of security services in the IoT environment, we walk through a practical scenario of the smart home. We explain each function involved and the required data at each layer. To meet the requirements of the low-power and low-speed smart devices in the element layer, we should use the IEEE 802.15.4 wireless communication protocol to provide the needed security services of confidentiality, authentication and integrity.

At the network layer, we need to use the 6LoPWAN protocol, which implement the low-power and lossy networks routing mechanism. The routing mechanism implements AES with 128-bit keys for MAC and supporting RSA with SHA-256 for the digital signatures to provide the security services of confidentiality and integrity.

At the application layer, we need to use the CoAP protocol which runs over the UDP to reduce the bandwidth requirements and support the resource-constrained devices and low-power consumption devices. The CoAP protocol provides a "request and response" communication model between the end-points and adopts the AES as the cryptographic algorithm to provide the aforementioned security services. Figure 22 shows the reference protocols used in this smart home scenario and Table 3 shows the comparing of existing security protocols in the smart home scenario.

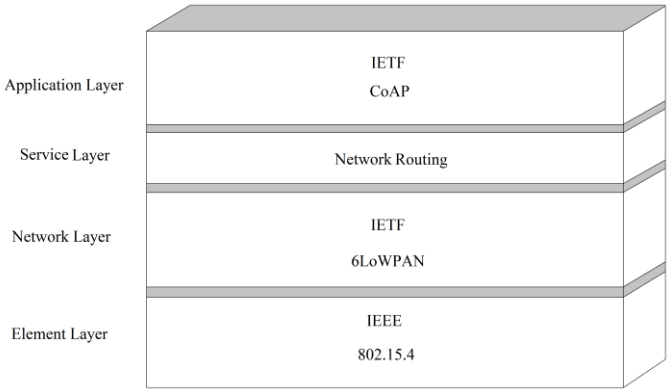

Figure 22. Protocols Used in The Smart Home.

Table 3. Comparing of Existing Security Protocols in the Smart Home Scenario.

Layers	Protocols	Security Services			
Application Layer	IETF CoAP	Confidentiality	Authentication	Integrity	Nonrepudiation
Service Layer	IEEE Routing	Confidentiality	Authentication	Integrity	Key Management
Network Layer	IETF 6LoWPAN	Confidentiality	Authentication	Integrity	Availability
Element Layer	IEEE 802.15.4	Confidentiality	Authentication	Integrity	Access Control

Table 3 shows that most of security services required at each layer are the same except for different mechanisms that will be used in practice.

4.8 Data Flow of the Smart Home Scenario

By considering the corresponding security service module, security mechanism module, and the fundamental security primitive module, we can figure out the data flow in the smart home security management scenario.

(1) The data of the environment information such as temperature, vapor concentration and light intensity are collected by the different sensors. Then the data is processed via a one-way hash function to create a digital signature message, which is invoked by the authentication service management module in the element layer. The IEEE 802.15.4 protocol implements the AES symmetric-key cryptography mechanism to encrypt the data in CCM mode with message authentication code and message integrity code in 32-bit keys.

(2) The data that came from the element layer was encrypted using the symmetric encryption function, which is invoked by the data integrity service management module in

the network layer. The 6LoWPAN protocol implements the low-power and lossy networks (RPL) routing mechanism, which implements the AES with 128-bit keys providing the confidentiality, and integrity security services.

(3) The service layer received the encrypted data and the availability service management module invokes the Network Intrusion Detection System (NIDS) function module to prevent the DoS attack during the transmission through the Internet, WIFI or cellular network.

(4) The authentication service management module in the application layer invokes the key certification authority module to verify the identity of the user by comparing the user profile. Then, the user decrypts the message using the private-key which is provided by the PKI module. The CoAP protocol provides a "request and response" communication model between the end-points and uses the AES as the cryptographic symmetric-key algorithm to provide the security services of confidentiality.

(5) The user now can use the Application Programming Interface (API) on smart phone to monitor the temperature, humidity as well as illumination in the house under the efficient security protection remotely.

Figure 23 shows the data flow of the smart home scenario. The diagram shows the management an IoT entities involve in each layer for the smart home scenario under consideration.

The above scenario illustrates a simplified application. In case of intruders and difficulties, a number of potential problem may occur that need to be resolved. This can easily be resolved if the proposed IoTSMS is in place.

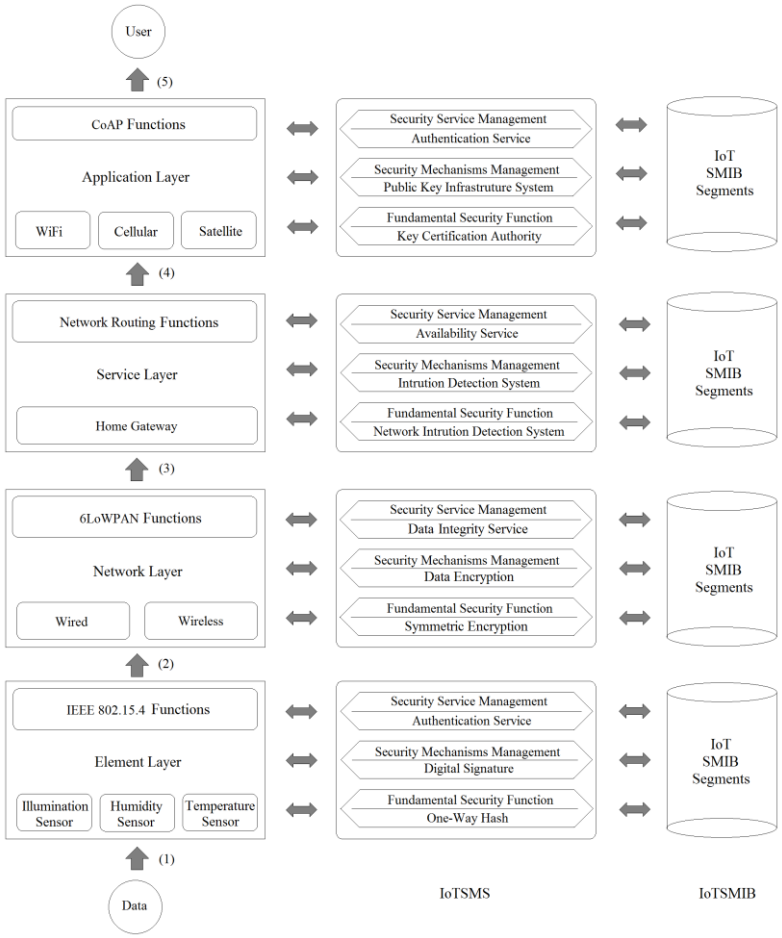

Figure 23. Data Flow of The Smart Home Scenario.

CHAPTER 5

CONCLUSIONS

5.1 Summary

This study begins by reviewing many case studies and research designs for the IoT system. The IoT system is both a function and a state-of-the-art conception for today's IT industry. Many research papers and academic journals have been published that were focused on the security requirements for the IoT system. However, none of them were pointing out to a comprehensive security management system in this environment.

The development of Google automatic drive, wearable and health devices, virtual reality (VR) video games system and amount home network system were the author's motivation to perform this research work.

The first part of this research was all about the conception of the security in the IoT environment as well as the review of the literature to obtain the needed background. The IoT is a new concept that is very vulnerable to the sophisticated cyberattacks using the Internet, telephone, mobile and satellite network systems. The mainly focus, at first, was on understanding these attacks and their point-of-attacks in the IoT system.

The second part of this research was focus on analysis and comprehension of security and techniques used in the IoT system. More specifically, the security protocols, its components and entities needed at each layer of the IoT system architecture have been determined to analyze the vulnerabilities.

The third part of the research was to provide a comprehensive solution for the security problems of the IoT system. In this part of the study a comprehensive autonomous security management system was proposed that it may provide security to multiple applications at

the same time in the IoT environment. The designed IoT security management system (IoTSMS) is a layered functional architecture that consists of many entities or modules. The modular architecture of the IoTSMS provides the capability to secure all layers of the IoT system model against all potential threats and cyberattacks.

5.2 Concluding Remarks

There are number of proposals and patents concerning the security systems and methods for the IoT security. However, to the author's knowledge, most of them describing an incomplete and noncomprehensive system for this purpose; in most cases, they focus on a particular issue and supply a partial solution for a single-piece of the ioT system. The proposed IoTSMS in this study includes the steps of providing a plurality of mechanisms, and linking the services and mechanisms with a plurality of security management functions. The method supports all existing IoT protocols in the IoT system environment. The security functional architecture assumes four functional hierarchical layers, along the same lines as the hierarchical layer model of the IoT system, and including an IoTSMIB (security management information base) segment according to the four security functional layers. Implementation of this IoTSMS facilitates integration of new techniques and technologies.

5.3 Future Work

This study was mainly focused on security management functionalities for the IoT system. The proposed IoTSMS model does not include a particular platform provide and associated platform functionalities. In general, a number of services and network providers are involved in implementation of the IoT system. The optimum implementation of the IoTSMS or its variations suitable for different network platforms need to be investigated as future work in this area.

REFERENCES/BIBLIOGRAPHY

[01] Ovidiu Vermesan, Peter Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystem*. Aalborg, Denmark: River Publishers, 2013.

[02] Punit Gupta, Jasmeet Chhabra, "IoT Based Smart Home Design Using Power and Security Management," *International Conference on Innovation and Challenges in Cyber Security*, pp. 6-10, August 2016.

[03] M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *International Journal of Computer Applications*, vol. 111, pp. 1-4, February 2015.

[04] Ovidiu Vermesan, Peter Friess*, Internet of Things from Research and Innovation to Market Deployment*. Aalborg, Denmark: River Publishers, 2014.

[05] Klaus Finkenzeller, *RFID Handbook Fundamental and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. Wiltshire, UK: John Wiley & Sons, 3rd ed., 2010.

[06] Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "A Survey of Beacon-Enabled IEEE 802.15.4 MAC Protocol in Wireless Sensor Networks," *IEEE Communication Survey & Tutorials*, vol. 16, pp. 856-876, December 2013.

[07] Saniya Vohra, Rohit Srivastava, "A Survey on Techniques for Securing 6LoWPAN," *Fifth International Conference on Communication Systems and Network Technologies*, pp. 643-646, April 2015.

[08] Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, Jesus Alonso-Zarate, "A Survey on Application Layer Protocols for the Internet of Things," *Transaction on IoT and Cloud Computing*, pp. 1-8, April 2015.

[09] Davide Conzon, Thomas Bolognesi, Paolo Brizzi, Antonio Lotito, Riccardo Tomasi, Maurizio A. Spirito, "An XMPP Based Architecture for Secure IoT Communications," *Interational Conference on Computer Communications and Networks,* pp. 1-6, August 2012.

[10] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, pp.1497-1516, September 2012.

[11] Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, pp. 2787-2805, October 2010.

[12] Mr. Ravi Uttarkar and Prof. Raj Kulkarni, "Internet of Things: Architecture and Security," *International Journal of Computer Application*, vol 3, pp. 12-19, June 2014.

[13] Fahandezh, M., "A Framework for IPSec Functional Architecture," MASc Thesis, ECE, Faculty of Grad. Studies and Research, U. Windsor, 2005.

[14] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, "Classification of RFID Attacks," *A Journal of Research and Innovation*, vol. 12, pp. 491-505, November 2010.

[15] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *International Journal of Computer Science and Information Security*, vol 4, pp. 2-7, September 2009.

[16] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges," *International Journal of Computer Science and Information Technology & Security*, vol. 1, pp. 13-18, December 2010.

[17] Priyanka S. Fulare and Nikita Chavhan, "False Data Detection in Wireless Sensor Network with Secure Communication," *International Journal of Smart Sensors and AdHoc Networks*, vol. 1, pp, 66-69, 2011.

[18] Jason R.C Nurse, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, Sadie Creese, "Smart Insiders: Exploring the Threats from Insiders Using the Internet of Things," Secure Internet of Things (SIoT), *International Workshop on Secure Internet of Things*, pp.5-14, September 2015.

[19] Audrey A. Gendreau, Michael Moorman, "Survey of Intrusion Detection System towards an End to End Secure Internet of Things," *IEEE 4th International Conference on Future Internet of Things and Cloud*, pp. 84-90, August 2016.

[20] K. Narasimha Mallikarjunan, K. Muthupriya, S. Mercy Shalinie, "A Survey of Distributed Denial of Service Attack," *International Conference on Intelligent System and Control*, IEEE, pp. 1-6, January 2016.

[21] Amnar Almomani, B. B. Gupta, Samer Atawneh, A. Meulenberg, Eman Almomani, "A Survey of Phising Email Filtering Techniques," *IEEE Communication Survey & Tutorials*, vol. 15, pp. 2070-2090, March 2013.

[22] N. S. Vipin, M. Abdul Nizar, "Efficient On-line SPAM Filtering for Encrypted Message," *IEEE International Conference on Signal Processing, Informatics, Communication and Energy System*, IEEE, pp. 1-5, February 2015.

[23] Reem Abdul Rahman, Babar Shah, "Security analysis of IoT protocols: A focus in CoAP," *MEC International Conference on Big Data and Smart City*, IEEE, pp. 1-7, March 2016.

[24] M. Fahandezh, M. Bondy, S. Erfani, "A Framework For Implementing IPSec Functional Architecture," *Canadian Conference on Electrical & Computer Engineering (CCECE)*, pp. 71-76, May 2009.

[25] James Wiebe, "Implementing IPsec using the Five-Layer Security Framework and FPGAs," MASc Thesis, ECE, Faculty of Grad. Studies and Research, U. Windsor, 2005.

[26] OASIS, "Advancing Open Standards for the Information Society," *published on OASIS (https://www.oasis-open.org),* pp. 1-2, check date November 2016.

[27] ISO/IEC, "Standardization and Related Actives General Vocabulary," ICS, pp. 1-76, 2004.

[28] Jurgen Quittek, Joe Touch, "Recent Advances in IETF Standards," *IEEE Communication Magazine,* vol. 49, pp. 76-77, April 2011.

[29] Lee Stogner, “An Introduction to the Internet of Things from the perspective of the IEEE Internet of Things initiative,” *International Conference on Collaboration Technologies and System*, pp. 506-506, August 2015.

[30] ITU-T SG20: IoT and its application including smart cities and communities (SC&C), Singapore, January 2016.

[31] Muhonen. T, “Standardization of Industrial internet and IoT – perspective on Condition-Based Maintenance,” *University of Oulu, Finland*, pp.2-92, February 2016.

[32] Thread Group, “Thread Overview,” pp. 1-21, 2015.

[33] Ashok Subash, “IoTivity – Connecting Things in IoT,” *TIZEN Developer Summit*, pp. 1-48, July 2015.

APPENDICES

OASIS

The Advancing Open Standards for the Information Society (OASIS) is a non-profit consortium that drives the open standards of global information society. OASIS produces standards for security, the IoT, Cloud computing, energy management, content technologies and emergency management.

OASIS member section includes Advanced Message Queuing Protocol (AMPQ), OASIS Identity and Trusted Infrastructure (IDtrust), OASIS Open Composite Services Architecture (CSA) and OASIS Web Services Interoperability (WS-I). The membership of OASIS are levels include foundational sponsors around the world such as Cryptsoft, IBM and Microsoft, sponsors such as Dell, Hewlett Packard, Intel and TELUS. [26]

ISO

The International Organization for Standard (ISO) was founded on 23 February 1947, the headquartered in Geneva, Switzerland. The ISO is an independent, non-governmental organization. The organization promotes worldwide industrial, proprietary and commercial standards. ISO has 162 national members from 206 total countries in the world. [27]

IEFT

The Internet Engineering Task Force (IETF) develops Internet standards and the Internet protocol suite (TCP/IP). The IETF was supported by the U.S federal government in January 16, 1986. Since 1993 it has operated as an international membership-based non-profit organization. [28]

IEEE

Institute of Electrical and Electronics Engineers (IEEE) is a professional association founded in January 1, 1963. It is the world's largest association of technical professional with more than 400,000 members worldwide. IEEE promotes the educational and technical of electrical and electronic engineering, computer engineering and telecommunications. The IEEE leading the standards development organization such as electric power and energy, biomedical technology and healthcare, information technology, information assurance, telecommunications, consumer electronics, transportation, aerospace, and nanotechnology. [29]

ITU-T Study Group 20

The International Telecommunication Union Study Group 20 was established in June 2015. The ITU-T SG 20 is concerned with designing for smart cities and communities (SC&C). [30]

IEEE P2413 Framework

IEEE Project 2413 covers from the definition of basic IoT architectures to the entire system, IEEE P2413 is an umbrella for many IEEE standards that applying for IoT. There are more than 350 IEEE standards such as IEEE 754, IEEE 802.1AS, IEEE 802.1Q, IEEE 802.1ad, IEEE 802.15.4. [31]

Thread Group

Thread is a very young standard group but also very ambitious, their wireless standard covers networking, power conservation and security. Thread looks forward into the new wireless networking standard could offer the advancement over the ZigBee which is based

on IEEE 802.15.4 standard and Z-Wave which is announced by Z-Wave Alliance. Thread has more than 80 members from industry such as Dell, Huawei, LG and Philips. [32]

Open Interconnect Consortium

The OIC was founded by Intel and released a project called IoTivity, it is a framework for Device-to-Device communication and it is a competitor of AllJoyn. The OIC has more than 100 members such as DLNA (Digital Living Network Alliance) which was established by Sony in June 2003 and UPnP (Universal Plug and Play Forum). [33]

VITA AUCTORIS

NAME:	Long Chen
PLACE OF BIRTH:	Wu Han, China
YEAR OF BIRTH:	1989
EDUCATION:	Wuhan Institute of Technology, B.Sc., Wuhan, Hubei, 2008
	University of Windsor, M.Eng., Windsor, ON, 2013
	University of Windsor, M.Sc., Windsor, ON, 2015