IT SECURITY AND PRIVACY GUIDANCE TOOL

FOR IOT DESIGNS AND PRODUCTS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS OF
THE MIDDLE EAST TECHNICAL UNIVERSITY
BY

MUTLU ERHAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

OCTOBER 2019

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 : Mutlu ERHAN

Signature : _____

ABSTRACT

IT SECURITY AND PRIVACY GUIDANCE TOOL

FOR IOT DESIGNS AND PRODUCTS

Erhan, Mutlu

MSc., Department of Information Systems

Supervisor: Assoc. Prof. Dr. Banu Günel Kılıç

October 2019, 126 pages

Security and privacy issues in the Internet of Things (IoT) have received much attention in recent years because of the attacks, which have increased both in quantity and diversity. Many studies have been done to make the IoT ecosystem more secure, and these have managed to ease some risks partially by presenting security frameworks or basic standards. However; presented frameworks or standards have not been accepted by all the stakeholders in the IoT ecosystem and have not been able to provide solutions for design and evaluation. One way to decrease the risks posed by the vulnerabilities is to increase awareness of the stakeholders for security and privacy issues in the IoT system via providing simple, usable and enough protection skills, methods, standards and framework models in a design and evaluation environment.

Previous studies have analyzed reference framework models, presented security threats as a layered structure and managed to demonstrate the visibility of risks with a model of building blocks. However, besides the demonstration of the general security problems in the IoT stack, little attention was given to the generation of an evaluation environment and its usability. This study aims to present an environment, named as the Secure IoT Design Environment (SIDE), for IoT system developers to evaluate their products security risks against related vulnerabilities and to correct their deficits in the ecosystem, especially at the design phase. It was shown that the SIDE is practical and highly usable in identifying threats related to a design decision and evaluating the security of alternative solutions based on their known vulnerabilities.

Keywords: Internet of Things, Secure IoT, Secure Design, SIDE, IoT Framework

ÖZ

NESNELERİN İNTERNETİ TASARIMLARI VE ÜRÜNLERİ İÇİN BT GÜVENLİĞİ VE GİZLİLİĞİ REHBERLİK ARACI

Erhan, Mutlu

Yüksek Lisans, Bilişim Sistemleri Bölümü

Tez Yöneticisi: Doç. Dr. Banu Günel Kılıç

Ekim 2019, 126 sayfa

Nesnelerin İnternetindeki (Nİ) güvenlik ve gizlilik sorunları, son yıllarda hem miktar hem de çeşitlilik açısından artan saldırılar nedeniyle çok dikkat çekti. Nİ ekosistemini daha güvenli hale getirmek için birçok çalışma yapılmıştır ve bunlar güvenlik çerçeveleri veya temel standartlar sunarak riskleri azaltmayı kısmen başarmıştır. Ancak bu çalışmalarda sunulan çerçeveler veya standartlar Nİ ekosistemindeki tüm paydaşlar tarafından kabul edilmemiştir ve tasarım ve değerlendirme için çözümler sunamamıştır. Güvenlik açıklarının yol açtığı riskleri azaltmanın bir yolu, bir tasarım ve değerlendirme ortamında basit, kullanılabilir ve yeterli koruma becerileri, yöntemleri, standartları ve çerçeve modelleri sağlayarak, paydaşların Nİ sistemindeki güvenlik ve gizlilik sorunları konusundaki farkındalığını artırmaktır.

Daha önce yapılan çalışmalar referans çerçeve modellerini analiz etmiş, güvenlik tehditlerini katmanlı bir yapı olarak sunmuş ve risklerin görünürlüğünü sistemi oluşturan bir yapı taşı modeli ile göstermeyi başarmıştır. Ancak; Nİ yığınındaki genel güvenlik sorunları gösterilmesine rağmen, bir değerlendirme ortamının oluşturulmasına ve kullanılabilirliğine çok az dikkat edilmiştir. Bu çalışma, Nİ sistem geliştiricilerinin ürünlerinin güvenlik risklerini ilgili güvenlik açıkları kapsamında değerlendirmelerine ve özellikle tasarım aşamasında düzeltmelerine yönelik olarak, Güvenli Nİ Tasarım Ortamı (İng. Secure IoT Design Environment), SIDE, olarak adlandırılan bir ortam sunmayı amaçlamaktadır. SIDE'ın bir tasarım kararıyla ilgili tehditleri tespit etmede ve bilinen güvenlik açıklarına dayanarak alternatif çözümlerin güvenliğini değerlendirmede pratik ve son derece kullanışlı olduğu gösterilmiştir.

Anahtar Sözcükler: Nesnelerin İnterneti, Güvenli Nİ, Güvenli Tasarım, Nİ Çerçeve Modeli, SIDE

*Dedicated to **my father and mother** who have raised me and to my **beloved wife** and **sons** with whom I feel the real value of the life.*

ACKNOWLEDGMENTS

First of all, I would like to express my deep gratitude to my supervisor Assoc.Prof. Dr. Banu Günel Kılıç whose knowledge, encouragement, guidance, support and experience have made this thesis possible. Her helpful manner, careful evaluations, constructive feedbacks and high communication skills have opened the doors for me to overcome all the obstacles on my way.

Besides my supervisor, I would like to specially thank Seyyit Alper SERT who have inspired me to study on this topic and have spent lots of time to ignite fruitful ideas in my mind to enrich the content of the thesis.

I would also like to thank all of my colleagues for their help in design, development and test of my application. Also, I am grateful for all the participants who have taken my questionnaire and shared their ideas to make this thesis better. Additionally, my organization and managers deserve a special thank for providing needed permission and support.

I want to present my deep regards and thanks to the valuable members of examining comittee of my thesis, Assoc. Prof. Dr. Altan Koçyiğit and Prof. Dr. Ali Aydın Selçuk, Assoc. Professor Dr. Aysu Betin Can and Asst. Professor Dr. Cihangir Tezcan, whose findings and constructive feedbacks made this thesis more compherensive and more efficient.

Thesis period was hard for us because we have experienced serious health problems during this term in my father-in-law and mother-in-law. That is why my wife deserves the highest thanks, because she has spent lots of effort to encourage me on my study, to support her family and to deal with our beloved sons Umut and Uğur. I appreciate her devotion through my research. Love you much and forever.

Finally, I would like to thank to my family and beloved ones who have always believed in me and prayed for my success.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

6LoWPAN	IP v6 for Low Power and Lossy Wireless Personal Area Network
AH	Authentication Header
APT	Advanced Persistent Threats
CC	Cloud Computing
CDMA	Code Division Multiple Access
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CoAP	Constrained Application Protocol
CPS	Cyber Physical Systems
CSA	Cloud Security Alliance
DDoS	Distributed Denial of Service
DoS	Denial-of-Service
DSL	Digital Subscribers Line
DTLS	Datagram Transport Layer Security
DVR	Digital Video Recorders
ENISA	European Network and Information Security Agency
ESP	Encapsulated Security Payload
FAN	Field Area Network
GIS	Geographic Information Systems
GPS	Global Positioning Systems
GSM	Global System for Mobile
GSMA	Global Systems for Mobile Access
HAN	Home Area Network
IaaS	Infrastructure as a Service
IAS	Information Assurance and Security
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engine Tasking Force
IoT	Internet of Things
IIOT	Industrial Internet of Things
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security
IPv6	Internet Version 6
IS-IS	Intermediate System to Intermediate System
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network

LLNs	Abstract Low-Power and Lossy Networks
LTE	Long-Term Evolution
METU	Middle East Technical University
M2M	Machine-to-Machine
MQTT	Message Queue Telemetry Transport
NAN	Neighborhood Area Network
NAT	Network Address Translation
NB-IOT	Narrow-Band IOT
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OLSP	Optimized Link State Protocol
OSI	Open System Interconnect
OSPF	Open Shortest Path First
PaaS	Platform as a service
REST	Representational State Transfer
RFC	Request for Comment
RFID	Radio Frequency Identification
RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks
SaaS	Software as a Service
SCADA	Supervisory control and data acquisition
SIDE	Secure IoT Design Environment
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User Interface
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access X
WSN	Wireless Sensor Networks
XMPP	Extensible Messaging and Presence Protocol

CHAPTER 1

INTRODUCTION

Many studies have been conducted in the security and privacy in the Internet of Things (IoT) in recent years because of the high number and diversity of the attacks. In 2016 and 2017, Mirai, BASHLITE and Hajime, which are IoT botnets, called thingbots, realized the most significant Distributed Denial of Service (DDoS) attack in the history, since the invention of the Internet[1]. The number of devices which took part in these attacks was above one million, and the amount of traffic load was higher than 1.5 Tbps. Cameras, digital video recorders (DVR), refrigerators, coffee machines and lots of different IoT devices were used in these attacks causing globally essential web sites to be out of service like Amazon, CNN, Github, HBO, Netflix, NY Times, PayPal, Reddit, Spotify and Twitter [1], [2]. Unfortunately, these attacks are just the beginning, not the end, and things will never be the same again. The number of devices connected to the Internet will reach nearly 20 billion by 2020, and the share of the IoT devices in the cyber-attacks will be 25% according to the Gartner report [2]. One of the most significant risks in the IoT is the repurposing of the internet from consumer usage to industry usage, because of the IoT utilization in production lines, transportation, and in many other industry fields. This utilization, i.e., things' connectivity to the internet, has created vulnerabilities in the critical infrastructures and services which can hinder the normal flow of life and result in injuries and deaths.

IoT is the ecosystem of the objects, which have sensing, and computation capabilities, network connectivity, and power to collect, process, and transfer data to a remote server or cloud environment. Besides, IoT is the interconnection of things (daily objects, animals, or human beings carrying these things) in order to realize some specific tasks like monitoring, sensing, detecting, and informing. Thanks to the IoT and its applications in many fields of life, unique benefits have been presented, such as energy saving, efficiency, productivity, comfort, entertainment, and security. Because of these benefits, IoT has found many application fields in transportation, health, wearable technologies, autonomous cars, home\building automation, electricity management, critical infrastructures, and the industry.

Such a wide range of applications maintains a high level of heterogeneity in IoT and increases the diversity of objects [3]. Objects such as temperature sensors, autonomous vehicles, refrigerators, coffee machines, smart meters, and security cameras are called smart objects in the IoT ecosystem. Unfortunately, the capabilities given to these smart objects to perform their tasks are limited, compared to other mainstream Information Technology (IT) devices, such as computers and smartphones. Security measures and standards developed for classic IT devices are not applicable for the IoT objects due to their limitations in network connectivity, processing power, energy, and data storage.

IoT is an extended version of the Machine-to-Machine (M2M) communication and the enabling technologies provide the needed features for it. Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID), cloud computing, actuators-sensors, and their related applications are some of the most critical enabling technologies in the Internet of Things[3]. WSN provides the cheapest and easiest way of communication for IoT, while RFID tags and readers are the most common way to store and receive data on the objects.

Studies have shown that the developmental history of the Internet of Things has similarities to the development of the Internet, but a vast difference in terms of speed and connected devices. Initially, the

researchers had designed the Internet environment for real purposes, such as sending messages between specific points. However, later on, the Internet became an indispensable part of life and entered into many areas from education to entertainment, from health to economy, from logistics and retail to production processes, from the management of critical systems to tracking traffic and flight information. Most of the technology users are using more than one device for achieving some tasks or just for fun. Because of the widespread use of the Internet in many areas other than its original intended use, security considerations were ignored at the design stage. Later on, as a result of losses in attacks carried out by malicious people, measures had to be taken. Because of the many benefits provided by the Internet of Things, it has been adopted by society very quickly and has achieved a high growth rate. While the IoT ecosystem is developing so rapidly, security issues are being ignored. It may be because of the ignorance of the stakeholders of the IoT, or because of the prioritization of cost reduction over security.

The fundamental value that is emphasized and studied on the Internet of Things is confidential data. This data is much larger than the data produced so far and continues to increase rapidly due to advances in processor, chip and network technologies. These data can include personal health data, status data of critical infrastructures, such as dams, ecological status data in environmental places, status information of nuclear power plants and traffic information of smart city management system. This new information environment, huge amount of data and accessibility has created new attack surfaces in addition to innovations and conveniences that have never existed before in these areas and ultimately has taken their place in the history of information technologies as a means and purpose of serious cyber-attacks.

Transformation of the internet from consumer usage to the industry usage have exacerbated the situation in the privacy and security aspects. Application of IoT technologies led to cost reductions in various areas and live data flow facilitating instant decision making, which increased the productivity and efficiency and brought adopting companies far ahead of their competitors. This situation encouraged other companies to start using these technologies as soon as possible. In this transformation, security issues were ignored or essential precautions were not included in the plan and design phases. Besides, the cost reductions in hardware and sensors required for the implementation of IoT technologies have enabled even people with mere knowledge to take part in this ecosystem. Because of their limited knowledge and unawareness about security and privacy issues in IoT, they have focused on product development and completion. As a result, these novice developers and producers have completed development processes without taking the necessary precautions for security and privacy.

Vulnerabilities mean weaknesses in a system or its design that allow an attacker to execute commands, access unauthorized data, or conduct several kinds of attacks like denial-of-service (DoS), Man in the Middle (MITM), DDoS, and industrial espionage [4]. Vulnerabilities can exist in any component of an IoT system, like hardware, software, cloud environment, connectivity, and process and policies used to operate them. Hardware vulnerabilities are usually arising from the production phase, and they are hard to correct, while software vulnerabilities arise from operating systems, firmware, and applications, and they are easy to fix. Vulnerabilities arise due to many reasons. The main reason for the problem is that organizations and companies are not aware of the security risks and threats in the field they are working on. This situation opens the doors for starting projects without needed resource, skills, knowledge and expertise. Based on this ignorance they cannot define requirements, make a comprehensive plan which covers all the security issues. In addition to that, managerial problems of projects, like lack of coordination and communication among members of the development team, make the IoT projects more vulnerable to the attacks and threats.

Misconfiguration of the systems intentionally or by fault causes exposure, which allows an attacker to penetrate the system and get information. Physical tampering is one of the most challenging issues in exposure because most of the IoT systems are left unattended and easily accessible outside. These exposures increase the risk of theft of cryptographic keys, destruction of the device, network loss, malicious node replacement, or node addition under the supervision of the attacker.

A threat is an action which benefits from the vulnerabilities and exposures in the systems and may harm them. The source of the threats can be human beings, nature, or systems. Earthquakes, floods,

hurricanes, and thunders are natural threats which can impede systems to run correctly. In order to protect systems and resume business activities, some precautions like backup, contingency plans should be applied, and disaster sites should be constructed for business-critical systems. Confidentiality, integrity, and availability are the essential security targets in information technology, and natural threats mostly threaten the availability. Human threats belonging to the organization are called intruder or insider, who have some authorization in the systems and tries to conquer the castle inside. Individuals, groups, organizations and even states can be human threats outside the organizations. Also, threats can be categorized as structured or unstructured by the preparation type and used skills\techniques or targets. Novice geeks who are in search of fame and fun are the applier of the unstructured threats. Most of the time, they use off-the-shelf exploits and simple toolkits, which can be found on the internet easily. On the other hand, the architects of the structured threats are the experts of the systems who have a high skill of hacking and deep expertise about the vulnerabilities of the target systems. Advanced Persistent Threats (APT) are the generic name of these structured threats, and Stuxnet in Iran, cyber-attack in Estonia in 2007 or petrochemical attacks in Saudi Arabia in 2017 are some examples of them.

By using the concepts mentioned above, all the events that are made to the systems for specific interests, earnings, reputation, or other reasons and cause them to be out of service are called attacks. The success of the attacker in carrying out these activities depends on the means he uses, the depth of information, and the resistance of the victim systems to the attacks. Security attacks have different motives, such as physical attacks, reconnaissance attacks, and access attacks which are chasing to exploit the security breaches. Data mining, cyber espionage, eavesdropping, tracking are attacks which violate privacy and try to steal critical info or use it. Another classification is dictionary attack and brute force attacks which focus on passwords. Also, attacks with high expertise like cyber-espionage or cyber-vandalism against the critical infrastructures like Stuxnet can be classified as APT's attacks. The last but not least are the trend attacks which have occurred in the late years like ransomware, form-jacking, extended DDos based on IoT botnets, session-hijacking, pass-the-hash, pass-the-ticket, and crypto-jacking attacks [5].

In this period, when the area of attack has expanded so much, and the number of attacks has increased, there is a significant increase in the measures taken. According to the analysis, the financial cost of IoT security incidents can reach to 13.4% of annual revenues for some organizations [6]. According to the survey, 32% of leaders in the IT world regard security as the most significant drawback. By 2020 25% of the security attacks on the Internet will be comprised of IoT attacks while spending in IoT security will stay in the 10% levels [2]. According to the reports, there is an increase in the expenditure on IoT security. In 2017, it was US$ 1.174 billion, and in 2018, it was US$ 1.506 billion. The information system and the academic world are working to create new measures, solutions, standards, and framework models that suit against these increasing threats.

Despite many studies on IoT security, different security needs arise due to the diversity of IoT application areas. The risks, attack surfaces, and degree of protection vary between an intelligent electric meter and an autonomous vehicle or city lighting system. In addition to this difference, the safety criteria and standards that all manufacturers in the world must comply with have not been completed yet. Although different players from different layers of the IoT ecosystem attempt to provide some standards relevant to their fields, they are still at a crawling level. Authorities in the IoT security domain have not proposed a suitable security framework solution for all IoT application areas.

Although there are some solutions for IoT security and the amount of expenditure on this issue has increased, awareness in this area is not at the expected level. One of the reasons for this is the complexity of the components used in the production processes of IoT products and the lack of information about the threats in the IoT ecosystem in general. Various framework model studies have been conducted and have been put into service to explain the structure of the essential components of IoT. However, these applications could not provide solutions for IoT security. They have only introduced and presented a layered architecture on a component basis.
These layers consist of perception or physical layer, protocols related to the connectivity, communication and networks, data, and software. The main difference of this reference model is that it combines its layered architecture with building blocks and presents them with threats against each

building block. In addition to this, it provides information about the attacks that correspond to each asset created, the security aims of these attacks, and the countermeasures that can be taken against these attacks. This study is a unique one in this field, and there is no similar study in the literature. With this study, they have added building blocks to the reference models previously presented only in the layered structure, and thus the visibility of the sub-components has increased. Due to the lack of building blocks, the security issue is considered as a whole. It has enabled to analyze the security risks in the building blocks and asset level. Thanks to the building blocks, there is a new classification of IoT assets as hardware components, protocols, data at rest, and software.

In the IT security world, conventional security targets are divided into three categories as a CIA (Confidentiality, Integrity, Availability) triad. However, increases in attack types have forced to extend these security targets. Researchers in the study [8], have analyzed the attacks in the IT world and has created IAS (Information Assurance and Security)-octave. These security targets consist of confidentiality, integrity, availability, non-repudiation, privacy, auditability, accountability, trustworthiness. In this perspective, a secure object is an object which provides these security targets. A security attack is an attack which compromises any of these security targets.

Although the framework models in the literature have provided a new perspective and new insights in the IoT security aspect they have some drawbacks in usage. For example, every asset is evaluated separately and they do not provide an interface to evaluate a product with its whole components. In order to reach attack definitions or counter measures you have to make manual work. Besides, because these models cover issues between 2000 and 2017, it lacks some up-to-date attacks and solutions. These models in the studies also have a static environment and addition of new updates is not possible.

In our study, there are different interfaces, which can provide evaluation of the products against security vulnerabilities and risks. Evaluators may test their systems or products with their subcomponents via selecting from checkboxes or keyword search. New threats and solutions that appeared in the literature between 2017 and 2019 and were not included in previous studies are also included in our study. The design environment called as SIDE is dynamic enough to add new threats, solutions and technological innovations to be proposed by users.

1.1. Aim And Objectives

This study aims to provide a design environment for developers and producers in the IoT ecosystem to evaluate their products against the vulnerabilities and threats to correct their deficits and make their products more secure. In order to achieve this aim, the objectives of this study are

- To collect data related to the IoT security and privacy, IoT applications fields and enabling technologies for IoT, through literature review.
- To analyze existing standards, frameworks, and models in the collected data.
- To compare with each other the building blocks of the frameworks, standards, and sub-components of the IoT ecosystem to find the most suitable ones for the design environment.
- To develop a user-friendly, dynamic web application, which considers the current threats, countermeasures, and compromised security targets.
- To evaluate IoT applications in different domains in the developed design environment to test the applicability of web applications.

- To validate the usability and usefulness of the developed design by expert evaluation which will be conducted by a group of test users who are experts in the area.

1.2. Contributions

There is no design environment for evaluating IoT products' security strength against malicious attacks in the literature. This study provides an easy to use online web application for IoT stakeholders to evaluate their designs or products to correct their security deficits considering the up-to-date threats and attacks related to IoT. In order to keep the system up-to-date a collaboration need seems as a must. This application can provide knowledge sharing environment related to the IoT security and privacy and if accepted by a certain amount of people, this system could be placed for collaboration.

1.3. Scope and Limitations

This study focuses on providing a design environment for the IoT community to evaluate their products against the threats in the IoT ecosystem and produce more secure products. In order to achieve this aim, books, journals, conference papers, reports, and white papers were analyzed. A systematic mapping like mentioned in the reference [9] were used to collect and combine the materials. In order to create a visible map, literature was reviewed by some defined keywords like "IoT security", "IoT countermeasures", "Standards and framework models for IoT", "IoT application fields", "IoT security goals", "IoT privacy", and "attacks on IoT" "IoT security challenges" between year 2000 and May 2019. As an exclusion relevant literature which did not include these keywords or which were published after May 2019 might have been missed. However, SIDE offers users and researchers a way of updating by entering relevant data.

Although, frameworks and the models were the specific targets of interest, this study is not in search of offering a model. Instead, it aims to create an evaluation environment based on the existing data.

1.4. Target audience

This study can be useful for the designers, developers, and producers of IoT who are searching for an environment for evaluating their product's resilience against the cyber-security threats in every phase of their production. Researchers in the IoT security domain can benefit from this study as a collection of information about the latest threats in the IoT ecosystem and solutions. They can test IoT application, products, processes in our application, and use their results in their studies. Also, CISOs can use SIDE as a guide or control list to test their IoT environment's security.

1.5. Structure of the Thesis

The structure and flow of the thesis is as follows. In Chapter 2, there is background information related to the general concepts of IoT. This chapter begins with the general definition of IoT, followed by its main components, enabling technologies which the IoT is comprised of, protocols used for data transfer and presentation. This chapter also discusses the application fields of IoT in detail for some selected ones like "Smart Home", "Industrial IoT", "Smart City", "Wearable Technology", and "Smart Energy". At the end of the second chapter, readers can find the standards and framework models developed for the IoT.

The methodology is provided in Chapter 3. This chapter explains the methods used in the study together with their justification. It outlines how the data was collected, classified, and reviewed for the research. This chapter also makes an introduction to the development of the application. Use cases, components

and requirements would be shared also in Chapter 3. Methodology chapter ends with the validation process of the thesis. In Chapter 4, phases and steps for the development of the web application and its essential characteristics are provided. This chapter also describes the necessary tests performed during development of the application. In Chapter 5, the results obtained from the evaluation study to determine the performance of the developed environment are presented in detail. Conclusions are drawn in Chapter 6. New opportunities for future work are also given in this chapter.

CHAPTER 2

OVERVIEW OF THE IOT ENVIRONMENT, TECHNOLOGIES, PROTOCOLS AND FRAMEWORKS

IoT consists of many different components and technologies. Therefore, in this chapter, it is aimed to give general information about the IoT's basic structure and its components. Threats to the IoT security considering their application areas will be the focus of examination.

In the first section, the concept of IoT, its essential components, and the changes it can bring in daily life is elaborated. In the second section, the readers can find the leading technologies and most commonly used protocols in the IoT infrastructure. In order to better understand the IoT environment, the leading IoT applications, their facilities, economic benefits, and opportunities are provided in the third section based on the market share and the devices produced. It is easily observable that the lack of standards related to the topics for security and privacy in IoT is one of the biggest problems for the IoT ecosystem. In order to show the latest situation about the standards in IoT and subcomponents, the fourth section focuses on the standards and the various organizations which have published them. Finally, the last section of this chapter is the evaluation of framework and reference models which have focused on IoT stack and its security.

2.1. What is IoT

IoT is an ecosystem that enables the collection of data from objects, monitoring of the environment according to the determined criteria and performing some tasks thanks to the sensor, energy, network connection and computational power added to them. These objects, equipped with some new abilities, are called smart objects. Adding intellect to objects is not a new process, and this concept was first used by Kevin Ashton in a presentation at Protector & Gamble in 1999 [10]. However, this concept is now expressed as the Internet of Everything because it can be applied not only to objects, but to all beings.

The main components of the IoT ecosystem, which are generally called smart objects, should have a physical presence, communication facilities, some necessary computing capabilities, can be uniquely identifiable and can interact with its environment [11]. There is a need for accessibility, communication, network connections, local or remote data storage space for smart devices or objects to achieve particular activities. Also, they need an operating system, software, and firmware to manage the processes and to interact with the user via interfaces.

The main reason why IoT has so much space in our lives is its benefits. Essentially, IoT brings capabilities such as comfort, savings, intelligent planning, security, and autonomy. Thanks to the developed applications, savings have increased severely in many areas, and reaction times have decreased in decision making, and some obstacles like physical distance have disappeared.

With the expectation that it will provide a solution to the problems experienced, IoT has been adopted very rapidly by the business world as an innovation move. For those who have not yet applied the IoT, the catalyst effect has been created through the benefits obtained in various fields of application. IoT provides efficiency in resource usage, reduces human efforts for routine activities, lowers cost and increase productivity, enables real-time monitoring and data collection, eases the decision-making process, provides a better user and customer experience [12]–[14].

2.2. Enabling Technologies

In order to understand the rapid development of the IoT infrastructure and to understand the security events that may occur in this infrastructure, it is beneficial to know the necessary components. These essential components are the result of increasing technological developments in network, chip, and battery technology. Thus, they have led to the rapid development of the RFID, WSN technologies, and eventually, the rapid development of the IoT ecosystem.

The development of IoT has been through the rapid advances in certain areas of the technology. At the beginning of these advances, the decrease in the size of the chip technologies and the increase in the processing power can be given. In addition to this, the production of new batteries, which can last longer and renew its energy with different renewable energy sources, can be considered as another factor. IoT can be defined as the integration of passive sensors and embedded devices on the Internet [20]. In this regard, four basic technologies will be discussed in this section. These are Internet Version 6 (IPv6), Radio Frequency Identification (RFID), wireless sensor networks (WSN) and cloud computing (CC). Some other technologies that are not mentioned in this section, but are used in the IoT environment can be listed as sensor devices, near field communication (NFC), global positioning systems (GPS) service-based architecture, geographic information systems (GIS) and mobile cellular devices [21]. A new technology, called "Fog Computing", which is caused by the necessity of performing some operations locally can also be included as one of the technologies used in the IoT ecosystem [15].

2.2.1. Internet Protocol Version 6 (IP v6)

Any entity on the Internet must be uniquely identifiable to communicate with another entity. In the classic IT infrastructure, this requirement was provided by Internet Protocol version 4. However, advances in technology and rapid increase in the number of devices have caused difficulties in the identification of new devices. Initially, this distress was solved by NAT technology, which uses devices such as modems, routers, and firewalls that are located in home or corporate environments. Thanks to these devices, special addresses have been assigned to the devices in the internal network and the process has been managed by using global addresses to the external world-speaking interfaces. Under IP v4 scheme, only 2^{32} devices can be addressed, which is about 4.3 billion. Due to the increasing number of computers, smart phones, tablets and finally IoT devices, the IPv4 schema has become insufficient. The fact that the number of devices connected to the internet will reach to 50 billion, especially in 2020, indicates the inadequacy of this existing IP v4 pool [16]. Internet Engine Tasking Force (IETF) IETF has predicted this situation 21 years ago in 1998 and the newest version of the Internet protocol IP v6 scheme with 2^{128} address spaces was introduced.

2.2.2. Radio Frequency Identification (RFID)

RFID is another key enabling technology which is used in many IoT devices and applications. Generally, RFID technology is composed of two devices: RFID tags and RFID readers [17]. An RFID tag is a unit attached to a device that is wanted to be monitored or tracked or collect information. An RFID reader is a unit which can sense the availability of an RFID and read the information kept on it. Radio waves and electromagnetic fields are used by RFID readers to sense and get information.

RFID tags can be classified into three categories according to their energy sources. These are named passive, semi-active and active. Passive RFID tags do not have energy on their own. They are energized via modification of the electromagnetic wave which is sent by the RFID reader in order to obtain information embedded in the sensor [18]. Semi-active devices have their own energy supply, but need energy which is created by the electromagnetic wave transformation during the information querying phase. Active tags have their own batteries to advertise themselves and communicate with the reader. Passive tags are more eligible for IoT applications because of their energy efficiency.

2.3.1. Network Layer Protocols

IP v6, which has been analyzed in detail in the previous section, is the basic network protocol used for IoT network layer, on which 6LoWPAN (IP v6 for Low Power and Lossy Wireless Personal Area Network) and RPL (Routing Protocol for Low Power and Lossy) protocols operate for different purposes. Only, these two protocols and IPSEC, which is used for secure encapsulation of IP packets will be discussed further.

2.3.1.1. 6LoWPAN

6LoWPAN, created by the Internet Infrastructure Task Force (IETF), is an extension of the internet protocol running over IP v6, allowing limited devices to send and receive information to/from other devices on the Internet. IoT devices have limited processing power to meet the additional overheads created by the Internet protocol and 6LoWPAN handles this obstacle thanks to its encapsulation and packet header compression mechanisms [27].

6LoWPAN is the basic protocol used for IoT applications and has several advantages to offer. 6LowPAN, which has support for TCP, UDP, HTTP, COAP and many IoT application protocols is an open-standard protocol which enables end-to-end communication of IoT devices and other devices on the Internet. Mesh routing support enables one-to-many and many-to-one routing scenarios, and provides a more robust network topology. In addition, thanks to its generic structure, Bluetooth, Wi-Fi and RF support up to 1 GHz or 2.4 GHz band supports many wireless physical communication layers. Although security support is not included in this protocol, this requirement is provided through the IPSEC protocol. RPL protocol is used for routing purposes.

2.3.1.2. RPL

RPL proposed by the IETF is a routing protocol developed for the IoT ecosystem [28]. This protocol has been developed specifically for low-energy and lossy networks utilizing the distance vector algorithm used on IP v6 networks [28], [29]. RPL has three different routings support, from point-to-point, multi-point-to-point and point-to-multipoint. It is a very energy-saving protocol thanks to the mechanism combining control traffic with data traffic. For this reason, RPL is preferred for IoT environment instead of OSPF, IS-IS, OLSR protocols used in the network layer in the Internet environment.

2.3.1.3. IPSEC

IPSEC is the IP protocol used to ensure the confidentiality, security and integrity of data in communication established between two or more points on unsafe IT networks and authentication of communication partners. By dealing security issues in the network layer and providing security services in a transparent manner, IPSEC saves application developers to implement different security solutions at different layers and different implementations [30]. IPSEC protocol consists of two phases in general and is applied in five steps. The formation stages can be named as the establishment of the security unity and then the transmission of the data, the implementation stages of the tunnel formation, IKE Phase-1, IKE Phase-2, data transfer and the termination of the tunnel.

In the IPSEC protocol, IKEv2 is often used to create a security association. Once the security union has been established, the data to be transmitted through the keys occurring in the previous stage is encrypted and transmitted. Since IPSEC has four different protocols such as ESP, AH, IKE and ISAKMP, it can be run in different modes for different purposes. In Authentication Header (AH) mode, the

confidentiality of the data is protected by Encapsulated Security Payload (ESP) mode while ensuring the integrity of the package. While the IKE mode is responsible for key exchange policies, the ISAKMP mode manages the security association process. Generally, the IPSEC protocol is used in conjunction with the ESP protocol and the AH protocol, combined with the ESP protocol and the AH protocol. It is the most widely used protocol for the Virtual Private Network facility in the current Internet environment [19] [30][31].

The main feature expected from the security mechanisms used in the IoT environment is that the cryptographic operations are light but the level of protection is high. When the IPSEC protocol is examined, it is not possible to use it in every IoT application due to additional loads. In this context, DTLS is preferred more because it contains lighter cryptographic operations than the IPSEC protocol [22].

2.3.2. Transport Layer Protocols

In this layer, TCP protocol is used for reliable communication and UPD protocol is used for unreliable communication. The purpose of this section is to examine the TLS and DTLS security protocols applied on TCP and UDP transport layer protocols, respectively and to introduce their advantages and disadvantages.

2.3.2.1. TLS ve DTLS Security Protocols

The TLS protocol is used with secure reliable connection protocols, such as TCP. The security, confidentiality and integrity of the TLS communication layer ensures that the communication is not stolen, tampered or eavesdropped. In the TLS protocol, as in the IPSEC protocol, generally shared public keys are used for the establishment of a secure communication channel by two IT objects. Although TLS provides these services in terms of security, it causes excessive resource consumption due to the overhead in encryption and decryption process. Therefore, it is not available for IoT objects with limited power. In addition to the lossy and low-energy IoT applications, TLS supports the reliable TCP protocol.

UDP protocol is used in IoT applications mostly due to its lower overhead than TCP. It is more suited to applications for which packet losses or disturbances to the package order are not too important. The safety of the UDP protocol used in the transport layer of the IoT protocol is met by DTLS, which is based on TLS. DTLS provides privacy, security and integrity to prevent attacks on the packet communication environment, such as stealing, modifying or listening to data.

2.3.3. Application Layer Protocols

In this section most known and used IoT application layer protocols will be analyzed based upon the services provided by them. General overview of these services can be seen in Table 2-2 [32]. Application-level protocols enable organizations to transmit the information gathered by sensors running in GSM or wireless communication infrastructures shown in Figure 2-1 to a server located in their system halls or in a cloud service provider environment. However, these protocols enable users to monitor updated information from sensors by smart devices or computers. It also allows user-modified command and configuration updates to be transmitted to the sensors.

Table 2-2 Comparison of IoT Application Protocols [32]

		COAP	MQTT	XMPP	REST	AMQP	Web Socket
Data Carrier Protocol	UDP	*					
	TCP		*	*		*	*
	HTTP				*		
QoS	Yes	*	*			*	
	No			*	*		*
Communication Method	Request/Response	*	*	*			
	Publish/Subscribe		*			*	*
	Client/Server						*
Security	TLS		*	*			
	DTLS	*				*	
	HTTPS				*		

2.3.3.1. Constrained Application Protocol (CoAP)

CoAP is an application layer protocol developed by IETF for devices with limited energy that can run in client server architecture, allowing request and response flow [37], [38]. This protocol has been developed specifically for the machine-to-machine IoT ecosystem including smart home systems, smart energy, smart city and smart building applications [39]. This protocol has an interface that can talk with the http protocol, because it is developed based on a limited set of commands that contain the basic features of the http protocol [35], [40]. It facilitates access to the requested resource as it specifies the resources on the devices with URI addresses as in the http protocol [40].

In contrast to the HTTP program working on the TCP protocol that provides secure communication, the greatest advantage of the CoAP protocol running on the UDP protocol is that it does not carry additional loads due to TCP [35], [40]. Nevertheless, in addition to the ability to provide reliable communication with the authorization messages contained in the packet header, the CoAP protocol also allows for device discovery [35], [37]. The CoAP protocol also differs from the http protocol with support for unicast and multi cast traffic [40].

The CoAP protocol, which does not have an integrated security mechanism in itself, uses the DTLS protocol running on UDP for security purposes [35] [40]. The DTLS protocol provides authentication, confidentiality, automatic key management, and cryptographic algorithms [38]. Although it offers security services, DTLS protocol is not designed specifically for IoT environments, and it may cause some difficulties in communication interfaces with other application layer protocols. One of the biggest shortcomings of DTLS is that it does not support multicast traffic, which is one of the biggest advantages of the CoAP protocol. [38] However, the DTLS protocol requires a handshake process at the outset for

a secure communication channel, which leads to a shorter discharging of the batteries in less energy [41]. Another protocol that can be used to ensure the security of the CoAP protocol other than DTLS is the IPsec protocol, but there is no recommendation by the IETF for the use of the IPSec protocol with CoAP [31][32][33].

2.3.3.2. Message Queue Telemetry Transport (MQTT)

MQTT protocol is an application level protocol developed by IBM in 1999 for devices operating on restricted network bandwidth [34]. It is one of the most common protocols in the IoT ecosystem with CoAP protocol. Unlike the CoAP protocol, the MQTT protocol works on the TCP protocol. The MQTT protocol, which works in the substructure of architecture-propagation-subscriber, is in an asynchronous messaging application protocol [34], [35].

In the MQTT infrastructure, the messaging process between the subscriber and the publisher is managed by the component called a broker. Broker sends the messages received from the publishers to the subscribers with the address information. Since there is no obligation to be connected at the same time between the publisher and the subscriber, the energy losses in access distortions in the connection phase can be prevented.

The MQTT protocol does not include an integrated security mechanism. For security purposes, it uses SSL / TLS protocol running on TCP. A username and password mechanism can be used in order to provide security by the broker server for both publisher and subscriber [35], [36].

Despite the fact that MQTT runs over TCP protocol it has lower overheads than CoAP. It is not necessary to respond like other application protocols running over TCP which saves lots of energy on battery-run devices.

2.3.3.3. Extensible Messaging and Presence Protocol (XMPP)

XMPP is developed by IETF for the real time applications like chatting and message exchange. It has support for both publish-subscribe and request-response methods [35]. Although it is used commonly in the Internet applications shortcomings for new technology needs caused this protocol not to be supported by Google [37].

XMPP protocol runs on TCP protocol stack and it has additional overhead because of XML parsing process. Lack of QoS mechanism makes this protocol less efficient for IoT applications than CoAP and MQTT.

XMPP protocol has built-in security support in protocol specification. However, it does not provide QoS options that make it impractical for M2M communications. TCP based TLS/SSL protocol is used for security [35].

2.3.3.4. RESTFUL Services

The Representational State Transfer (REST) is a style or architecture and was published by Roy Fielding 19 years ago. Since 2000, it has been used by applications on different platforms.

REST has a simple architecture and uses basic htpp “GET”, “POST”, “PUT”, and “DELETE” methods to achieve messaging. As it is a kind of http protocol, it uses the request-response mechanism. REST

2.4.2. Smart Home System (Home Automation)

Smart home systems are one of the trendy IoT application areas of the last period that allow access, monitoring and control of the homes on the internet by adding various sensors and network connectivity to everyday devices. Appliances and devices in smart home systems can communicate with other devices in the house, remote server and smart phone or tablet devices and exchange data. Energy saving, security and comfort are the main capabilities offered by intelligent home systems for household residents. It is one of the most preferred IoT applications, especially due to the energy savings it provides in lighting, heating and cooling.

There is a coordinator, called hub providing an interface for the outer world, in the communication of the household appliances. Household appliances, security cameras, doors and garage locks in smart home systems use different network protocols to talk to the hub and exchange data. Some of these network components include Wi-Fi, Bluetooth LE, ZigBee, Z-Wave, Thread, NFC, and RFID [48]. The energy needs of the smart home system devices, both inside and outside the home, can be met from the mains power, the batteries on them, or from renewable energy sources such as solar energy [49].

In smart home systems, a learning system analyzes the behavior of the people living in the home and offers a more comfortable, fun and energy-saving life. In fact, the basic behavior expected from smart home systems is to automate the optimized results according to the input received [50]. Although this automation seems to be one of the most advantageous components of smart home systems, the intense collection of information from residents can offer a very large attack surface for security and privacy violations. Security is considered by customers as one of the biggest obstacles to the use of the smart home system [51].

Smart home applications allow remote access to the appliances like refrigerator or thermostat, as well as opening and closing the door of your home or garage remotely. It is not a critical problem that the smart coffee machine is closed for access from the internet, but it may be considered critical if the smart lock system is out of service or is taken over by malicious people. Therefore, the criticality of smart home systems is considered to be high.

2.4.3. Wearable Technology

Wearable technology is one of the fastest adapters of IoT applications. Smart wristbands, watches, clothes and other additional sensors, which have become widespread recently, can provide meaningful information about the activities of patients, athletes or normal users. Nowadays, rapidly developing chip technologies can create new wearable sensors for early warning and preventive treatment.

Wearable clothing can offer a pro-active state to the potential serious health problems that babies may experience in their early stages. Alarms can be generated through sensors for scenarios such as high fever or sudden exhalation, which cannot be detected without parental supervision. With early intervention, the lives of babies can be saved or this situation can be overcome with less damage.

Wearable technology not only transmits information to users' clock screens or smart devices, but can also transfer data in the cloud environment, creating recordable media and historical information about the user's activities. The collected activity information can be valued with intelligent analysis applications and produce meaningful information and present findings. These records can be used by physicians to monitor the patient remotely and to intervene when necessary.

The sensors in wearable technology are integrated with some triggers and can be used in the treatment of chronic diseases such as diabetes and high blood pressure. In other words, for a bedridden patient with increased sugar level, insulin injections can be performed according to the triggering values created for certain values according to the information received from the sensors.

Wearable technology can be used not only for people but also for devices and industrial areas. In order to monitor the accuracy of the precision measuring devices, sensors are placed and a continuous data flow is provided. Sensors to be worn in mining areas or in industrial areas where chemical gases are used can alert the users early on the presence of temperature, pressure and toxic gases in the environment. In addition, the wakefulness of long-distance drivers can be determined by some of the worn technologies, and the centers that follow these vehicles can be stimulated and the drivers can be awakened by mechanisms such as alarms, vibrations or electrical signals. Medical personnel who deal with patients in the medical field can easily see whether they have infections before approaching patients through smart gloves. Wearable technology can be used to protect the people working in potentially life threatening fields like soldiers, firemen, space and deep sea explorers [52].

Sensors used in wearable technologies generally use RFID technology in data communication infrastructure. The RFID ecosystem consists of a unique tags containing embedded information for objects and readers which can read and understand the information contained therein. Information collected by the RFID readers from tags are transmitted via Bluetooth, Wi-Fi or Zigbee protocols to the local storage or cloud environment and also to the monitoring devices of the users.

Wearable technology, which has application areas in preventive health, in particular, carries great risks to security and privacy [52]. The information collected and processed in this environment is personal information, so privacy must be ensured. The data collected, processed and transmitted in the system must be encrypted, protected and verified for the purpose of presenting the obtained items according to the principle of the need to know. Since many applications are real-time, the availability of the environments in which these systems are processed should be kept at the highest level. In addition, the scenarios such as seizing the devices used in the systems, changing their configuration, manipulating the collected information can often create consequences that can endanger human life. For this reason, it is imperative that each component in the network infrastructure, storage or applications should be secured. The criticality of wearable technology is evaluated to be high due to the above-mentioned reasons.

2.4.4. Smart Energy (Smart Grid and Smart Meter)

The design of the energy networks has been made according to the needs of the 1900s and generally solved by local energy sources. In this structure, where energy flow is provided one way, the end users have no information about the energy resources and the energy resources have no information about the end user. Increasing energy needs in 21 century made it necessary to establish a structure that is more intelligent, economic, safe and sustainable.

The energy distribution networks are called grid and they are composed of energy production sources, intermediate distribution points, transmission lines and end users. At the time when the energy networks were first established, because of the lower energy requirements, a simpler and often one-way transmission line was sufficient, but due to the increasing energy requirement, a mesh structure was established. Thanks to the developments in technology, new sensors, computers and smart measuring devices were added to these elements to provide a two-way flow of information and real-time and instantaneous measurement of the needs provided more intelligent energy solutions.

Recently, there has been a very rapid increase in the production of alternative energy by means of solar and wind as well as classical power generation processes produced by hydroelectric power plants, natural gas, diesel and nuclear energy sources [56]. In this way, houses or workplaces have come to a level that they not only use the energy from the external source, but also use their own energy and even they sell their increased energy to the state or the private sector.

Intelligent measurements from smart homes, buildings and in-home networks can primarily show the energy map in real time. Thanks to this information, smart home appliances can be connected to the intelligent energy measurement system in smart homes and the user's energy costs can be saved significantly. As a result of the developments in the vehicle technology and the large increase in recent years, electric vehicles can be connected to the home area network. In light of the information obtained from the smart measuring devices, the electric vehicles can be charged at low energy costs and a significant saving in user bills can be achieved.

Intelligent grid systems are able to detect real-time energy needs thanks to the new infrastructure it has, and can instantly detect the interruptions in energy networks and direct energy needs in different ways. The energy production process obtained from wind power plants and solar panels, which are highly dependent on weather conditions, are continuously monitored and accordingly production in classical power plants is increased or decreased. The electricity generated by users is measured by smart devices and the difference between consumption and production is reflected in the invoices.

Smart energy networks consist of the Home Area Network (HAN), the Neighborhood Area Network (NAN), the Field Area Network (FAN) and the Wide Area Network (WAN). The Home-Plug protocol, ZigBee, Z-Wave, Bluetooth and 802.15.4 protocols are used in the Home Area Network. The connection between the end user and NAN and FAN can be done via Wi-Fi, DSL, WiMAX, fiber lines or GSM [58].

Smart grids that bring many innovations in terms of savings, flexibility and continuity can breed new security threats. By exploiting the weaknesses in this structure cyber-attacks on smart grids can make a huge burden on the energy lines, making the systems ineffective and causing power outages throughout the country or even throughout a continent [57][59] . In this respect, the level of criticism of these systems was evaluated as high.

2.4.5. Industrial Internet of Things (IIOT)

IIoT can be defined as the use of IoT in production, logistics, oil, gas, transportation, energy, utilities, mining, aviation and other industrial sectors in order to achieve certain targets. An IIoT system is the environment of connection and integration of industrial control systems with operational technology, business processes and data analytics [62].

Although IoT is mainly used to improve end-user life, energy saving and comfort in consumer products, IIoT is used in industry to improve production processes. Equipped with sensors, actuators, internet access and business intelligence software used in industrial environment, whole production process can be monitored, managed and restructured as necessary.

The main purpose of the use of smart devices in IIoT is to collect, transfer and process information from systems and produce meaningful results. These results and meaningful reports allow continuous monitoring of production processes and environments. Monitoring the general state of the systems and operating the alarms and alerts correctly can be considered as another usage scenario. Supporting decision-making processes to assist the predictive maintenance process, which has recently become popular in the industry, is another scenario. One of the other scenarios is the management of systems of operational technologies (OT) that are completely isolated from the IT environment, or partially isolated or segmented by different IT technologies.

Improvements in many areas of the industry by using IIoT have led to an increase in the amount of investments made in this field day by day and new application areas have emerged. According to the study conducted by Morgan Stanley, the market share of IIoT is expected to reach 121 billion dollars in 2021 and the impact on the economy in 2030 is 14.2 trillion dollars [63]. Increasing productivity, creating new business opportunities, reducing inactivity of systems, increasing the utilization rate of existing assets, marketing products as a service, increasing depreciation and life cycle costs, and increasing customer satisfaction are among the main objectives of IIoT. In this way, significant reductions in costs, increase in efficiency, higher utilization and operation of the systems and increasing the competitive power are the main benefits. Companies, which are far from this technology in their industry, lose their competitiveness and remain behind their competitors.

The necessary network connections in IIoT systems are met with different technologies. In mission-critical systems of operational technology (OT) side, serial control interfaces (such as RS-232, RS485 or USB) with more controlled and low connection speeds are one option and wired connection like Ethernet is another. In order to collect information from production environments and devices, wireless communication protocols such as ZigBee, Bluetooth and NFC are used throughout the systems. The connections of the systems to the Internet are made via Cellular networks (GSM, LTE, CDMA), Licensed RF / Radio Spectrum Wi-Fi networks (IEEE 802.11, ISA100) or wired networks. The collected information is usually transferred to a cloud environment and stored. In these cloud environments, business intelligence software and analysis tools are run for producing meaningful reports and results based on the processed data [60].

Despite the fact that it offers many benefits, there are a bunch of threats and attack surfaces, which have been introduced by IIoT. Cyber-attacks against connected assets can result in the loss of intellectual property; the loss of production through disruption or damage to the physical equipment, systems and products, huge financial losses, and serious injuries or death. Orchestrating meaningful network communication across a variety of endpoints can be challenging, especially when proprietary protocols and vendor-specific implementations still overlay open standards, making interoperability complicated, if not unachievable. IIoT appears to be a rapidly growing field in the IoT ecosystem and a new branch of activity [64]. Every new connection expands an attack surface to the IIoT solution and other systems with which it interacts. Research reveals that many IT people who are responsible from IT security of IIoT expects 20% increase in attacks based on IIoT. Only ransomware type attacks have shown an increase by 23% in 2018.

Industrial smart systems can be called as Cyber Physical Systems (CPSs) with their most prevalent applications in different industrial domains like smart transportation, smart grids, smart medical and e-healthcare, and many more. Supervisory control and data acquisition (SCADA) systems are generally used in the backbone infrastructure of CPS to control and monitor their critical infrastructure (CI) [65]. These SCADA systems which have been positioned in some mission-critical systems like chemical industry, nuclear power plants, energy sectors, water plants, space communication, civil administration and transport have higher risk factors and more catastrophic results based on the experienced attacks. Attacks targeted to the SCADA systems have been started in 1982 by Siberian pipeline explosion. In 2000, a water plant in Mariachi Shire area of Australia was hacked by a former worker and caused floods in the area. One of the most famous attacks is STUXNET which had targeted Iranian nuclear power plant and achieved to block or postpone Iranian uranium enrichment project. Triton, which was a very sophisticated attack targeting industrial control systems produced by Schneider Electric company and used in 18000 locations all around the world, was conducted in 2017 against Saudi Arabia petrochemical plant to trigger an explosion and make it out of service [66].

IIoT devices are vulnerable to IoT specific attacks and if compromised, may have a more serious impact than compromised commercial IoT devices [64]. These results can be explosions, floods, chemical gas leakages and destruction of critical infrastructure. These results may cause lots of deaths and serious

injuries. Therefore, criticality of these systems was evaluated as high. If legacy design patterns are used in the IIoT system devices, serious security and privacy concerns are possible in the next decades. It is why security problems should be solved by the security-by-design approach [64].

2.5. Standards and Organizations

After analyzing several resources, articles, and whitepapers to understand the basics of the IoT ecosystem, root causes of the problem areas and possible solutions, it has become clear that the main problem area for the IoT was the diversity of the devices and lack of standards to obey in the IoT community. There are many organizations, which have developed, offered, and used their standards for their domain, but there is no authority on top of the community, which organizes the rules and enforces standards. For the presentation of the current scene , this section will analyze organizations and common standards. Although many researchers have demonstrated common protocols like Wi-Fi, RFID, and RPL in their studies focusing on the standards, this section will not analyze these protocols as Section 2.2 has examined them already.

2.5.1. GSMA (Global Systems for Mobile Access)

GSMA has focused on providing guidelines for secure design, implementation, development and production of IoT products. Besides, in order to evaluate products in the context of security, it has developed a security assessment document, too. In their studies they have presented solutions for different ecosystems like service, endpoint and network. In their latest work, they have implemented their point of view with a case study related to the harbors of the future. GSMA has developed new mobile technology standards with the name of NB-IOT and LTE-M which uses mobile network infrastructure and enable IoT devices to communicate with less energy consumption [67].

2.5.2. European Network and Information Security Agency (ENISA)

ENISA follows different approaches to mitigate the security risks in the IoT infrastructure, like security standard gap analysis, online tools to evaluate products in specific application domains, and baseline security recommendations. In their security standard gap analysis work, they have focused on adapting the current security standards to the IoT and to determine the blank areas, which need new standards to cover security problems. Online analysis tool presents their experience in the previous studies in specific application domains like smart home, smart city, intelligent public transport, smart grid, smart cars, smart airport, e-health, and smart hospitals [68], [69]. Baseline security recommendation is a comprehensive work and forerunner for the other studies because ENISA has published the other documents after this study. Besides, the feedbacks and learned lessons from this baseline has played a role as input for the other documents. They have aimed to provide a security insight for the IoT stakeholders to create their products with security awareness starting from the design phase. It also has some comprehensive work for the convergence of the cloud and IoT in a secure structure.

2.5.3. Cloud Security Alliance (CSA)

Cloud Security Alliance has focused on the standards, baselines, best practices, and even some security frameworks for specific domains like drones, connected vehicles. Also, they have analyzed the usability of blockchain technology to secure the IoT ecosystem [70], [71].They have developed and offered a 13 step approach to develop secure products in the IoT infrastructure, and they evaluated the system as a whole from sensor to the application including data, connectivity and cloud component. In addition to that, they have prepared a security guide for the early adopter of the IoT, and they have some studies in the identity and access management processes of the IoT [72].

2.5.4. International Telecommunication Union (ITU)

ITU has an initiative body called Global Standards initiative, and it concluded their studies in 2015 with a decision of creating a security group for IoT standards. This group has taken the name of Study Group 20 and initiated their studies in many areas of IoT. Some of them are IPv6 usage in IoT, guides for requirements in IoT network, framework, and models about IoT application domains. They have focused on particular application areas, especially smart cities, interoperability of the different systems and providing IoT environment which is secure and private [73], [74].

2.5.5. Institute of Electrical and Electronics Engineers (IEEE)

IEEE, being aware of the value of the IoT and its benefits both for the industry and the public, have been producing several new standards, creating projects and organizing events. Besides, they have been trying to adapt current security countermeasures and other standards to align with constrained IoT devices. In that manner, they have created a standard association in 2014 to coordinate its efforts in the IoT. They have contacted the stakeholders from both the academic world and the industry to produce best practices and develop new standards. According to the feedback received from the community, they have been discussing problems and issues to find optimum solutions. Some of the most known protocols tuned for IoT are IEEE Std. 802.11 series on wireless LAN, IEEE Std 802.15 series on wireless personal area networks, IEEE Std 1609 series on intelligent transportation, IEEE Std 2030 series on the Smart Grid, including electric vehicle infrastructure, IEEE Std 2040 series on connected, automated, and intelligent vehicles [75].

2.5.6. National Institute of Standards and Technology (NIST)

NIST is one of the significant authorities in the world, which has accepted the great advantages of IoT in production and user satisfaction, so that they have created a cyber-security program for IoT. Thanks to this program, they have created coordination among producers, developers, and academia all around the world. This initiative has led to studies in the form of small subgroups in many sub-domains. These groups analyze the current picture of specific problem areas, like cloud security, smart grids, and cyber-physical systems. Their studies have been combined especially in some programs like NIST 8222 and NIST 8228 programs [76], [77]. These programs continue to analyze and evaluate security and privacy concerns in IoT and update their white papers or reports according to the new threats and solutions.

2.6. Framework Models

The main problems regarding IoT security and privacy stems from the very different nature of the so-called IoT objects. This is because a temperature sensor in the smart home system, a smart meter in the smart grid, an autonomous vehicle or wearable electronics and sensor items are considered as IoT objects. This has led to a focus on standards and framework models. The need to put forward a framework model according to the standards examined became clear during the working phase. As the research in this field was deepened, framework models created through previous studies were determined. When these were examined, it was found that the researchers proposed framework models in a layered structure and tried to increase the comprehensibility of the IoT infrastructure.

The first model have proposed the IoT ecosystem as an extension of the Wireless Sensor Networks (WSN) and presented this in a 3-layered structure. These layers start at the bottom with WSN. Cloud or remote servers exist in the middle of the model. In the top application layer, software, user interfaces and applications exist [78].

A five-layered model has a more detailed structure as it divides the components in a more organized way. This model has higher communication ability and visibility when compared the 3-layered model. However, this model also does not present any issues related to the security [79].

The last model, which has been developed by Cisco, is the most mature and understandable one, because it has seven layers which presents sub-components in a detailed way. This model can be evaluated as the ideal model for presenting IoT stack and infrastructure [80]. All the models have been presented in Table 2.3.

Though the framework models have made contributions for the distinguishment of the components and relations among them, they have not matched the layers with security threats and risks in the IoT ecosystem. There are some studies which have focused on integrating security issues with the layered models in the literature.

In one study, the reserarchers have created a 4-layered model and have mentioned some attacks which affects some layers. However, this model has left many threats untouched and have provided limited match between layers and security risks [80].

In another study, researchers have explored the edge components and edge computing with their threats, but have left other layers untouched. Besides, they have offered countermeasures for the threats to prevent this kind of attacks [81].

A more compherensive study has divided the layers into four category and named them as perception layer, network layer, adoptation layer and application layer. This study has explored the existing situation and described the security attacks for each layer, but did not provide a compherensive or a detailed model for the ecosytem [82]. This study has shown security attacks with violated security targets.

Another study has presented a 6-layered framework model with security threats for each layer, but have limited attacks with certain types and have not matched the attacks with security targets [83].

Many researchers have spent quite some time to analyze the security concerns in IoT and tried to create new solutions and reference models. They have offered some new security reference models with layered architecture. Although the number and naming of the layers differ in the model, the models have tried to cover the same issues. The details of these studies can be found in these references [84][81][85][86][83]. Researchers have analyzed these models and merged threats, countermesures and security requirements with related layers in the context of building blocks [7] A study in the search of a general framework solution for Industrial IoT (IIoT) evaluated the following references [81][87][88][89][90][91][92][93][94][95][96]. After evaluation of the referenced documents, they presented a mixed framework by integrating Cisco and Microsoft cloud security references [97].

Although there are different layers and different mappings for components for related layers in the referenced studies, classification of assets are nearly the same. The reseacrrhes have classified components into four categories which are hardware, protocols, data and software. In some studies the data has been merged with software while in others it has been evaluated as different because of the physical presence of it either in local or in the cloud.

Although these studies mentioned above have presented a more comprehensive ecosystem, they are hard to use by stakeholders who are trying to test their design or products for security vulnerabilities. Especially considering the individuals and organizations at every level operating in the ecosystem and making production, it is very difficult to access, use or evaluate the product, process or design that with the model in that study. In order to realize the mentioned environment, the existence of a user-friendly, and online environment has become a necessity where the technology is advancing very fast.

Moreover, in these studies reviewed and presented the security and privacy issues in the IoT between 2000 and 2017. Since the technological threats are changing rapidly and varying day by day, assessments with an outdated environment can cause risks and threats to be overlooked on certain issues. The static structure of that study abolishes the validity of its use every day. Our study provides a more up-to-date environment by adding works until May 2019. As mentioned before this is another exclusion for the systematic mapping which has been adopted to analyze the literature. In addition to that, our study provides an environment to collect the opinions, findings and proposals of other stakeholders in this field. Our study has a dynamism that can transfer the ideas and proposals of the stakeholders who are interested in the IoT security, to the environment if deemed appropriate as a result of certain evaluations.

Table 3-1 Security Targets and definitions.

Security Target	Meaning
Confidentiality (C)	Data can be accessed by only authorized users.
Integrity (I)	Data is preserved with original state, no modification or tampering have been done.
Availability (A)	Resource or data can be reachable for the authorized entities whenever requested.
Non-repudiation (NR)	System can identify if an action occurs or not.
Privacy (P)	System provides mechanism for entities in the IoT ecosystem to keep their sensitive information secret.
Auditability (AU)	IoT system keeps the logs of the actions and can present whenever needed.
Accountability (AC)	All the entities in the ecosystem knows every action is under control and take responsibility of their own actions.
Trustworthiness (TW)	Ensuring the ability of an IoT system to prove identity and confirm trust in third party

The threats which have been defined in [7] were classified according to the layer position and then connected with the real asset in that layer. Although they offered 109 attack types, some of the attacks exist in more than one layer. As a result, the researchers analyzed 104 unique attack types in their study. The classification of the related attacks according to their layers was presented in Table 3-2. The same scenario was valid for countermeasures, because they used 226 countermeasures against the threats, but 30 of them were offered for more than one layer. Eventually, 196 unique countermeasures were used in that research. The details can be seen in Table 3-2. Some attack types were ignored in these studies because of the relevant relations they have offered in the layers. One of them is social engineering which were covered in the attacks related to the physical devices. However, these attacks can be applied in the application layer or network layers with different methods. Therefore, this attack was ignored. Also, some attack types have different naming in the literature. Therefore, their different representations have been combined such as Man-in-the-Middle, MITM, MIM, etc. In Table 3-2 threats which were not mentioned in the referenced models and found with our research are shown with (*) in the end.

After finding comprehensive IoT security framework models, all the efforts were diverted into the analysis of the work to detect the weak and missing parts of the research. The three main shortcomings identified were:

- The reference models presented in the studies were not easy to use,
- New issues emerging in IoT ecosystem could not be added to the models, because they did not present a suitable interface.
- They were not up-to-date as they could not present threats and countermeasures that emerged in the field of IoT security after 2017.

After determining these deficits, our study was directed at finding solutions to eliminate them. In order to provide an easy to use environment, the development of an application was necessary. To make the application updatable in the future, a suitable interface in the application was necessary. To update the study conducted in 2017, a new literature searches in Google Scholar, Web of Science and IEEE libraries with the same keywords was necessary. Classification of the papers according to their topics and publication years are presented in Table 3-3. As a result of this literature search, 320 research papers were identified. If the paper had the keywords of “attack”, “threat” and “countermeasure”, the paper was analyzed thoroughly. In the end, 22 new attack types and 52 new countermeasures have been found. Details are presented in Table 3-4. In the table, the background colors of the cells with new threats are painted in green, while the new measures are indicated in yellow. More detailed analysis of the attacks and countermeasures will be elaborated in the results section thoroughly.

Detailed stages of the application development are explained in Chapter 4 for the researchers who are interested in creating the same evaluation environment for different purposes. User interfaces, database components and the interactions among these elements are shown step by step.

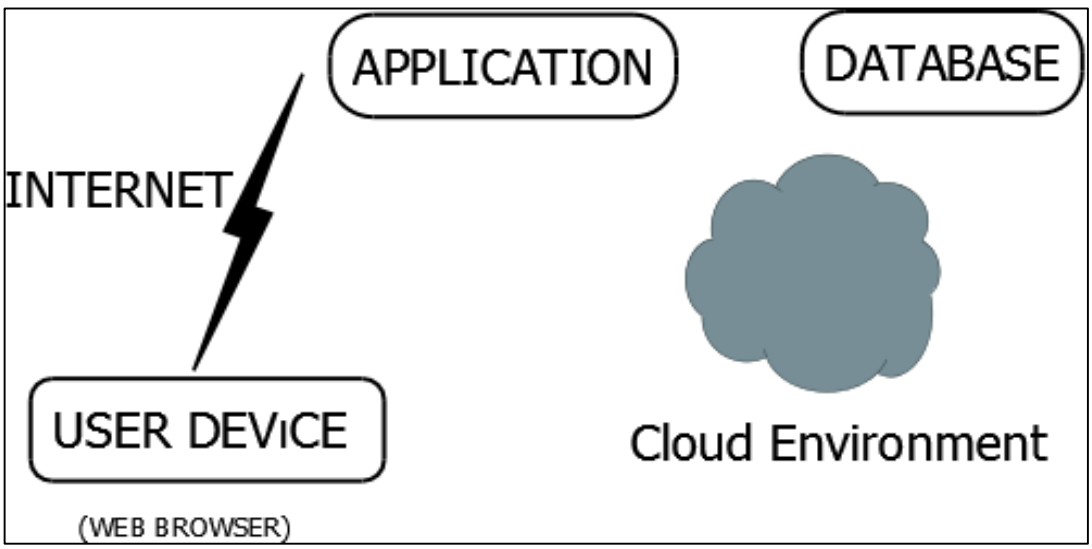

Figure 3-2 Component diagram of the application

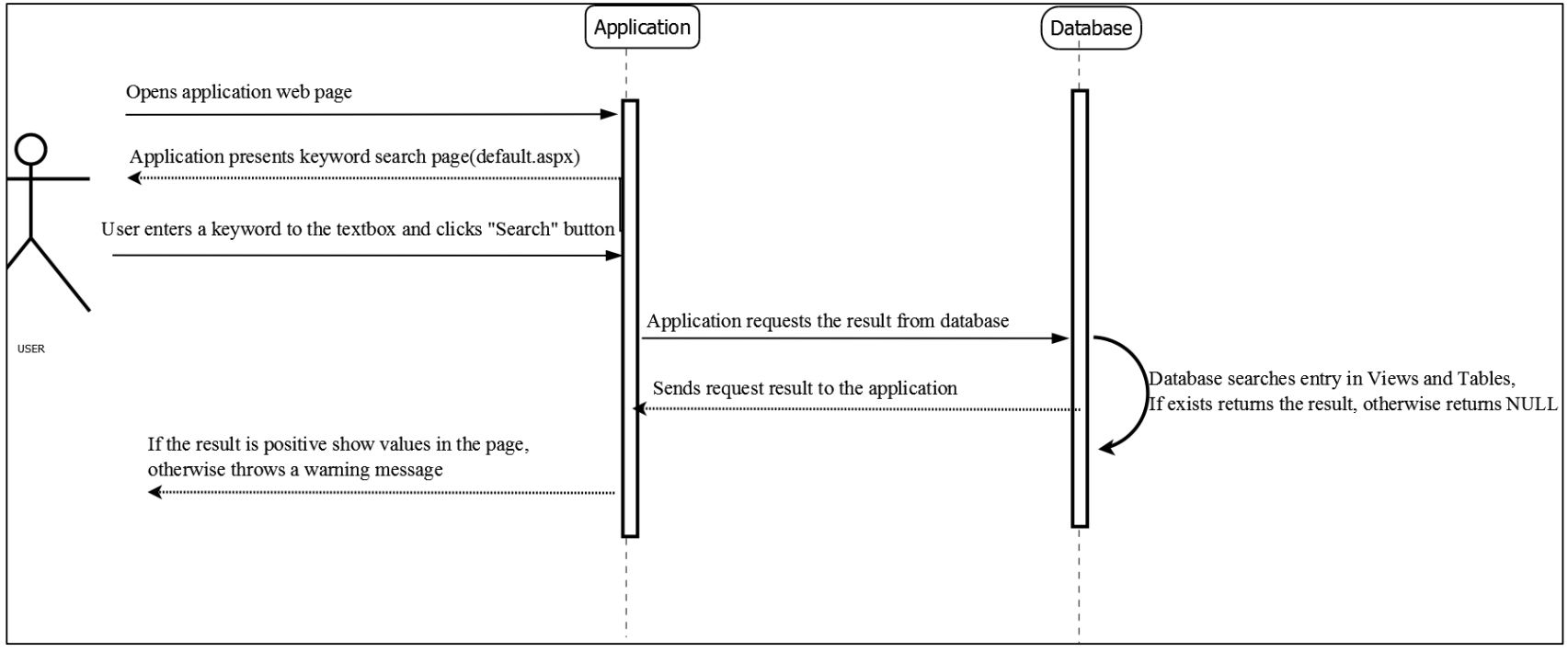

Figure 3-3 Keyword search scenario

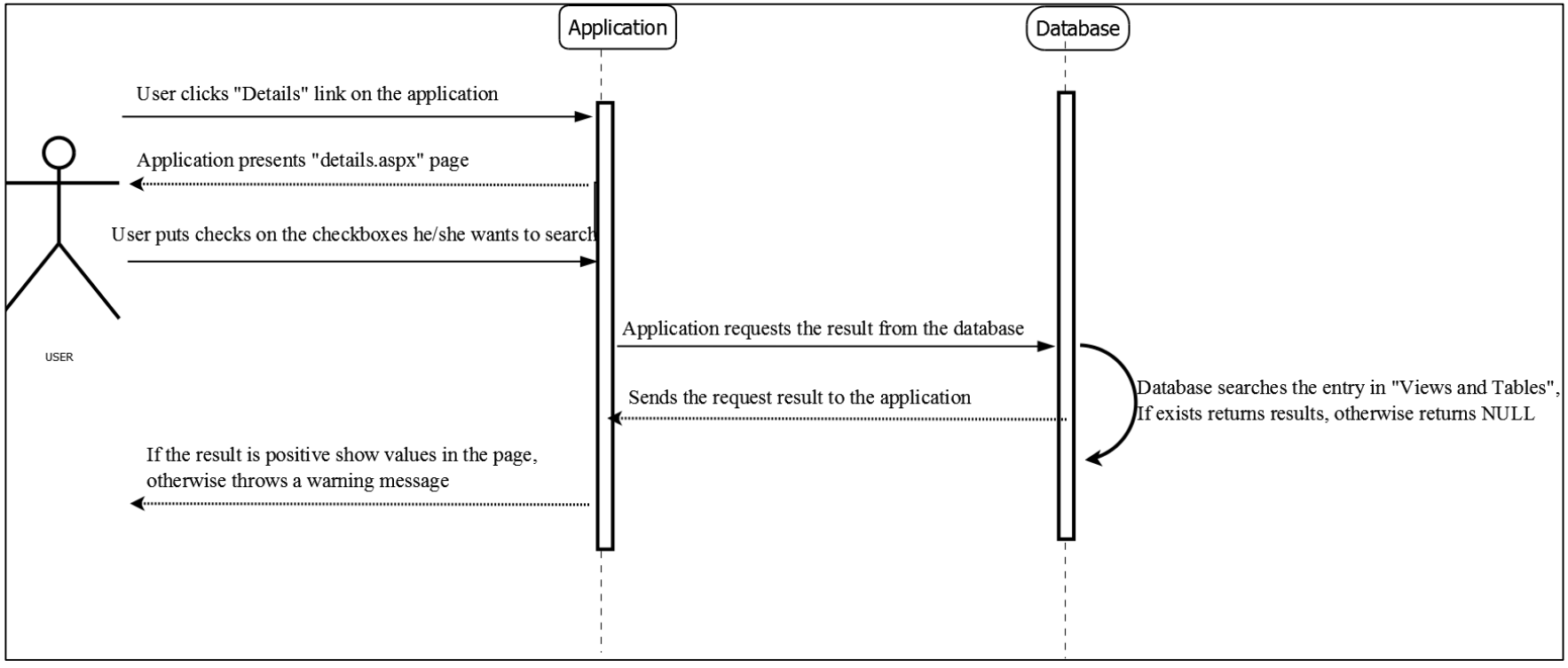

Figure 3-4 Selective Search Scenario

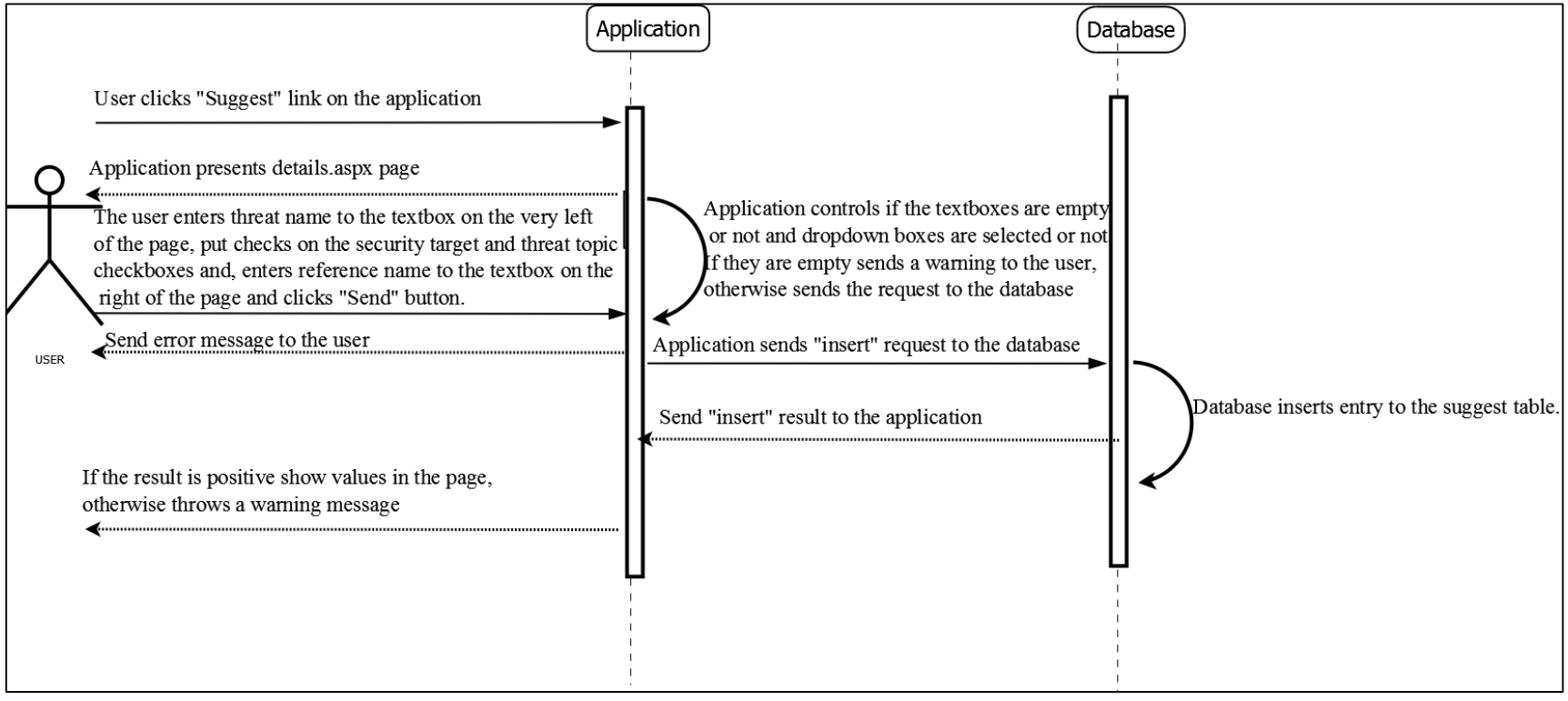

Figure 3-5 Suggest Insert Scenario

3.3.2 Verification and validation tests

During the development, four tests were executed. For the three of them, the application was shared with a group of colleagues in closed local area networks. For the last test, the application was shared on the internet and was open to anyone who wanted to reach. Details of these tests are provided in Chapter 4.

3.4 Validation Phase

At the beginning, the main aim of the study had been identified as creating an online, user-friendly and easy to use evaluation environment for the users with low-level knowledge about IoT security to test their designs' and products' strength against the threats and risks in the IoT ecosystem. In order to evaluate our system in a real environment, a scenario was prepared related to the smart home which had 12 components inside of it and two components outside of it. The details about the questionnaire may be seen on Appendix-A. Two groups of participants were created and in both groups, there were 9 participants, three of them have no experience in IT, three of them have been working in IT\IoT production, management areas and the last three have been selected among the people who are in the security field of IT or IoT.

For all groups, 30 minutes were given to fulfill the task required in the Smart Home scenario and just before this task a general brief was given to the groups about the scenario, task, security targets, connectivity protocols and components in the Smart Home. For the first group internet usage was permitted for achieving the task in the first fifteen-minutes. They were declared that they could use any kind of material they found on the internet for doing the task. In the second half of the task, participants were directed to SIDE web application page and requested to fill the forms according to the results they grabbed while they were using the application.

The second group differed from the first group in the first half of the task, because they were not permitted to use the internet in that period. They completed their task based on the knowledge they already had about the topics. After the first half, they also used SIDE to complete the task. Both groups filled the questionnaire after finishing the task and their answers were transferred to the Google forms to increase visually and reporting. The Smart Home Task is provided in Appendix A and the questionnaire and evaluation of the whole study based on the results was shown in Chapter 5.

Other validation tests have also been performed related to the functionality of web application defined at the beginning of the development. An internal test has also been executed to prove the usability of the application in different application fields, for both today and the future. Physical components like sensors, actuators or protocols related to the connectivity and networks have been selected among the application fields and analyzed asset by asset. Since all the components existed in the database, both the keyword and the selective search have been executed successfully.

Every application needs pre-tests and evaluation throughout the development lifecycle to eliminate bugs, improve performance and to learn user opinion about the product. The same scenario came true for our application and a number of tests were implemented on it. The summary of that process was realized as follows. As soon as the coding and the integration of the database with the application reached a functional level, the application was shared with a group of 10 IT workers in the closed area network. The group members had experience in software development and IT security. Their evaluation was requested in the context of metrics usability, functionality, content, and usefulness, which were used in the studies of Olsina et al. in 2008 [82]. After the development of the application was completed, for validation testing, it was published to the www.secureiot.somee.com . For sytem and study validation a scenario was prepared and based on this scenario validation phase were completed. Findings found at the end of every test phase can be seen in Table 3-5 in detail. Every step of the test showed some compulsive actions to be taken and some arrangements were applied to the application.

Table 3-4 Test Phases of the Application

Test-Phase	Test Purpose	Findings	Action
Initial	Prototype Testing Main function control	Readability in the About.aspx page was low and information related to the directions was not clear enough.	About.aspx page was redesigned
		In details.aspx when select/Unselect all checkboxes were checked and selected, an exception was shown.	Code was changed and fixed.
		In details.aspx page, the components are so small and not aligned which caused problems in usability.	Details.aspx was redesigned and components were aligned.
		In default.aspx the button name was not changed from default value “Button” which could be an obstacle for a new user. Some part of the background was yellow.	Button was renamed as search. Background color was changed.
Second	Check integration of (Suggest.aspx page with application	Button name were left with default name.	Name was changed as “Save”
		Dropdown and text boxes are small. Components are not aligned	Size of dropdown and text boxes was increased. Components were aligned.
		Label on the components was “Request Table”	As this page is an interface it was modified Suggestion interface
Third	Check updated database tables’ compatibility with the system.	Application throws an exception when details.aspx and default.aspx were used.	Required definition was made in the code.
		New columns were not visible	Synchronization of the database columns and code side were completed.
		Values in the new columns were missing in the application.	Incompatible data type were detected between database and application and solved.
Last	Test application in real internet environment	People thought keyword search feature as a search engine and in their answers, they have mentioned they could not find any result from this interface.	A warning was put on the default.aspx.

Table 5-1 Individual Answers for Smart Home Scenario of Group1 (Internet)

Item Numbers						**1**		**2**		**3**		**4**		**5**		**6**		**7**		**8**		**9**		**10**		**11**		**12**		**13**		**14**	
Age	G	Edu.	Job	Exp. (Years)	Part.	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS
32	M	Mas.	IT Sec	5-10	P1	0	0	1	26	0	26	0	0	0	0	1	26	1	26	1	26		46	1	26		0	1	46		46		46
38	M	Uni.	IT Sec	3-5	P2	1	5	1	28	1	38	1	8	1	28	1	28	1	28	1	28	1	1	0	28	0	5	0	28	0	28	0	2
27	M	Mas.	IT Sec	1-3	P3	1	5	0	28	3	15	2	8	1	33	0	28	0	28	0	28	1	15	0	28	1	5	3	19	0	43	0	0
33	M	Uni.	IT	5-10	P4	0	66	0	36	1	66	0	0	1	91	0	83	0	83	0	83	0	83	0	0	0	83	0	83	0	0	0	0
38	M	Mas.	IT	10+	P5	3	5	1	46	3	14	0	8	4	34	1	28	1	28	1	28	0	15	1	28	0	5	1	36	0	42	0	0
38	M	Mas.	IT	10 +	P6	4	55	1	34	0	35	0	8	0	28	0	28	0	28	0	28	0	15	0	28	0	5	0	28	0	28	0	0
38	M	Uni.	Non-IT	10+	P7	1	66	0	28	5	33	0	8	0	33	0	28	0	28	0	28	0	14	0	28	0	0	0	58	0	244	0	33
35	M	Mas.	Non-IT	10+	P8	1	8	1	36	1	5	1	8	0	3	0	21	0	27	0	28	0	1	0	13	0	21	0	52	0	0	0	0
34	M	Doc.	Non-IT	5-10	P9	1	5	1	28	1	15	1	8	1	4	1	6	1	6	1	8	0	0	1	0	1	4	0	32	0	271	0	25

(NS) = No SIDE (WS) = With SIDE (G.) =Gender (Edu.) = Education (Doc.) = Doctorate (Lic.) = Licence (Mas.) = Master (ITSec.) = IT Security

Table 5-2 Individual Answers for Smart Home Scenario of Group2 (No Internet)

Item Numbers						**1**		**2**		**3**		**4**		**5**		**6**		**7**		**8**		**9**		**10**		**11**		**12**		**13**		**14**	
Age	G	Edu.	Job	Exp. (Years)	Part.	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS	NS	WS
31	M	Uni.	IT Sec	1-3	P1	0	76	0	17	1	22	1	8	1	12	0	30	0	30	0	30	0	15	1	25	1	4	0	32	0	271	1	25
38	M	Mas.	IT Sec	1-3	P2	1	6	1	8	1	9	1	9	1	6	1	7	1	11	1	7	1	13	1	5	1	15	1	24	1	21	1	21
36	M	Doc.	IT Sec	5-10	P3	1	6	2	49	1	30	1	9	1	17	2	10	1	10	1	10	1	16	1	6	1	30	1	19	1	226	1	44
35	M	Mas.	Non-IT	5-10	P4	1	19	0	2	1	4	0	2	0	5	0	3	1	4	0	3	0	3	0	2	1	25	0	12	1	18	1	17
38	M	Uni.	Non-IT	5-10	P5	0	50	1	28	1	41	0	33	0	31	0	5	0	8	0	0	0	0	0	0	1	0	1	0	0	0	0	0
35	M	Uni.	Non-IT	5-10	P6	0	80	0	20	0	8	0	5	0	20	0	0	0	0	0	0	0	0	0	0	1	4	0	0	0	0	0	0
38	M	Mas.	IT	5-10	P7	1	4	1	3	11	2	1	2	0	3	0	4	0	4	0	3	0	4	0	4	0	3	0	3	0	4	0	4
34	F	Uni.	IT	10+	P8	0	31	1	20	0	11	0	16	2	3	2	14	2	4	2	1	0	2	0	3	0	3	0	1	0	1	0	44
32	M	Uni.	IT	1-3	P9	0	23	0	49	1	82	0	89	0	74	0	14	0	78	0	71	0	84	0	92	0	87	1	63	0	68	0	14

(NS) = No Side (WS) = With Side (G.)=Gender (Edu.) = Education (Doc.) = Doctorate (Lic.) = Licence (Mas.) = Master (ITSec.) = IT Security

5.2.2 Results of Validation Questionnaire

At the end of the task, participants were asked to fill in a questionnaire to evaluate SIDE in four categories; general system evaluation, usability, perceived usefulness and perceived ease of use. For the general system evaluation, the criteria in the reference by Chin et al. in 1994 were selected and adapted for SIDE [239]. Nielsen's attributes were used as the criteria for usability [240], [241]. Perceived ease of use and usefulness related questions were adapted from the study done in 1994 by Davis [242]. The questionnaire can be found in Table 5-3 and 5-4. In total, there were 39 questions.

The answers of Group1 (Internet) are presented in Table 5-5 and Table 5-6. The answers of Group2 (No Internet) are presented in Table 5-7 and 5-8. Explanations for abbreviations were put under all the tables. In order to fit the information into one page, the font size was reduced. The questions related to general system evaluation, usability, perceived usefulness and perceived ease of use categories were represented with gray, yellow, blue and pink colors, respectively.

A Likert scale was used in the questionnaire where 1 means “Totally disagree” and 5 means “Completely agree”. When the means of the answers given to individual questions under each category was above 3, it was interpreted as a positive evaluation, otherwise a negative evaluation.

Table 5-3 Questionnaire (Front Page)

QUESTIONNAIRE FOR EVALUATION OF SIDE APPLICATION

1	Age										
2	Gender	Male		Female							
3	Education	Lower		High School		University		Master		Doctorate	
4	Profession	IT Related		Other		(Please specify)					
If you have selected IT Related in the 4th question please select one of the below.											
5	Experience in IT	0-1 years		1-3 years		3-5 years		5-10 years		More	
6	Experience in IT Security	0-1 years		1-3 years		3-5 years		5-10 years		More	
7	Experience in IoT	0-1 years		1-3 years		3-5 years		5-10 years		More	
8	Experience in IoT Security	0-1 years		1-3 years		3-5 years		5-10 years		More	

Table 5-4 Questionnaire (Evaluation Pages)

Overall Reaction to SIDE								
1	Overall Reaction to the Software	terrible						wonderful
2		difficult						easy
3		frustrating						Satisfying
4		dull						stimulating
5		rigid						Flexible
Screen								
6	Organization of information	confusing						very clear
7	Sequence of screens	confusing						very clear
8	Characters on the computer screen hard to read easy to read	not at all						very much
Terminology and System Information								
9	Use of terms throughout system	inconsistent						consistent
10	Terminology related to task	never						always
11	Position of messages on screen	inconsistent						consistent
12	Messages on screen which prompt user for input	confusing						clear
13	Computer keeps you informed about what it is doing	never						always
14	Error message	unhelpful						helpful
Learning								
15	Learning to operate the system	difficult						easy
16	Exploring new features by trial and error	difficult						easy
17	Remembering names and use of commands	difficult						easy
18	Performing tasks is straightforward	never						always
19	Help messages on the screen	unhelpful						Helpful
System Capabilities								
20	System speed	too slow						fast enough
21	System reliability	unreliable						reliable
22	System tends to be	noisy						quiet
23	Correcting your mistakes	difficult						easy
24	Designed for all levels of users(Experienced and inexperienced users' needs are taken into consideration	never						always
Usability of the SIDE								

25	Learnability	bad						good
26	Efficiency	bad						good
27	Memorability	bad						good
28	Errors (Accuracy)	bad						good
29	Subjective Satisfaction	bad						Good
Perceived Usefullness								
30	Using the SIDE in “Smart Home” task would enable me to accomplish the task more quickly	unlikely						likely
31	Using the SIDE would improve my task performance	unlikely						likely
32	Using the the SIDE in Smart Home Task would increase my productivity	unlikely						likely
33	Using the SIDE would enhance my effectiveness on for Smart Home task	unlikely						likely
34	Using the SIDE would make it easier to do my task	unlikely						likely
35	I would find the SIDE useful for achieving task	unlikely						Likely
Perceived Ease of Use								
36	Learning to operate the SIDE would be easy for me	unlikely						likely
37	I would find it easy to get the SIDE to do what I want it to do for task.	unlikely						likely
38	It would be easy for me to become skillful at using the SIDE.	unlikely						likely
39	I find the SIDE easy to use.	unlikely						likely

Table 5-9 Evaluation of Results in Groups and Sub-groups for Questionnaire.

Group Info		Mean values of answers Evaluation Parts and Their Represented Colors and Average Points							
Group	Sub-group	System Evaluation (Q1-24)	Color	Usability (Q25-29)	Color	Usefulness (Q30-35)	Color	Ease of Use (Q36-39)	Color
Internet	IT\IoT sec.	4.76	Gray	4.93	Yellow	4.89	Blue	4.92	Pink
	Non IT	4.29		4.27		4.61		4.25	
	IT	4.38		4.87		4.89		4.92	
No Internet	IT\IoT sec.	4.51	Gray	4.73	Yellow	4.50	Blue	4.83	Pink
	Non IT	4.33		4.53		4.61		4.42	
	IT	4.38		4.47		4.22		4.33	

As shown in Table 5-9, for all the criteria and by all the groups, the SIDE application were voted as positive. In fact, there is no mean value below 4.22. This means SIDE was evaluated as highly positive for the Smart Home task and as a tool for IoT security and privacy.

Table 5-10 Evaluation of Results According to Experience for Questionnaire.

		Average Values of Evaluated Criteria			
Job	**Exp (Years)**	System Evaluation (Q1-24)	Usability (Q25-29)	Usefulness (Q30-35)	Ease of Use (Q36-39)
IoT Sec	5-10	5.00	5.00	4.50	5.00
IT Sec	3-5	4.68	4.80	4.16	4.50
IoT Sec	1-3	4.72	4.72	4.83	5.00
Non-IT	5-10	4.33	4.53	4.61	4.41
IT	5-10	4.33	4.60	4.00	4.25
IT	10+	4.37	4.60	4.50	4.25
IT	1-3	4.41	4.25	4.16	4.50

If the results are evaluated according to the participants' experience, it can be seen in Table 5-10 that there is no correlation between experience and evaluation grade. However, participants with the most experience in IoT security evaluated the SIDE application the most positively.

CHAPTER 6

CONCLUSION, DISCUSSION AND FUTURE WORKS

The rapid increase, in both quantitative and qualitative terms, in the IoT area has exacerbated the security and privacy vulnerabilities and threats, causing insecurity in the ecosystem. If these barriers to the IoT development are not removed, opportunities and expansion in new areas of the application may be hampered. The risks of existing products may cause damages that may interfere with the financial, human and community life in different usage scenarios. For this purpose, the weaknesses and risks of the products that will arise in the present and in the future should be minimized.

Increasing the security level depends on the awareness of all stakeholders in the IoT ecosystem. The studies carried out in this field should provide a user-friendly environment in which stakeholders with knowledge at all levels can easily use. Unfortunately, although many studies have been conducted in this area, the majority of them do not provide comprehensive information on the security for all components of the IoT ecosystem, except a few. In previous component-based security studies for frameworks and modals, an easy-to-use and online environment users are not provided to the users.

It is considered that this study will increase the awareness of the stakeholders in the field of security and privacy by providing a user-friendly environment that will eliminate this deficiency in the literature. As a result of the questionnaire applied to the users who have tested the assessment environment, it is expected that the developed application will increase awareness and the use of the environment by the people working in this field will help to reduce the security vulnerabilities.

Several improvements are possible as future work. If threats and countermeasures to IoT application areas are privatized, application users can access threats and solutions related to their areas in less time. The online connection states of the references already presented in plain text on the application may be presented as links in a column. In this case, it may shorten the access time of users for reaching the information on mentioned in these references.

In this study, risk assessment of threats and vulnerabilities have not been carried out. As a future work, it can be included in the design environment to present a risk score as a result of the risk assessment conducted on a component and a scaling to be performed throughout the system. If this scaling can be carried out in a healthy way and if sufficient confirmation can be obtained from the technology companies, organizations and the academic world that have authority in this field, component-based risk maps of the organizations can be provided. This in turn, can help organizations in resource management in IoT design, production and evaluation processes in a more realistic way.

REFERENCES

[1] I. Research, “The weaponization of IoT devices: Rise of the thingbots,” 2017.

[2] M. Hung, “Leading the IoT,” 2017.

[3] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, “IoT Security: Ongoing Challenges and Research Opportunities,” in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 2014, pp. 230–234.

[4] M. Abomhara and G. M. Koien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” *J. Cyber Secur. Mobil.*, vol. 4, no. 1, pp. 65–88, Jan. 2015.

[5] “ISTR Internet Security Threat Report Volume 24 |,” 2019.

[6] A. V. Company, “IoT Security White Paper,” 2017.

[7] H. A. Abdulghani, D. Konstantas, and M. Mahyoub, “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018.

[8] Y. Cherdantseva and J. Hilton, “A Reference Model of Information Assurance & Security,” in *2013 International Conference on Availability, Reliability and Security*, 2013, pp. 546–555.

[9] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, “Systematic mapping studies in software engineering,” *12th Int. Conf. Eval. Assess. Softw. Eng. EASE 2008*, pp. 1–10, 2008.

[10] K. Asthon, “That ’ Internet of Things ’ Thing,” *RFID J.*, p. 4986, 2010.

[11] F. R. and H. G.P., “DTLS for lightweight secure data streaming in the internet of things,” *Proc. - 2014 9th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. 3PGCIC 2014*, vol. 13, no. 4, pp. 585–590, 2014.

[12] “What are the benefits of IoT? - Quora.” [Online]. Available: https://www.quora.com/What-are-the-benefits-of-IoT. [Accessed: 07-Jul-2019].

[13] “The advantages and disadvantages of Internet Of Things (IoT).” [Online]. Available: https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek. [Accessed: 07-Jul-2019].

[14] “The Advantages Of Internet Of Things (IoT) – STIC AMSUD.” [Online]. Available: http://sticamsud.org/2018/10/09/the-advantages-of-internet-of-things-iot/. [Accessed: 07-Jul-2019].

[15] M. Yannuzzi, R. Milito, R. Serral-Gracia, D. Montero, and M. Nemirovsky, “Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing,” *2014 IEEE 19th Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD 2014*, pp. 325–329, 2014.

[16] D. Evans, “The Internet of Things How the Next Evolution of the Internet The Internet of Things How the Next Evolution of the Internet Is Changing Everything,” no. April, 2011.

[17] B. Glavour and H. Bhatt, *RFID Essentials*. O’Reilly Media, Inc., 2006.

[18] D. He and S. Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography,” *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, 2015.

[19] K. Cooper, “Security for the Internet of Things,” 2015.

[20] R. Benabdessalem, M. Hamdi, and T. H. Kim, “A Survey on Security Models, Techniques, and Tools for the Internet of Things,” *Proc. - 7th Int. Conf. Adv. Softw. Eng. Its Appl. ASEA 2014*, pp. 44–48, 2014.

[21] E. Borgia, “The Internet of Things vision : Key features , applications and open issues,” *Comput. Commun.*, vol. 54, pp. 1–31, 2014.

[22] P. Marshall, “Security for the Internet of Things,” KTH Royal Institute of Technologhy, 2015.

[23] T. Stack, “Internet of Things (IoT) Data Continues to Explode Exponentially. Who Is Using That Data and How? - Cisco Blog,” 2018. [Online]. Available: https://blogs.cisco.com/datacenter/internet-of-things-iot-data-continues-to-explode-exponentially-who-is-using-that-data-and-how. [Accessed: 12-May-2019].

[24] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” 2011.

[25] A. R. Biswas and R. Giaffreda, “IoT and Cloud Convergence : Opportunities and Challenges,” *2014 IEEE World Forum Internet Things*, pp. 375–376, 2014.

[26] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, “Secure integration of IoT and Cloud Computing,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 964–975, 2018.

[27] J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, “Toward a lightweight authentication and authorization framework for smart objects,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 4, pp. 690–702, 2015.

[28] T. Winter, P. Thubert, A. R. Corporation, and R. Kelsey, “IPv6 Routing Protocol for Low-Power and Lossy Networks,” 2012.

[29] J. Vasseur and J. Hui, “RFC 6553 - The Routing Protocol for Low-Power and Lossy Networks RPL, Option for Carrying RPL Information in Data-Plane Datagrams,” 2012.
[30] Y. Zhang and S. Bikramjit, “A Multi-Layer IPsec Protocol,” *9th USENIX Security Symposium Paper*, 2000. [Online]. Available: https://www.usenix.org/legacy/events/sec2000/full_papers/zhangipsec/zhangipsec_html/. [Accessed: 16-May-2019].
[31] S. Frankel and S. Krishnan, “RFC 6071 - IP Security IPsec, and Internet Key Exchange IKE, Document Roadmap,” 2011.
[32] V. Karagiannis, P. Chatzimisios, F. Vazquez-gallego, and J. Alonso-zarate, “A Survey on Application Layer Protocols for the Internet of Things Research motivation,” vol. 3, no. 1, pp. 9–18, 2015.
[33] A. P. Castellani, M. Gheda, N. Bui, M. Rossi, and M. Zorzi, “Web Services for the Internet of Things through CoAP and EXI,” in *2011 IEEE International Conference on Communications Workshops (ICC)*, 2011, vol. 1, no. July, pp. 1–6.
[34] S. Kraijak and P. Tuwanut, “A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends,” in *2015 IEEE 16th International Conference on Communication Technology (ICCT)*, 2015, pp. 26–31.
[35] D. Soni and A. Makwana, “A survey on mqtt: a protocol of internet of things(IoT),” *Int. Conf. Telecommun. Power Anal. Comput. Tech. (Ictpact - 2017)*, no. April, pp. 0–5, 2017.
[36] T. Yokotani and Y. Sasaki, “Comparison with HTTP and MQTT on required network resources for IoT,” in *2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, 2016, pp. 1–6.
[37] H. Wang, D. Xiong, P. Wang, and Y. Liu, “A Lightweight XMPP Publish/Subscribe Scheme for Resource-Constrained IoT Devices,” *IEEE Access*, vol. 5, pp. 16393–16405, 2017.
[38] M. Laine, “RESTful Web Services for the Internet of Things,” [*Online]. Saatavilla http//media. tkk. fi/webservices/personnel/markku_laine/restful_web_services_for _the_internet_of_things*, pp. 2–4, 2012.
[39] B. N. Nakhuva and T. A. Champaneria, “Security provisioning for RESTful web services in Internet of Things,” in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017, pp. 1–6.
[40] “June | 2015 | MonacoTrades.com.” [Online]. Available: http://monacotrades.com/2015/06/. [Accessed: 25-May-2019].
[41] “The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects - IoT Analytics.” [Online]. Available: https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/. [Accessed: 25-May-2019].
[42] “50 Sensor Applications for a Smarter World.”
[43] S. Mdukaza, B. Isong, N. Dladlu, and A. M. Abu-Mahfouz, “Analysis of IoT-Enabled Solutions in Smart Waste Management,” in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 4639–4644.
[44] S. Javaid, A. Sufian, S. Pervaiz, and M. Tanveer, “Smart traffic management system using Internet of Things,” in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 2018, pp. 393–398.
[45] A. Sharif, J. Li, M. Khalil, R. Kumar, M. I. Sharif, and A. Sharif, “Internet of things - Smart traffic management system for smart cities using big data analytics,” *2016 13th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. ICCWAMTIP 2017*, vol. 2018-Febru, no. November, pp. 281–284, 2017.
[46] A. Khanna and R. Anand, “IoT based smart parking system,” no. December 2018, pp. 266–270, 2016.
[47] P. Chippalkatti, G. Kadam, and V. Ichake, “I-SPARK: IoT Based Smart Parking System,” *2018 Int. Conf. Adv. Commun. Comput. Technol. ICACCT 2018*, no. January 2016, pp. 473–477, 2018.
[48] S. S. I. Samuel, “A review of connectivity challenges in IoT-smart home,” *2016 3rd MEC Int. Conf. Big Data Smart City, ICBDSC 2016*, pp. 364–367, 2016.
[49] A. R. Boynuegri, B. Yagcitekin, M. Baysal, A. Karakas, and M. Uzunoglu, “Energy management algorithm for smart home with renewable energy sources,” *Int. Conf. Power Eng. Energy Electr. Drives*, no. May, pp. 1753–1758, May 2013.
[50] V. Ricquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche, and C. Loge, “The Smart Home Concept : our immediate future,” in *2006 1ST IEEE International Conference on E-Learning in Industrial Electronics*, 2006, pp. 23–28.
[51] F. K. Santoso and N. C. H. Vun, “Securing IoT for smart home system,” in *2015 International Symposium on Consumer Electronics (ISCE)*, 2015, pp. 1–2.
[52] M. A. M. A. Hanson *et al.*, “Body Area Sensor Networks : Challenges and Opportunities,” *IEEE Comput. Soc.*, vol. 42, no. 1, p. 58, Jan. 2009.
[53] M. Li, W. Lou, and K. Ren, “Data security and privacy in wireless body area networks,” *IEEE Wirel. Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.
[54] C. Otto, A. Milenković, C. Sanders, and E. Jovanov, “SYSTEM ARCHITECTURE OF A WIRELESS BODY AREA SENSOR NETWORK FOR UBIQUITOUS HEALTH MONITORING 1 Introduction,” 2006.

[55] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, “RFID Technology for IoT-Based Personal Healthcare in Smart Spaces,” *IEEE Internet Things J.*, vol. 1, no. 2, pp. 144–152, Apr. 2014.
[56] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart Grid – The New and Improved Power Grid :,” *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.
[57] E. Fadel *et al.*, “A survey on wireless sensor networks for smart grid,” *Comput. Commun.*, 2015.
[58] Y. Kabalci, “A survey on smart metering and smart grid communication,” *Renewable and Sustainable Energy Reviews*. 2016.
[59] P. McDaniel and S. McLaughlin, “Security and Privacy Challenges in the Smart Grid,” *IEEE Secur. Priv. Mag.*, vol. 7, no. 3, pp. 75–77, May 2009.
[60] B. Filkins and D. Wylie, “The 2018 SANS Industrial IoT Security Survey.”
[61] R. Sanchez-Iborra, M.-D. Cano, R. Sanchez-Iborra, and M.-D. Cano, “State of the Art in LP-WAN Solutions for Industrial IoT Services,” *Sensors*, vol. 16, no. 5, p. 708, May 2016.
[62] A. (Waterfall S. S. Ginter, R. Martin, and S. (Intel) Schrecker, “Industrial Internet of Things Volume G4: Security Framework,” ENT Technologies, 2016.
[63] https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/, “The Industrial Internet of Things (IIoT): the business guide to Industrial IoT.” [Online]. Available: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/. [Accessed: 30-May-2019].
[64] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, “Security analysis on consumer and industrial IoT devices,” in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016, pp. 519–524.
[65] A. Sajid, H. Abbas, and K. Saleem, “Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges,” *IEEE Access*, vol. 4, pp. 1375–1384, 2016.
[66] B. Leitl, “Challenges in Securing Industrial IoT and Critical Infrastructure,” in *Smart Card Research and Advanced Application Conference*, 2018.
[67] “GSMA IoT Security Guidelines | Internet of Things.” [Online]. Available: https://www.gsma.com/iot/iot-security/iot-security-guidelines/. [Accessed: 07-Jul-2019].
[68] “ENISA Good practices for IoT and Smart Infrastructures Tool — ENISA.” [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#Smart Cars. [Accessed: 08-Jul-2019].
[69] “Baseline Security Recommendations for IoT — ENISA.”
[70] “CSA Guide to the IoT Security Controls | Cloud Security Alliance.” [Online]. Available: https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/. [Accessed: 08-Jul-2019].
[71] “Future Proofing the Connected World | Cloud Security Alliance.” [Online]. Available: https://cloudsecurityalliance.org/artifacts/future-proofing-the-connected-world/. [Accessed: 08-Jul-2019].
[72] “Identity and Access Management for the | Cloud Security Alliance.” [Online]. Available: https://cloudsecurityalliance.org/artifacts/identity-and-access-management-for-the-iot/. [Accessed: 08-Jul-2019].
[73] “ITU Smart Sustainable Cities and Communities Initiatives: Towards a Smart Global Vision Ramy A. Fathy SG20 Vice chairman.”
[74] “ITU-T WP: 2013-2016: SG20.” [Online]. Available: https://www.itu.int/itu-t/workprog/wp_search.aspx?isn_sp=1749&isn_sg=2758&isn_status=-1%2C1%2C3%2C7%2C2%2C5&details=0&field=acdefghijo. [Accessed: 08-Jul-2019].
[75] “Internet of Things (IoT) Ecosystem Study Executive Summary,” 2015.
[76] J. Voas, R. K. Kuhn, P. Laplante, and S. Applebaum, “Internet of Things (IoT) Trust Concerns,” 2018.
[77] K. Boeckl, M. Fagan, W. Fisher, and K. Scarfone, “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,” 2018.
[78] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.
[79] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[80] “The Internet of Things Reference Model,” 2014.
[81] A. Mosenia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 4, pp. 586–602, Oct. 2017.
[82] R. Kajaree, D and Behera, “A Survey on IoT Security Threats and Solutions.” International Journal of Innovative Research in Computer and Communication Engineering, pp. 1302–1309, 2016.
[83] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed Security Model and Threat Taxonomy for the

Internet of Things (IoT)," Springer, Berlin, Heidelberg, 2010, pp. 420–429.
[84] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "A new approach to investigate IoT threats based on a four layer model," in *2016 13th International Conference on New Technologies for Distributed Systems (NOTERE)*, 2016, pp. 1–6.
[85] A. Radovici, C. Rusu, and R. Serban, "A Survey of IoT Security Threats and Solutions," *Proc. - 17th RoEduNet IEEE Int. Conf. Netw. Educ. Res. RoEduNet 2018*, pp. 1–5, 2018.
[86] J. SathishKumar, D. R. Patel, and J. S. Kumar, "A Survey on Internet of Things: Security and Privacy Issues," *Int. J. Comput. Appl.*, vol. 90, no. 11, pp. 20–26, Mar. 2014.
[87] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 269–284, 2016.
[88] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," *Proc. 2015 Int. Conf. Green Comput. Internet Things, ICGCIoT 2015*, pp. 1577–1581, 2016.
[89] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 336–341, 2016.
[90] J. Kuusijarvi, R. Savola, P. Savolainen, and A. Evesti, "Mitigating IoT security threats with a trusted Network element," *2016 11th Int. Conf. Internet Technol. Secur. Trans. ICITST 2016*, pp. 260–265, 2017.
[91] H. He *et al.*, "The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence," in *2016 IEEE Congress on Evolutionary Computation (CEC)*, 2016, pp. 1015–1021.
[92] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, 2017.
[93] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
[94] B. Mukherjee, R. L. Neupane, and P. Calyam, "End-to-End IoT Security Middleware for Cloud-Fog Communication," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2017, pp. 151–156.
[95] H. Guo, J. Ren, D. Zhang, Y. Zhang, and J. Hu, "A scalable and manageable IoT architecture based on transparent computing," *J. Parallel Distrib. Comput.*, vol. 118, pp. 5–13, 2018.
[96] P. Tuwanut and S. Kraijak, "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends," pp. 6 .-6 ., 2016.
[97] Z. Bakhshi, A. Balador, and J. Mustafa, "Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models," in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2018, pp. 173–178.
[98] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance and Security," in *2013 International Conference on Availability, Reliability and Security*, 2013, pp. 546–555.
[99] Y. Xiao and Yang, *Security in distributed, grid, mobile, and pervasive computing*. Auerbach Publications, 2007.
[100] G. Kulkarni, R. Shelke, R. Sutar, and S. Mohite, "RFID security issues and challenges," in *2014 International Conference on Electronics and Communication Systems (ICECS)*, 2014, pp. 1–4.
[101] E. Tews, "Attacks on the WEP protocol," no. December 2007, 2007.
[102] M. Caneill and J. Gilis, "Attacks against the WiFi protocols WEP and WPA," *Journal*, no. December, pp. 1–15, 2010.
[103] M. Beck and E. Tews, "Practical attacks against WEP and WPA," *Proc. 2nd ACM Conf. Wirel. Netw. Secur. WiSec'09*, no. January 2008, pp. 79–85, 2009.
[104] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based internet of things," *Int. J. Netw. Secur.*, vol. 18, no. 3, pp. 459–473, 2016.
[105] L. Markowsky and G. Markowsky, "Scanning for vulnerable devices in the Internet of Things," *Proc. 2015 IEEE 8th Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. Technol. Appl. IDAACS 2015*, vol. 1, no. February 2016, pp. 463–467, 2015.
[106] H. Al-Alami, A. Hadi, and H. Al-Bahadili, *Vulnerability Scanning of IoT Devices in Jordan using Shodan*. 2017.
[107] A. Sivanathan, H. Habibi Gharakheili, and V. Sivaraman, "Can We Classify an {IoT} Device Using {TCP} Port Scan?," *2018 IEEE Int. Conf. Inf. Autom. Sustain. (ICIAfS 2018)*, 2018.
[108] "The Five-Layer TCP/IP Model: Description/Attacks/Defense - Computing and Software Wiki." [Online]. Available: http://wiki.cas.mcmaster.ca/index.php/The_Five-Layer_TCP/IP_Model:_Description/Attacks/Defense. [Accessed: 17-Sep-2019].
[109] N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," *Computer Communications*. 2017.

[110] C. Rong, S. Nguyen, and M. Jaatun, “Beyond lightning: A survey on security challenges in cloud computing,” *Comput. Electr. Eng.*, vol. 39, pp. 47–54, Jan. 2013.
[111] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, “Hardware Trojan Attacks: Threat Analysis and Countermeasures,” *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.
[112] P. Pongle and G. Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT,” *2015 Int. Conf. Pervasive Comput. Adv. Commun. Technol. Appl. Soc. ICPC 2015*, vol. 00, no. c, pp. 1–6, 2015.
[113] S. Kumarasamy and G. A. Shankar, “An Active Defense Mechanism for TCP SYN flooding attacks,” *arXiv.org*, pp. 1–6, 2012.
[114] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, “IoDDoS -The internet of distributed denial of sevice attacks A case study of the mirai malware and IoT-Based botnets,” *IoTBDS 2017 - Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, no. IoTBDS, pp. 47–58, 2017.
[115] N.-N. Dao, T. V. Phan, U. S. ad, J. Kim, T. Bauschert, and S. Cho, “Securing Heterogeneous IoT with Intelligent DDoS Attack Behavior Learning,” 2017.
[116] A. Bijalwan, M. Wazid, E. Pilli, and R. Joshi, “Forensics of Random-UDP Flooding Attacks,” *J. Networks*, vol. 10, May 2015.
[117] “UDP Flood DDoS Attack | Cloudflare.” [Online]. Available: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/. [Accessed: 17-Sep-2019].
[118] S. N. Swamy, D. Jadhav, and N. Kulkarni, “Security threats in the application layer in IOT applications,” in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 477–480.
[119] H. Li, Y. Chen, and Z. He, “The Survey of RFID Attacks and Defenses,” in *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, 2012, pp. 1–4.
[120] J. Sen, “A Survey on Wireless Sensor Network Security,” *Int. J. Commun. Networks Inf. Secur.*, vol. 1, no. 2, pp. 55–68, Nov. 2010.
[121] A. Belfkih, C. Duvallet, and B. Sadeg, “A survey on wireless sensor network databases,” *Wirel. Networks*, vol. 1, no. 2, pp. 59–82, 2019.
[122] O. Zheng, J. Poon, and K. Beznosov, “Application-based TCP Hijacking,” in *Proceedings of the Second European Workshop on System Security*, 2009, pp. 9–15.
[123] T. Bhattasali, R. Chaki, and N. Chaki, “Secure and trusted cloud of things,” in *2013 Annual IEEE India Conference (INDICON)*, 2013, pp. 1–6.
[124] F. Alsubaei, A. Abuhussein, and S. Shiva, “Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment,” in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, 2017, pp. 112–120.
[125] P. P. Lokulwar and H. R. Deshmukh, “Threat analysis and attacks modelling in routing towards IoT,” in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 721–726.
[126] S. Rupinder, J. Singh, and R. Singh, “ATTACKS IN WIRELESS SENSOR NETWORKS: A SURVEY,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 5, no. 5, pp. 10–16, 2016.
[127] A. S., S. E., and A. EL-Sayed, “A Survey of Wireless Sensor Network Attacks,” *Commun. Appl. Electron.*, vol. 6, no. 10, pp. 10–20, 2017.
[128] J. Deogirikar and A. Vidhate, “Security attacks in IoT: A survey,” *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, pp. 32–37, 2017.
[129] M. M. Ahemd, M. A. Shah, and A. Wahid, “IoT security: A layered approach for attacks & defenses,” in *International Conference on Communication Technologies, ComTech 2017*, 2017, pp. 104–110.
[130] A. Bittau, M. Handley, and J. Lackey, “The final nail in WEP’s coffin,” in *2006 IEEE Symposium on Security and Privacy (S&P’06)*, 2006, pp. 15 pp. – 400.
[131] “What is a TCP SYN Flood | DDoS Attack Glossary | Imperva.” [Online]. Available: https://www.imperva.com/learn/application-security/syn-flood/. [Accessed: 17-Sep-2019].
[132] W. A. Jansen, “Cloud Hooks: Security and Privacy Issues in Cloud Computing,” in *Proceedings of the 2011 44th Hawaii International Conference on System Sciences*, 2011, pp. 1–10.
[133] S. Chandna, R. Singh, and F. Akhtar, “Data scavenging threat in cloud computing,” *Int. J. Adv. Comput. Sci. Cloud Comput.*, vol. 2, no. 2, pp. 17–22, 2014.
[134] U. Sabeel and S. Maqbool, “Categorized Security Threats in the Wireless Sensor Networks: Countermeasures and Security Management Schemes,” *Int. J. Comput. Appl.*, vol. 64, no. 16, pp. 19–28, Feb. 2013.
[135] H. Chaudhari and L. Kadam, “Wireless Sensor Networks: Security, Attacks and Challenges,” *Int. J. Netw.*, vol. 1, no. 1, pp. 4–16, 2011.

[136] Q. Xiao, C. Boulet, and T. Gibbons, “RFID Security Issues in Military Supply Chains,” in *The Second International Conference on Availability, Reliability and Security (ARES’07)*, 2007, pp. 599–605.
[137] “What is an IP/ICMP Fragmentation Attack? | NETSCOUT.” [Online]. Available: https://www.netscout.com/what-is-ddos/ip-icmp-fragmentation. [Accessed: 18-Sep-2019].
[138] “What is an IP Fragmentation Attack (Teardrop ICMP/UDP) | Imperva.” [Online]. Available: https://www.imperva.com/learn/application-security/ip-fragmentation-attack-teardrop/. [Accessed: 18-Sep-2019].
[139] H. Kim, *Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer*. 2008.
[140] W. Dawoud, I. Takouna, and C. Meinel, “Infrastructure as a service security: Challenges and solutions,” *INFOS2010 - 2010 7th Int. Conf. Informatics Syst.*, pp. 1–8, 2010.
[141] S. Boddy and J. Shattuck, “The Hunt for IoT: The Rise of Thingbots,” f5, 2017.
[142] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, “Smart Nest Thermostat : A Smart Spy in Your Home,” *Black Hat USA*, pp. 1–8, 2014.
[143] S. Jucker, “Securing the Constrained Application Protocol,” *no. Oct.*, no. October, pp. 1–103, 2012.
[144] I. Ali, S. Sabir, and Z. Ullah, “Internet of Things Security , Device Authentication and Access Control : A Review,” *Ijcsis*, vol. 14, no. 8, pp. 1–11, 2016.
[145] C. C. V, “CSA - Top Threaths to Cloud Computing v1.0,” *Security*, no. March, pp. 1–14, 2010.
[146] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” *Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004.
[147] Neeta B. Thorat; C. A. Laulkar, “Survey on Security Threats and Solutions for Near Field Communication,” *Int. J. Res. Eng. Technol.*, vol. 03, no. 12, pp. 291–295, 2014.
[148] M. Beck, “Enhanced TKIP Michael Attacks,” 2014.
[149] “Data Loss vs. Data Leakage Prevention: What’s the Difference?” [Online]. Available: https://blogs.informatica.com/2017/05/03/data-loss-vs-data-leakage-prevention-whats-difference/#fbid=SiguP6WmSms. [Accessed: 18-Sep-2019].
[150] B. Grobauer, T. Walloschek, and E. Stöcker, “Understanding cloud computing vulnerabilities,” *IEEE Secur. Priv.*, vol. 9, no. 2, pp. 50–57, 2011.
[151] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, “Cyber Security Threats to IoT Applications and Service Domains,” *Wirel. Pers. Commun.*, vol. 95, no. 1, pp. 169–185, 2017.
[152] M. Roland, J. Langer, and J. Scharinger, “Practical Attack Scenarios on Secure Element-Enabled Mobile Devices,” in *2012 4th International Workshop on Near Field Communication*, 2012, pp. 19–24.
[153] A. RGHIOUI, A. KHANNOUS, and M. BOUHORMA, “Denial-of-Service attacks on 6LoWPAN-RPL networks: Issues and practical solutions,” *J. Adv. Comput. Sci. Technol.*, vol. 3, no. 2, p. 143, Sep. 2014.
[154] M. Marlinspike, “sslstrip.” [Online]. Available: https://moxie.org/software/sslstrip/. [Accessed: 18-Sep-2019].
[155] “What is SSL Stripping? How to Prevent from SSL Strip?” [Online]. Available: https://comodosslstore.com/blog/what-is-ssl-stripping-beginners-guide-to-ssl-strip-attacks.html. [Accessed: 18-Sep-2019].
[156] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing:Impşementation, Management and Security*, vol. 112, no. 483. 2010.
[157] N. Gelernter, “Cross-Site Challenge-Response Attacks.”
[158] E. Haselsteiner and K. Breitfuß, “Security in near field communication (NFC),” *Work. RFID Secur.*, pp. 12–14, 2006.
[159] M. S. Ahmad, “WPA Too!,” *Defcon 18*, p. 7, 2010.
[160] “What is SSL BEAST? Webopedia Definition.” [Online]. Available: https://www.webopedia.com/TERM/S/ssl_beast.html. [Accessed: 18-Sep-2019].
[161] J. Rizzo, “Files from Packet Storm.” [Online]. Available: https://packetstormsecurity.com/files/author/2672/. [Accessed: 18-Sep-2019].
[162] E. Haselsteiner and P. Semiconductors, “Security in Near Field Communication (NFC),” *Work. RFID Secur.*, Jan. 2006.
[163] N. Mavrogiannopoulos, F. Vercauteren, V. Velichkov, and B. Preneel, “A Cross-protocol Attack on the TLS Protocol,” in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 2012, pp. 62–72.
[164] A. Tsow, “Phishing with consumer electronics - Malicious home routers,” *CEUR Workshop Proc.*, vol. 190, 2006.
[165] X. Fan *et al.*, “Security Analysis of Zigbee,” *MWR InfoSecurity*, no. May, pp. 1–18, 2017.
[166] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, *6LoWPAN Fragmentation Attacks and Mitigation Mechanisms*. 2013.
[167] C. Paper and C. Republic, “Attacking RSA-based sessions in SSL / TLS Attacking RSA-based Sessions in SSL / TLS,” no. April, 2014.
[168] J. Domzal, “Securing the cloud: Cloud computer security techniques and tactics (Winkler, V.; 2011) [Book reviews],”

IEEE Commun. Mag., vol. 49, no. 9, pp. 20–20, 2011.
[169] "IoT Devices Easily Hacked to be Backdoors: Experiment | SecurityWeek.Com." [Online]. Available: https://www.securityweek.com/iot-devices-easily-hacked-be-backdoors-experiment. [Accessed: 19-Sep-2019].
[170] B. Mullinax, "Security without IoT Mandatory Backdoors To cite this version : HAL Id : hal-01152495 Security without IoT Mandatory Backdoors," 2016.
[171] L. M. L. Oliveira, J. J. P. C. Rodrigues, C. Neto, and A. F. De Sousa, "Network admission control solution for 6LoWPAN networks," *Proc. - 7th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2013*, pp. 472–477, 2013.
[172] Y. Sheffer, R. Holz, and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)," Feb. 2015.
[173] "Hacker's Choice: Top Six Database Attacks." [Online]. Available: https://www.darkreading.com/risk/hackers-choice-top-six-database-attacks/d/d-id/1129481. [Accessed: 18-Sep-2019].
[174] "Top 10 2013-Top 10 - OWASP." [Online]. Available: https://www.owasp.org/index.php/Top_10_2013-Top_10. [Accessed: 19-Sep-2019].
[175] N. B. N. Ibn Minar, "Bluetooth Security Threats And Solutions: A Survey," *Int. J. Distrib. Parallel Syst.*, vol. 3, no. 1, pp. 127–148, 2012.
[176] B. Fan, "Analysis on the Security Architecture of ZigBee Based on IEEE 802.15.4," *Proc. - 2017 IEEE 13th Int. Symp. Auton. Decentralized Syst. ISADS 2017*, pp. 241–246, 2017.
[177] K. Masica, "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments Networks in Process Control," *Program*, no. April, p. 24, 2007.
[178] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2654–2668, 2014.
[179] R. Focardi, "Practical Padding Oracle Attacks on RSA," *SecGroup*, pp. 1–9, 2012.
[180] N. J. AlFardan and K. G. Paterson, "Lucky thirteen: Breaking the TLS and DTLS record protocols," *Proc. - IEEE Symp. Secur. Priv.*, pp. 526–540, 2013.
[181] M. Stevens, A. Lenstra, and B. de Weger, "Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities BT - Advances in Cryptology - EUROCRYPT 2007," 2007, pp. 1–22.
[182] J. Wright, "KillerBee: Practical ZigBee Exploitation Framework or 'Wireless Hacking and the Kinetic World,'" *11th ToorCon Conf.*, 2009.
[183] M. Wang, "Understanding security flaws of IoT protocols through honeypot technologies," *J. Opt. Soc. Am.*, 2006.
[184] J. Markert, M. Massoth, K.-P. Fischer-Hellmann, S. Furnell, and C. Bolan, "Attack Vectors to Wireless ZigBee Network Communications - Analysis and Countermeasures," *Proc. Seventh Collab. Res. Symp. Secur. E-learning, Internet Netw. (SEIN 2011), Furtwangen, Ger.*, 2011.
[185] D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," *2015 13th Annu. Conf. Privacy, Secur. Trust. PST 2015*, pp. 145–152, 2015.
[186] M. Backes and C. Hriţcu, "Practical Aspects of Security Control Hijacking Attacks," 2009.
[187] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, "Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned," in *2013 46th Hawaii International Conference on System Sciences*, 2013, pp. 5132–5138.
[188] M. Tan and K. A. Masagca, "An Investigation of Bluetooth Security Threats," in *2011 International Conference on Information Science and Applications*, 2011, pp. 1–7.
[189] "IoT Message Protocols: The Next Security Challenge for Service Providers?" [Online]. Available: https://www.f5.com/company/blog/iot-message-protocols-the-next-security-challenge-for-service-providers. [Accessed: 18-Sep-2019].
[190] F. A. Teixeira *et al.*, "Defending Code from the Internet of Things against Buffer Overflow," in *2014 Brazilian Symposium on Computer Networks and Distributed Systems*, 2014, pp. 293–301.
[191] J. B. Hou, T. Li, and C. Chang, "Research for Vulnerability Detection of Embedded System Firmware," *Procedia Comput. Sci.*, vol. 107, no. Icict, pp. 814–818, 2017.
[192] S. Jasek, "Gattacking Bluetooth smart devices," in *Black Hat USA Conference*, 2016.
[193] B. Fouladi and S. Ghanoun, "Security Evaluation of the Z-Wave Wireless Protocol," *Black hat*, p. 6, 2013.
[194] K. Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets," Feb. 2017.
[195] H. J. Tay, J. Tan, and P. Narasimhan, "A Survey of Security Vulnerabilities in Bluetooth Low Energy Beacons," *Parallel Data Lab.*, no. November, 2016.
[196] J. D. Fuller, B. W. Ramsey, M. J. Rice, and J. M. Pecarina, "Misuse-based detection of Z-Wave network attacks," *Comput.*

Secur., vol. 64, pp. 44–58, 2017.
[197] A. Tierney, "Z-Shave. Exploiting Z-Wave downgrade attacks | Pen Test Partners." [Online]. Available: https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/. [Accessed: 15-Sep-2019].
[198] X. Zheng, Y. Zhang, J. Zhang, and W. Hu, "Design Impedance Mismatch Physical Unclonable Functions for IoT Security," *Act. Passiv. Electron. Components*, vol. 2017, pp. 1–8, 2017.
[199] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21046–21056, 2017.
[200] G. Sun *et al.*, "Efficient location privacy algorithm for Internet of Things (IoT) services and applications," *J. Netw. Comput. Appl.*, vol. 89, pp. 3–13, 2017.
[201] C. Shi, "A Novel Ensemble Learning Algorithm Based on D-S Evidence Theory for IoT Security," *Comput. Mater. Contin.*, vol. 57, no. 3, pp. 635–652, 2018.
[202] P. Salva-Garcia, J. M. Alcaraz-Calero, Q. Wang, J. B. Bernabe, and A. Skarmeta, "5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks," *Secur. Commun. Networks*, vol. 2018, pp. 1–21, 2018.
[203] B. Santos, V. T. Do, B. Feng, and T. Van Do, "Identity Federation for Cellular Internet of Things," in *Proceedings of the 2018 7th International Conference on Software and Computer Applications - ICSCA 2018*, 2018.
[204] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Networks*, vol. 4, no. 2, pp. 118–137, Apr. 2018.
[205] R. Leveugle, A. Mkhinini, and P. Maistri, "Hardware Support for Security in the Internet of Things: From Lightweight Countermeasures to Accelerated Homomorphic Encryption," *Information*, vol. 9, no. 5, p. 114, 2018.
[206] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digit. Commun. Networks*, vol. 4, no. 3, pp. 149–160, 2018.
[207] A. Molina Zarca, J. Bernal Bernabe, I. Farris, Y. Khettab, T. Taleb, and A. Skarmeta, "Enhancing IoT security through network softwarization and virtual security appliances," *Int. J. Netw. Manag.*, vol. 28, no. 5, p. e2038, Sep. 2018.
[208] G. Li, P. Wang, and H. Zhang, "High performance bistable weak physical unclonable function for IoT security," *IEICE Electron. Express*, vol. 15, no. 21, pp. 20180879–20201808, 2018.
[209] J. R and P. Chandran, "Secure and Dynamic Memory Management Architecture for Virtualization Technologies in IoT Devices," *Futur. Internet*, vol. 10, no. 12, p. 119, 2018.
[210] D. Díaz López *et al.*, "Developing Secure IoT Services: A Security-Oriented Review of IoT Platforms," *Symmetry (Basel).*, vol. 10, no. 12, p. 669, 2018.
[211] B. Sudqi Khater, A. W. Bin Abdul Wahab, M. Y. I. Bin Idris, M. Abdulla Hussain, and A. Ahmed Ibrahim, "A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing," *Appl. Sci.*, vol. 9, no. 1, p. 178, 2019.
[212] M. Kose, S. Tascioglu, and Z. Telatar, "RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum," *IEEE Access*, vol. 7, pp. 18715–18726, 2019.
[213] F. Xiao, Z. Lin, Y. Sun, and Y. Ma, "Malware Detection Based on Deep Learning of Behavior Graphs," *Math. Probl. Eng.*, vol. 2019, pp. 1–10, 2019.
[214] J. C.-W. Lin, J. M.-T. Wu, P. Fournier-Viger, Y. Djenouri, C.-H. Chen, and Y. Zhang, "A Sanitization Approach to Secure Shared Data in an IoT Environment," *IEEE Access*, vol. 7, pp. 25359–25368, 2019.
[215] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating Brute Force Attack Patterns in IoT Network," *J. Electr. Comput. Eng.*, vol. 2019, pp. 1–13, 2019.
[216] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy Depletion Attacks in Low Power Wireless Networks," *IEEE Access*, vol. 7, pp. 51915–51932, 2019.
[217] Y. Shen, Y. Li, H. Kang, X. Sun, Q. Chen, and C. Zang, "A Security Protocol Model of Internet of Things for Resisting Known Plaintext Attack," *J. Phys. Conf. Ser.*, vol. 1176, p. 42001, 2019.
[218] O. Sahinaslan, "Encryption protocols on wireless IoT tools," *AIP Conf. Proc.*, vol. 2086, no. 1, p. 30036, Apr. 2019.
[219] F. Servida and E. Casey, "IoT forensic challenges and opportunities for digital traces," *Digit. Investig.*, vol. 28, pp. S22–S29, Apr. 2019.
[220] A. Bellini, E. Bellini, M. Gherardelli, and F. Pirri, "Enhancing IoT Data Dependability through a Blockchain Mirror Model," *Futur. Internet*, vol. 11, no. 5, p. 117, 2019.
[221] Y. Sun and B. Lo, "An Artificial Neural Network Framework for Gait-Based Biometrics," *IEEE J. Biomed. Heal. Informatics*, vol. 23, no. 3, pp. 987–998, 2019.
[222] L. Marin, "White Box Implementations Using Non-Commutative Cryptography," *Sensors* , vol. 19, no. 5. 2019.
[223] Y.-H. Lin, C.-H. Hsia, B.-Y. Chen, and Y.-Y. Chen, "Visual IoT Security: Data Hiding in AMBTC Images Using Block-Wise Embedding Strategy," *Sensors*, vol. 19, no. 9, p. 1974, 2019.

[224] H. Watanabe and H. Fan, “A Novel Chip-Level Blockchain Security Solution for the Internet of Things Networks,” *Technologies*, vol. 7, no. 1, p. 28, 2019.
[225] S. Sathyadevan, K. Achuthan, R. Doss, and L. Pan, “Protean Authentication Scheme – A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments,” *IEEE Access*, vol. 7, pp. 92419–92435, 2019.
[226] W. Razouk, D. Sgandurra, and K. Sakurai, “A new security middleware architecture based on fog computing and cloud to support IoT constrained devices,” in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning - IML ’17*, 2017.
[227] S. Okul and M. Ali Aydin, “Security Attacks on IoT,” in *2017 International Conference on Computer Science and Engineering (UBMK)*, 2017, pp. 1–5.
[228] Z. Čekerevac, Z. Dvorak, L. Prigoda, and P. Čekerevac, “INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS – SECURITY AND ECONOMIC RISKS,” *MEST J.*, vol. 5, no. 2, pp. 15–5, Jul. 2017.
[229] A. D. Oza, G. Naresh Kumar, and M. Khorajiya, *Survey of Snaring Cyber Attacks on IoT Devices with Honeypots and Honeynets*. 2018.
[230] D. M. Junior, W. Rodrigues, and K. Gama, “Towards a Multilayer Strategy Against Attacks on IoT Environments,” *Proc. 1st Int. Work. Softw. Eng. Res. Pract. Internet Things*, pp. 17–20, 2019.
[231] H. Alaiz-Moreton, J. Aveleira-Mata, J. Ondicol-Garcia, A. L. Muñoz-Castañeda, I. García, and C. Benavides, “Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol,” *Complexity*, vol. 2019, pp. 1–11, 2019.
[232] and M. S. Prasesh Adina, Raghav H. Venkatnarayan, “Impacts & Detection of Network Layer Attacks on IoT Networks.”
[233] F. Dang *et al.*, “Understanding Fileless Attacks on Linux-based IoT Devices with HoneyCloud,” 2019.
[234] T. Kawamura, M. Fukushi, Y. Hirano, Y. Fujita, and Y. Hamamoto, “A network-based event detection module using NTP for cyber attacks on IoT,” in *Proceedings - 2018 6th International Symposium on Computing and Networking Workshops, CANDARW 2018*, 2018.
[235] J. Zhang, R. S. Blum, and H. V Poor, “Approaches to Secure Inference in the Internet of Things: Performance Bounds, Algorithms, and Effective Attacks on IoT Sensor Networks,” *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 50–63, 2018.
[236] M. N. Islam and S. Kundu, “Poster Abstract: Preserving IoT Privacy in Sharing Economy Via Smart Contract,” in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018, pp. 296–297.
[237] E. H. Teguig and Y. Touati, “Security in Wireless Sensor Network and IoT: An Elliptic Curves Cryptosystem based Approach,” in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2018, pp. 526–530.
[238] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019.
[239] J. P. Chin, V. A. Diehl, and K. L. Norman, “Development of an Instrument Measuring User Satisfaction of the Human-computer Interface,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1988, pp. 213–218.
[240] J. Nielsen, “Usability inspection methods,” *Conf. Hum. Factors Comput. Syst. - Proc.*, vol. 1994-April, pp. 413–414, 1994.
[241] “10 Usability Heuristics for User Interface Design.” [Online]. Available: https://www.nngroup.com/articles/ten-usability-heuristics/. [Accessed: 03-Oct-2019].
[242] F. D. Davis, “Preparation of Rutile TiO 2 Films by RF Magnetron Sputtering Related content Role of He Gas Mixture on the Growth of Anatase and Rutile TiO 2 Films in RF Magnetron Sputtering Kunio Okimura and Akira Shibata - Deposition of High-Quality TiO 2 Films by RF M,” *Japanese J. Appl. Phys. Kunio Okimura al Jpn. J. Appl. Phys*, vol. 34, no. September, 1989.

Table A-0 Components in Smart Home Case-Study

Item Nu.	Component	Purpose of Use	Connectivity
1	Smart sensors	For measuring temperature\ humidity\gas and sending info to the related sub-component.	Zig-bee
2	Smart camera	For surveillance and recording everything in its view and sensing motion	Wi-Fi
3	Smart lock	Remotely locking/unlocking the house door.	NFC, Zig-bee, RFID
4	Smart garage	For keeping allowed resident's cars securely.	Near Field Communication (NFC)
5	Smart thermostat	For controlling HVAC issues based on the user preference automatically	Zig-bee, Wi-Fi
6	Smart washing machine	For turning on and of remotely , informing residents about start and finish time of washing and also sending information about forgotten clothes.	Wi-Fi
7	Smart assistant	Smart assistant like Alexa or Siri which recognizes its owner via its voice and responds requests of its owner.	Wi-Fi
8	Smart refrigerator	Automatic ordering shopping list.	Wi-Fi
9	Smart light	Automatic control of lights based on existence of home residents, motion sensors, and preferences.	Bluetooth
10	Smart windows	For ventilation purpose opening and closing the window automatically via commands coming from smart thermostat.	Wi-Fi
11	Smart insulin pen	One of the residents of the smart home has diabetes. This pen is for calculating glucose level in his blood and injecting the needed amount of insulin.	Z-Wave
12	Smart device	It is a smart phone or tablet for controlling smart home.	Wi-Fi, NFC, Bluetooth
13	Smart Hub	It is a control unit which collect info from subsystem, a bridge among sub-components, cloud and smart device.	All protocols mentioned previously.
14	Cloud environment	Data collected from systems are sent to this environment. System configurations and, directions of operation are kept in here and sent to the systems. Applications are run on this cloud environment. Triggers and alarms for certain thresholds are stored in here According to the configuration certain actions are implemented	

Table A-2 Security Targets and Definitions

Security Targets and Abbreviations	**Meaning**
Confidentiality (C)	Data can be accessed by only authorized users.
Integrity (I)	Data is preserved with original state, no modification or tampering have been done.
Availability (A)	Resource or data can be reachable for the authorized entities whenever requested.
Non-repudiation (NR)	System can identify if an action occurs or not.
Privacy (P)	System provides mechanism for entities in the IoT ecosystem to keep their sensitive information secret.
Auditability (AU)	IoT system keeps the logs of the actions and can present whenever needed.
Accountability (AC)	All the entities in the ecosystem know every action is under control and take responsibility of their own actions.
Trustworthiness (TW)	Ensuring the ability of an IoT system to prove identity and confirm trust in third party

Name: Surname: E-mail address:

(Before Using SIDE)

Table A-3 Threats and Countermeasures in Smart Home System

Item Nu.	Threat	Compromised Security Target (Abbreviation)	Countermeasure

(After Using SIDE)

Table A-4 Threats and Countermeasures in Smart Home System

Item Nu.	Threat	Compromised Security Target (Abbreviation)	Countermeasure

APPENDIX C

TABLES WITH VALUES IN THE IOT DATABASE

Table C-1 Threats table in IOT Database

TABLE NAME:**THREATS$**				
id	threat_name	compromised_security_target	threat_topic id	threat_after_2017
1	Object tempering	ALL	1	FALSE
2	Outage attack	A,AC,P,AU,NP	1	FALSE
3	Object replication	ALL	1	FALSE
4	Camouflage	ALL	1	FALSE
5	Side-channel attacks	C, AU, NR, P	1	FALSE
6	Tag cloning	ALL	1	FALSE
7	Social engineering	ALL	1	FALSE
8	Physical damage	ALL	1	FALSE
9	Malicious Code In-jection	ALL	1	FALSE
10	Hardware Trojans	ALL	1	FALSE
11	Object jamming	ALL	1	FALSE
12	Tag Tempering	ALL	1	FALSE
13	Killing Tag	ALL	2	FALSE
14	Spoofing	ALL	2	FALSE
15	Man in the middle	C, I, P, NR	2	FALSE
16	Tracking	P, NR	2	FALSE
17	Virus	P, I, AU, TW,NR, C	2	FALSE
18	Evesdropping	C, NR, P	2	FALSE
19	Replay	C,I,AC,NR,P	2	FALSE
20	RFID unauthorized access	All	2	FALSE
21	Eavesdropping	C, NR, P	3	FALSE
22	Data modification	ALL	3	FALSE
23	data corruption	A, AC, AU, NR	3	FALSE
24	Relay attack	C, I, AC, NR, P	3	FALSE
25	Data insertion	P, I, AU, TW, NR	3	FALSE
26	Man-in-the middle	C, I, P, NR	3	FALSE
27	Sniffing	C, NR, P	4	FALSE

28	Replay attack	C,I,AC,NR,P	4	FALSE
29	ZED Sabotage attack	All	4	FALSE
30	Obtaining keys	P,I,AU,TW,NR	4	FALSE
31	Redirecting Communication	C, I, AC, NR, P	4	FALSE
32	Bluejacking	NR, AU, TW, AU	5	FALSE
33	Bluebugging	All	5	FALSE
34	Interception	C,NR,P	5	FALSE
35	DoS	A AC, AU, NR, P	5	FALSE
36	Bluesnarfing	All	5	FALSE
37	Spoofing	P,I,AU, TW, NR	5	FALSE
38	Hijacking	All	5	FALSE
39	FMS	P, I, AU, TW,	6	FALSE
40	Korek,	P, I, AU, TW,NR, C	6	FALSE
41	Chopchop,	P, I, AU, TW,NR, C	6	FALSE
42	Fragmentation,	P, I, AU, TW,NR, C	6	FALSE
43	PTW	P, I, AU, TW,NR, C	6	FALSE
44	Google,replay	P, I, AU, TW,NR, C	6	FALSE
45	Michael	P, I, AU, TW,NR, C	6	FALSE
46	Ohigashi-Morii	P, I, AU, TW, NR,	6	FALSE
47	Dictionary Attack	P, I, AU, TW, NR,C	6	FALSE
48	Selective forward attack	C,I,AC,NR,P	7	FALSE
49	Sniffing attack	C, NR, P	7	FALSE
50	Sybil attack	C,I,AC,NR,P	7	FALSE
51	Wormhole attack	C,I,AC,NR,P	7	FALSE
52	Blackhole attack	C,I,AC,NR,P	7	FALSE
53	Identity attack	A, AC, I	7	FALSE
54	Hello flood attack	C,I,AC,NR,P, A	7	FALSE
55	Version attack	C,I,AC,NR,P, A	7	FALSE
56	Sinkhole attack	A, C, I	7	FALSE
57	Fragmentation attack	P,I,AU,TW,NR	8	FALSE
58	Authentication attack	C, I, P, NR	8	FALSE
59	Confidentiality attack	C, I, P, NR	8	FALSE
60	TCP SYN flood	A,AC,AU,NR,P	9	FALSE
61	UDP flood	A,AC,AU,NR,P	9	FALSE
62	TCP-UDP Port scan	A,AC,AU,NR,P	9	FALSE
63	TCP-UDP session hijacking	P,I,AU,TW,NR, C	9	FALSE
64	TCP-UDP Fragmentation	A,AC,AU,NR,P	9	FALSE
65	XMPPloit	P,I,AU,TW,NR	10	FALSE
66	Sniffing	C, NR, P	10	FALSE
67	Pre-shared key attack	P,I,AU,TW,NR, C	10	FALSE
68	MITM	C, I, P, NR	10	FALSE

69	Buffer overflow	P,I,AU,TW,NR, C	10	FALSE
70	XMPP: Authentication attack	P,I,AU,TW,NR, C	10	FALSE
71	Xmpp bomb	P,I,AU,TW,NR, C	10	FALSE
72	Daemon crash	P,I,AU,TW,NR, C	10	FALSE
73	Padding oracle (Thirteen)	P,I,AU,TW,NR, C	11	FALSE
74	Time	P,I,AU,TW,NR, C	11	FALSE
75	Klima03	P,I,AU,TW,NR, C	11	FALSE
76	Beast	P,I,AU,TW,NR, C	11	FALSE
77	Diffie-Hellman parameters	P,I,AU,TW,NR, C	11	FALSE
78	SSL stripping	P,I,AU,TW,NR, C	11	FALSE
79	DOS Exposure	C, I, PP	12	FALSE
80	Data loss	ALL	12	FALSE
81	Data Scavenging	C, I, P	12	FALSE
82	VM Hopping	ALL	12	FALSE
83	Malicious VM Creation	ALL	12	FALSE
84	Insecure VM Migration	All	12	FALSE
85	Account Hijacking	ALL	12	FALSE
86	Data Manipulation	ALL	12	FALSE
87	VM Escape	ALL	12	FALSE
88	Data leakage	C, I	12	FALSE
89	Dos	P , A	12	FALSE
90	Hash collision	C, I	12	FALSE
91	Brute-force	C, I	12	FALSE
92	Virus	All	13	FALSE
93	Backdoor attack	ALL	13	FALSE
94	Malicious Scripts	ALL	13	FALSE
95	Phishing Attacks	ALL	13	FALSE
96	Brute-force search attack	ALL	13	FALSE
97	SQL injection	ALL	14	FALSE
98	Cross-Site Scripting	P,I,AU,TW,NR, C	14	FALSE
99	Cross Site Request	P,I,AU,TW,NR, C	14	FALSE
100	Forgery	All	14	FALSE
101	Exploitation of a misconfiguration	All	14	FALSE
102	DoS attack	A,AC,AU,NR,P	14	FALSE
103	Malware	All	15	FALSE
104	Path-based DOS attack	A,AC,AU,NR,P	15	FALSE
105	Reprogram attack	P,I,AU,TW,NR, C	15	FALSE
106	Control hijacking	All	15	FALSE
107	Reverse Engineering	All	15	FALSE
108	Eavesdropping	C, NR, P	15	FALSE
109	Worms	All	15	FALSE

Table C-2 Countermeasures Table in IOT Database

TABLE NAME:COUNTERMASURES$				
id	countermeasures	threat_id	reference_id	countermesure_after_2017
1	Tamper proofing and self-destruction,	1	25	FALSE
2	Minimizing information leakage [25]	1	25	FALSE
3	Integrating Physically Unclonable Function (PUF) into object [26]	1	26	FALSE
4	Secure physical design [27]	2	27	FALSE
5	Encryption,	3	8	FALSE
6	Lightweight cartographic mechanisms,	3	8	FALSE
7	Hash-based techniques [8]	3	8	FALSE
8	Securing firmware update,	4	8	FALSE
9	Encryption	4	8	FALSE
10	Hash-based schemes,	4	8	FALSE
11	Authentication Technique [8]	4	8	FALSE
12	Blocking,	5	8	FALSE
13	Isolation,	5	8	FALSE
14	Kill command,	5	8	FALSE
15	Sleep Command	5	8	FALSE
16	Tamper proofing and self-destruction,	5	8	FALSE
17	Mimimizing information leakage	5	8	FALSE
18	Obfuscating techniques [8]	5	8	FALSE
19	Encryption	6	8	FALSE
20	Hash-based schemes[28]	6	28	FALSE
21	Authentication Technique [8]	6	8	FALSE
22	Blocking,	6	8	FALSE
23	Isolation,	6	8	FALSE
24	Kill command,	6	8	FALSE
25	Sleep Command	6	8	FALSE
26	Distance Estimation[8]	6	8	FALSE
27	Integrating PUFs into RFID tags [29]	6	29	FALSE
28	Back up techniques,	7	29	FALSE
29	Education of IoT users	7	29	FALSE
30	Tamper proofing and self-destruction	7	30	FALSE
31	Secure physical design	8	30	FALSE

32	Tamper proofing and self-destruction	8	8	FALSE
33	Tamper proofing and self-destruction	9	8	FALSE
34	IDS	9	8	FALSE
35	Side-channel signal analysis (based on path-delay fingerprint, based on symmetry breaking, based on thermal and power, based on machine learning),	10	8	FALSE
36	Trojan activation [31]	10	31	FALSE
37	Spread Spectrum,	11	31	FALSE
38	Priority messages	11	31	FALSE
39	Lower duty cycle	11	31	FALSE
40	Region mapping, [32]	11	32	FALSE
41	Integrating PUFs into RFID tags,	12	32	FALSE
42	Encryption	12	32	FALSE
43	Hash-based schemes[28]	12	28	FALSE
44	Tamper-release layer RFID	12	28	FALSE
45	Alarm Function for active Tags[33]	12	33	FALSE
46	Users or objects authentication [56]	13	56	FALSE
47	RFID authentication and encryption techniques [51]	14	51	FALSE
48	Encryption of the RFID communication channel [45]	15	45	FALSE
49	Authentication techniques	15	45	FALSE
50	Kill/sleep command	16	45	FALSE
51	Isolation	16	45	FALSE
52	Anonymous tag	16	45	FALSE
53	Blocking[57]	16	57	FALSE
54	Blocking strange bits from the tag using well-developed middleware	17	57	FALSE
55	Bounds checking and parameter	17	41	FALSE
56	Encryption techniques	18	41	FALSE
57	Shift data to the back end	18	41	FALSE
58	A challenge and response mechanism	19	41	FALSE
59	The time-based or counter- based scheme	19	41	FALSE
60	Network authentication	20	40	FALSE
61	Secure channel (authentication and encryption) [43]	21	43	FALSE

62	Changing the baud rate(use of 106k Baud),	22	43	FALSE
63	The continuous monitoring of RF field, secure channel[43]	22	43	FALSE
64	The detection of RF fields during data transmission [43]	23	43	FALSE
65	Timing(enforcing stricter timing restraints on responses) [58]	24	58	FALSE
66	Distance Bounding (Round-Trip-Time (RTT) of cryptographic challenge-response pairs [59]	24	59	FALSE
67	Objects reply with no delay,	25	59	FALSE
68	A secure channel between the NFC objects	26	59	FALSE
69	A secure channel between the two objects [46]	26	46	FALSE
70	Implementing high security by preinstalling the network key on the ZigBee devices [60]	27	60	FALSE
71	The implementation of freshness counter (a 32-bit frame counter), [61]	28	61	FALSE
72	The remote alerting system for warning about power failures of ZigBee objects	29	61	FALSE
73	Configure the legitimate ZEDs in a cyclic sleep mode[61]	29	61	FALSE
74	Out-of-band key loading method Using [62]	30	62	FALSE
75	Secure network admission control, preconfigure nodes with the Trust Center address [63].	31	63	FALSE
76	Putting objects on nondiscoverable mode, stay offline [48]	32	48	FALSE
77	Firmware and software update, use of RF signatures [64]	33	64	FALSE
78	Data/voice encryption	34	64	FALSE
79	Increasing user understanding of security issues	34	64	FALSE
80	Minimization of transmit powers	34	64	FALSE

81	Using only long PIN codes [64], pairing process in private settings [48]	34	48	FALSE
82	Keeping a list of suspicious devices [65]	35	65	FALSE
83	Putting phones on nondiscoverable mode [48]	36	48	FALSE
84	Stay offline[64], verify incoming transmission	36	64	FALSE
85	Secure UUID - Rotating UUIDw/ limited token scope,	37	64	FALSE
86	Private Mode with Rotating UUID	37	64	FALSE
87	Secure Shuffling randomly rotating UUID[66]	37	66	FALSE
88	Cloud-based token authentication	38	66	FALSE
89	Secure Communications	38	66	FALSE
90	Software Lock[66]	38	66	FALSE
91	The use of RC4-based SSL (TLS)	39	67	FALSE
92	The use of higher-level security mechanisms such as IPsec [67]	39	67	FALSE
93	The use of a very short rekeying time,	40	67	FALSE
94	Disabling the sending of MIC failure report	40	67	FALSE
95	Disabling TKIP and using a CCMP only network [68],	40	68	FALSE
96	The use of higher-level security mechanisms such as IPsec, DTLS, HTTP/TLS or CoAP/DTLS, DTLS for CoAp[69]	40	69	FALSE
97	The use of a very short rekeying time,	41	69	FALSE
98	Disabling the sending of MIC failure report	41	69	FALSE
99	Disabling TKIP and using a CCMP only network [68],	41	68	FALSE

100	The use of higher-level security mechanisms such as IPsec, DTLS, HTTP/TLS or CoAP/DTLS, DTLS for CoAp[69]	41	69	FALSE
101	The use of a very short rekeying time,	42	69	FALSE
102	Disabling the sending of MIC failure report	42	69	FALSE
103	Disabling TKIP and using a CCMP only network [68],	42	68	FALSE
104	The use of higher-level security mechanisms such as IPsec, DTLS, HTTP/TLS or CoAP/DTLS, DTLS for CoAp[69]	42	69	FALSE
105	The use of a very short rekeying time,	43	69	FALSE
106	Disabling the sending of MIC failure report	43	69	FALSE
107	Disabling TKIP and using a CCMP only network [68],	43	68	FALSE
108	The use of higher-level security mechanisms such as IPsec, DTLS, HTTP/TLS or CoAP/DTLS, DTLS for CoAp[69]	43	69	FALSE
109	The use of a very short rekeying time,	44	69	FALSE
110	Disabling the sending of MIC failure report	44	69	FALSE
111	Disabling TKIP and using a CCMP only network [68],	44	68	FALSE
112	The use of higher-level security mechanisms such as IPsec, DTLS, HTTP/TLS or CoAP/DTLS, DTLS for CoAp[69]	44	69	FALSE
113	Deactivating QoS or settingthe rekeying timout to a low value[70]	45	70	FALSE
114	Disable TKIP and switch to the more secure CCMP	45	70	FALSE
115	Security protocols based on AES [71]	46	71	FALSE
116	The use of salt technique [72]	47	72	FALSE
117	Encryption technique	48	79	FALSE

118	Disjoint path or dynamic path between parent and children [79]	48	79	FALSE
119	Heartbeat protocol	48	79	FALSE
120	IDS solution	48	79	FALSE
121	Encryption [81]	49	81	FALSE
122	Classification-based Sybil detection (BCSD) [82]	50	82	FALSE
123	Markle tree authentication [82]	51	82	FALSE
124	Binding geographic information [83]	51	82	FALSE
125	The implementation of RPL in RIOT OS, Tiny OS,	52	83	FALSE
126	Monitoring of counters [84]	52	84	FALSE
127	SVELTE [85]	52	85	FALSE
128	Tracking number of instances of each identity,	53	85	FALSE
129	Storing Identities of nodes in RPL	53	85	FALSE
130	Ddistributed hash table (DHT) [79]	53	86	FALSE
131	Link-layer metric as a parameter in the selection of the default route [86]	54	86	FALSE
132	Version Number and rank authentication	55	86	FALSE
133	TRAIL [87]	55	87	FALSE
134	IDS solution [85]	56	85	FALSE
135	Identity certificates	56	85	FALSE
136	Parent fail-over [88],	56	88	FALSE
137	Rank authentication technique	56	88	FALSE
138	Split buffer approach	57	88	FALSE
139	Content chaining approach [89]	57	89	FALSE
140	Add new fields to the protocol fragmentation header	57	89	FALSE
141	Authentication mechanism [90]	58	90	FALSE
142	Moving Target IPv6 Defence in 6LoWPAN [91]	59	91	FALSE
143	SYN Cache mechanism [94]	60	94	FALSE
144	SYN cookies	60	94	FALSE
145	Firewalls , switches and routers with rate-limiting and ACL capability [94]	60	94	FALSE
146	Firewalls	61	94	FALSE
147	Deep Packet Inspection [104]	61	104	FALSE

148	Network intrusion detection system(NIDS)	62	104	FALSE
149	External firewall[93]	62	93	FALSE
150	Encrypted transport protocols[105] such as Secure Shell (SSH)	63	105	FALSE
151	Secure Socket Layers (SSL)	63	105	FALSE
152	Internet Protocol Security (IPSec)	63	105	FALSE
153	Blacklisting/whitelisting mechanisms	64	105	FALSE
154	A secure proxy [97]	64	97	FALSE
155	SSL	65	97	FALSE
156	DTLS [106]	66	106	FALSE
157	The use of the ephemeral keys as in ECDH key exchange guarantees PFS[99]	67	99	FALSE
158	Secure MQTT[107]	68	107	FALSE
159	Close the opening ports	69	107	FALSE
160	Awareness of security	69	40	FALSE
161	Authentication mechanism [90]	70	90	FALSE
162	Validating parsers using Document Type Definitions (DTD) and XML Schemas [108]	71	108	FALSE
163	Good implementation of TLS	72	108	FALSE
164	The encryption-then-MAC instead of the TLS default of MAC-then-encryption [109].	73	109	FALSE
165	Disabling TLS compression [110]	74	110	FALSE
166	TLS 1.1, [111]	75	111	FALSE
167	Authenticated encryption algorithm like AES-GCM [109]	76	109	FALSE
168	The of predefined DH groups [112]	77	112	FALSE
169	HTTP Strict Transport Security (HSTS) [113]	78	113	FALSE
170	Strong encryption techniques	79	113	FALSE
171	Key management methods [118]	79	118	FALSE
172	Strong key generation, storage and management, and destruction practices [119],	80	119	FALSE
173	Backup and retention strategies.	80	119	FALSE
174	Symmetric key Cryptography [120]	81	120	FALSE

175	None [120]	82	120	FALSE
176	Mirage [120]	83	120	FALSE
177	Protection aegis for live migration of VMs(PALM) [121]	84	121	FALSE
178	VNSS offers protection through virtual machine live migration [122]	84	122	FALSE
179	Identity and access management guidance, dynamic credentials [123]	85	123	FALSE
180	Web application scanners (such as firewall) [124]	86	124	FALSE
181	Trusted cloud computing platform	87	124	FALSE
182	Trusted Virtual Datacenter	87	124	FALSE
183	HyperSafe	87	124	FALSE
184	Properly configuring the host/guest interaction	87	124	FALSE
185	Digital Signature	88	124	FALSE
186	Fragmentation-redundancy-scattering (FRS) technique,	88	124	FALSE
187	Homomorphic encryption [126],	88	126	FALSE
188	Encryption[120]	88	120	FALSE
189	Policies provided by providers [120]	89	120	FALSE
190	Modern hashing algorithms like SHA-2, SHA-3, or bcrypt[127]	90	127	FALSE
191	Lockout mechanisms	91	127	FALSE
192	IP address lock-out	91	127	FALSE
193	Detection tools	91	127	FALSE
194	Brute force site scanners[128]	91	128	FALSE
195	Security updates	92	147	FALSE
196	Side-channel analysis	92	147	FALSE
197	Verify software integrity [147	92	147	FALSE
198	Control flow [148]	92	148	FALSE
199	Protective Software	92	149	FALSE
200	Circuit design modification	93	150	FALSE
201	Firewalls [149]	94	149	FALSE
202	Crptographic methods	95	149	FALSE
203	Securing firware update	96	149	FALSE
204	Cryptography methods	96	149	FALSE
205	Data validation	97	149	FALSE
206	Pretesting [150]	97	150	FALSE

207	Network-based intrusion detection (IDS)	97	150	FALSE
208	Data validation [17]	98	17	FALSE
209	Including a unique	99	17	FALSE
210	Disposable and random token [17]	99	17	FALSE
211	A strong application architecture	100	17	FALSE
212	Perform scans and audits continuously [151]	100	151	FALSE
213	Access Control Lists[152]	101	152	FALSE
214	Security updates	102	152	FALSE
215	Side-channel analysis	102	152	FALSE
216	Verify software integrity	102	152	FALSE
217	Control flow [148])	102	148	FALSE
218	IoT Scanner [153]	102	153	FALSE
219	Combining packet authentication and anti replay protection [154]	103	154	FALSE
220	Secure the reprogramming process [154]	104	154	FALSE
221	Use Safe programming languages	105	154	FALSE
222	Audit software	105	154	FALSE
223	Add runtime code [155]	105	155	FALSE
224	Tamper proofing and self-destruction(obfuscation)	106	155	FALSE
225	A secure channel	107	155	FALSE
226	Security updates, side-channel analysis, verify software integrity [147], control flow [148]), protective Software	108	147	FALSE

Table C-3 References Table in IOT Database

TABLE NAME:REFERENCES1	
id	Reference_Information
1	F. DaCosta, “Rethinking the Internet of Things: A scalable approach to connecting everything.” Apress Open, p. 185, 2013.
2	D. Konstantas, “An overview of wearable and implantable medical sensors.” Yearbook of medical informatics, pp. 66–69, 2007.
3	J. Pike, “Internet of Things - Standards for Things,” 2014.
4	E. Alsaadi and A. Tubaishat, “Internet of Things: Features, Challenges, and Vulnerabilities,” International Journal of Advanced Computer Science and Information Technology (IJACSIT), vol. 4, no. 1, pp. 1–13, 2015.
5	S. Institute, “InfoSec Reading Room Securing the Internet of Things Survey,” p. 22, 2014.
6	E&Y, “Cybersecurity and the Internet of Things,” E&Y, no. March, pp. 1–15, 2015.
7	European Research Cluster on The Internet of Things (IERC), “Inter-net of Things: IoT Governance, Privacy and Security Issues,” European Research Cluster on the Internet of Things, p. 128, 2015.
8	A. Mohsen Nia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” IEEE Transactions on Emerging Topics in Computing, vol. PP, no. 99, p. d, 2016.
9	J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
10	L. Atzori, A. Iera and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, oct 2010.
11	Cisco, “The Internet of Things Reference Model,” Internet of Things World Forum, pp. 1–12, 2014.
12	S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, “IoT architecture challenges and issues: Lack of standard-ization,” FTC 2016 - Proceedings of Future Technologies Conference, no. December, pp. 731–738, 2017.
13	Z.-K. Zhang, M. C. Y. Cho, and S. Shieh, “Emerging Security Threats and Countermeasures in IoT,” Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security - ASIA CCS ’15, pp. 1–6, 2015.
14	Andreas Fink, IoT: Lack of standards becoming a threat.
15	L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” 2010.
16	S. Agrawal, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” Abakos, vol. 1, no. 2, pp. 78–95, 2013.
17	B. Dorsemaine, J. P. Gaulier, J. P. Wary, N. Kheir, and P. Urien, “A new approach to investigate IoT threats based on a four layer model,” IEEE Transactions on Emerging Topics in Computing, no. Notere, 2016.
18	D. Kajaree and R. Behera, “A Survey on IoT Security Threats and Solutions,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, no. 2, pp. 1302–1309, 2017.
19	J. S. Kumar and D. R. Patel, “A Survey on Internet of Things : Security and Privacy Issues,” International Journal of Computer Applications, vol. 90, no. 11, pp. 20–26, 2014.

20	S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed security model and threat taxonomy for the Internet of Things (IoT),” International Conference on Network Security and Applications, vol. 89 CCIS, pp. 420–429, 2010.
21	J. Guo and I. R. Chen, “A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems,” Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015, pp. 324–331, 2015.
22	Y. Cherdantseva and J. Hilton, “A Reference Model of Information Assurance & Security*.”
23	Symantec, “An Internet of Things Reference Architecture,” 2016.
24	J. Sen, “A Survey on Wireless Sensor Network Security,” Interna-tional Journal of Communication Networks and Information Security (IJCNIS), vol. 1, no. 2, 2009.
25	A. M. Nia, S. Member, S. Sur-kolay, and S. Member, “Physiological Information Leakage : A New Frontier in Health Information Security,” vol. 4, no. 3, pp. 321–334, 2015.
26	C. Wachsmann, “Physically Unclonable Functions (PUFs),” Morgan & Claypool Publishers, 2014.
27	D. Puthal, S. Nepal, R. Ranjan, and J. Chen, “Threats to Networking Cloud and Edge Datacenters in the Internet of Things,” IEEE Cloud Computing, vol. 3, no. 3, pp. 64–71, 2016.
28	W. I. Khedr, “SRFID: A hash-based security scheme for low cost RFID systems,” elsevier, 2013.
29	H.-h. Huang, L.-y. Yeh, and W.-j. Tsaur, “Ultra-Lightweight Mutual Authentication and Ownership Transfer Protocol with PUF for Gen2 v2 RFID Systems,” vol. II, pp. 16–19, 2016.
30	Nate Lord, “Social Engineering Attacks: Common Techniques & How to Prevent an Attack — Digital Guardian.”
31	N. Lesperance, S. Kulkarni, and K.-t. T. Cheng, “Hardware Trojan Detection Using Exhaustive Testing of k -bit Subspaces,” IEEE Access, pp. 755–760, 2015.
32	A. Davis, “A Survey of Wireless Sensor Network Architectures,” International Journal of Computer Science & Engineering Survey, vol. 3, no. 6, pp. 1–22, 2012.
33	Q. Xiao, T. Gibbons, and H. Lebrun, “RFID technology, security vulnerabilities and countermeasures,” Supply Chain, The Way to Flat Organisation, no. December, pp. 357–382, 2009.
34	H. Li and Y. Chen, “The Survey of RFID Attacks and Defenses,” ieee, pp. 0–3, 2012.
35	H. Salmani, “Hardware Trojan Attacks: Threat Analysis and Counter-measures,” ieee, pp. 247–276, 2014.
36	J. Deogirikar, “Security Attacks inIoT : A Survey,” International conference on I-SMAC, pp. 32–37, 2017.
37	Walters, “Security in distributed, grid, mobile, and pervasive comput-ing,” ACM, 2007.
38	G. Hernandez, O. Arias, D. Buentello, and Y. Jin, “Smart Nest Thermostat : A Smart Spy in Your Home,” Black Hat USA, pp. 1–8, 2014.
39	M. Polytechnic and M. Polytechnic, “RFID Security Issues & Chal-lenges,” ieee, 2014.
40	M. M. Ahemd, M. A. Shah, and A. Wahid, “IoT security: A layered approach for attacks & defenses,” 2017 International Conference on Communication Technologies (ComTech), pp. 104–110, 2017.
41	Q. Xiao, C. Boulet, and T. Gibbons, “RFID security issues in military supply chains,” Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007, pp. 599–605, 2007.

42	A. Elbagoury, A. Mohsen, M. Ramadan, and M. Youssef, “Practical provably secure key sharing for near field communication devices,” in 2013 International Conference on Computing, Networking and Communications (ICNC). IEEE, jan 2013, pp. 750–755.
43	N. B. Thorat and C. A. Laulkar, “Survey on Security Threats and Solutions for Near Field Communication,” pp. 291–295, 2014.
44	M. Roland, J. Langer, and J. Scharinger, “Practical Attack Scenarios on Secure Element-Enabled Mobile Devices,” in 2012 4th International Workshop on Near Field Communication. IEEE, mar 2012, pp. 19–24.
45	A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, “Classifying RFID attacks and defenses,” springer, vol. 12, no. 5, pp. 491–505, 2010.
46	E. Haselsteiner and K. Breitfuß, “Security in Near Near Field Com-munication (NFC) Strengths,” Semiconductors, vol. 11, no. 71, p. 71, 2006.
47	C. H. Chen, I. C. Lin, and C. C. Yang, “NFC attacks analysis and survey,” Proceedings - 2014 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2014, pp. 458–462, 2014.
48	N. Be-Nazir, I. Minar, and M. Tarique, “BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY,” International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 1, 2012.
49	M. Tan, “An Investigation of Bluetooth Security Threats,” ieee, 2011.
50	Ubertooth One, “Great Scott Gadgets - Ubertooth One.”
51	H. Jun Tay, J. Tan, and P. Narasimhan, “A Survey of Security Vulnerabilities in Bluetooth Low Energy Beacons,” 2016.
52	N. Chen, “Bluetooth Low Energy Based CoAP Communication in IoT CoAPNonIP: An Architecture Grants CoAP in Wireless Personal Area Network,” 2016.
53	M. Caneill and J.-L. Gilis, “Attacks against the WiFi protocols WEP and WPA,” 2010.
54	K., “Korek Attack,” 2004.
55	A. Bittau, M. Handley, and J. Lackey, “The Final Nail in WEP’s Coffin,” 2006.
56	I. R. Adeyemi Norafida Bt Ithnin, “Users Authentication and Privacy control of RFID Card,” 2012.
57	Gan Yong, He Lei, Li Na-na, and Zhang Tao, “An improved forward secure RFID privacy protection scheme,” in 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010). IEEE, mar 2010, pp. 273–276.
58	L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, “Practical relay attack on contactless transactions by using NFC mobile phones,” Cryptology and Information Security Series, vol. 8, pp. 21–32, 2012.
59	G. P. Hancke and M. G. Kuhn, “Attacks on time-of-flight distance bounding channels,” Proceedings of the first ACM conference on Wireless network security - WiSec ’08, pp. 194–202, 2008.
60	Cyber Security Community, “Different Attacks and Counter Measures Against ZigBee Networks — TCS Cyber Security Community.”
61	N. Vidgren, K. Haataja, J. L. Pati??o-Andres, J. J. Ram??rez-Sanchis, and P. Toivanen, “Security threats in ZigBee-enabled systems: Vulner-ability evaluation, practical experiments, countermeasures, and lessons learned,” Proceedings of the Annual Hawaii I
62	X. Fan, F. Susan, W. Long, and S. Li, “Security Analysis of Zigbee,” 2017.

63	K. Masica, “Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments,” 2007.
64	K. HAATAJA, “Security Threats and Countermeasures in Bluetooth-Enabled Systems,” 2009.
65	M. Keijo and H. Senior, “Bluetooth network vulnerability to Disclo-sure, Integrity and Denial-of- Service attacks,” vol. 17, 2005.
66	Gofor, “Common attacks and how Kontakt.io can protect you.”
67	A. Stubblefield, J. Ioannidis, and A. Rubin, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.” Ndss, no. Iv, 2002.
68	E. Tews and M. Beck, “Practical Attacks Against WEP and WPA,” Proceedings of the second ACM conference on Wireless network security, pp. 79–85, 2009.
69	C. Schmitt, T. Kothmayr, W. Hu, and B. Stiller, “Two-Way Authenti-cation for the Internet-of-Things,” springer, vol. 25, pp. 27–57, 2017.
70	M. Beck, “Enhanced TKIP Michael Attacks,” 2010.
71	T. Mekhaznia and A. Zidani, “Wi-Fi Security Analysis,” Procedia Computer Science, vol. 73, no. Awict, pp. 172–178, 2015.
72	Wikipedia, “Dictionary attack - Wikipedia.”
73	M. Beck, “Enhanced TKIP Michael Attacks,” 2010.
74	M. S. Ahmad, “WPA Too!” Defcon 18, p. 7, 2010.
75	J. Wright, “KillerBee: Practical ZigBee Exploitation Framework or ”Wireless Hacking and the Kinetic World”,” 2009.
76	J. Markert, M. Massoth, K.-P. Fischer-Hellmann, S. Furnell, and
77	M. Asim, “IoT Operating Systems and Security Challenges,” vol. 14, no. 7, p. 5500, 2016.
78	A. Mayzaud, R. Badonnel, and I. Chrisment, “A taxonomy of attacks in RPL-based internet of things,” International Journal of Network Security, vol. 18, no. 3, pp. 459–473, 2016.
79	P. Pongle and G. Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT,” 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015, vol. 00, no. c, pp. 0–5, 2015.
80	J. Sen, “Security in Wireless Sensor Networks.”
81	T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister,
82	K. Zhang, X. Liang, R. Lu, and X. Shen, “Sybil attacks and their defenses in the internet of things,” IEEE Internet of Things Journal, vol. 1, no. 5, pp. 372–383, 2014.
83	L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach,” ieee, 2005.
84	K. Chugh, A. Lasebae, and J. Loo, “Case Study of a Black Hole Attack on 6LoWPAN-RPL,” SECURWARE 2012, The Sixth Interna-tional Conference on Emerging Security Information, Systems and Technologies, no. c, pp. 157–162, 2012.
85	S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” Ad Hoc Networks, vol. 11, pp. 2661–2674, 2013.
86	L. Wallgren, S. Raza, and T. Voigt, “Routing Attacks and Counter-measures in the RPL-Based Internet of Things,” International Journal of Distributed Sensor Networks, vol. 794326, no. 11, 2013.
87	H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wahlisch,¨ “TRAIL: Topology Authentication in RPL,” 2013.

88	K. Weekly and K. Pister, “Evaluating sinkhole defense techniques in RPL networks,” Proceedings - International Conference on Network Protocols, ICNP, 2012.
89	R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, “6LoWPAN Fragmentation Attacks and Mitigation Mechanisms,” 2013.
90	L. M. L. Oliveira, J. J. Rodrigues, A. F. De Sousa, and V. M. Denisov, “Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms,” IEEE Transactions on Industrial Informatics, vol. 12, no. 6, pp. 2186–2195, 2016.
91	M. Sherburne, R. Marchany, and J. Tront, “Implementing moving target IPv6 defense to secure 6LoWPAN in the internet of things and smart grid,” in Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR ’14. New York, New
92	Stephane´ GARCIA, “Wireless Security and the IEEE 802.11 Stan-dards,” 2004.
93	McMaster University, “The Five-Layer TCP/IP Model: Descrip-tion/Attacks/Defense - Computing and Software Wiki,” 2008.
94	S. Kumarasamy and G. A. Shankar, “An Active Defense Mechanism for TCP SYN flooding attacks,” arXiv.org, pp. 1–6, 2012.
95	O. Zheng, J. Poon, and K. Beznosov, “Application-Based TCP Hijack-ing,” 2009.
96	D. Moore, G. M. Voelker, and S. Savage, “Inferring Internet Denial-of-Service Activity,” 2000.
97	Incapsula, “What is an IP Fragmentation Attack (Teardrop ICMP/UDP) — DDoS Attack Glossary — Incapsula.”
98	Toby Jaffey, “MQTT and CoAP, IoT Protocols.”
99	S. Jucker, “Master ’ s Thesis Securing the Constrained Application Protocol by Stefan Jucker,” no. October, pp. 1–103, 2012.
100	S. N. Swamy, “Security Threats in the Application layer in IOT Applications,” pp. 477–480, 2017.
101	Moxie Marlinspike, “SSLstrip.”
102	T. D. Juliano Rizzo, “Browser Exploit Against SSL/TLS Packet Storm.”
103	N. Mavrogiannopoulos, F. Vercauteren, V. Velichkov, and B. Preneel, “A cross-protocol attack on the TLS protocol,” fACM g Conference on Computer and Communications Security, pp. 62–72, 2012.
104	Incapsula, “What is a UDP Flood — DDoS Attack Glossary — Incapsula.”
105	B. S. Kevin Lam, David LeBlanc, “Theft On The Web: Theft On The
106	J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294– 1312, 2015.
107	M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, “Se-cure MQTT for Internet of Things (IoT),” Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015, pp. 746–751, 2015.
108	UsingXML, “White Space in XML Documents.”
109	P. Gutmann and University, “Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS),” pp. 1–7, 2014.
110	T. Be’ery and A. Shulman, “A Perfect CRIME? Only TIME Will Tell,” BlackHat Europe 2013, 2013.
111	A. Choudhury and D. Mcgrew, “AES Galois Counter Mode (GCM) Cipher Suites for TLS Status,” pp. 1–8, 2008.

112	D. Gillmor, “Negotiated Finite Field Diffie-Hellman Ephemeral Pa-rameters for Transport Layer Security (TLS),” pp. 1–29, 2016.
113	P. S.-A. Y. Sheffer, R. Holz, “Summarizing Known Attacks on Trans-port Layer Security (TLS) and Datagram TLS (DTLS),” pp. 1–13, 2015.
114	V. Klima, O. Pokorny, and T. Rosa, “Attacking RSA-based sessions in SSL/TLS,” Cryptographic Hardware and Embedded Systems Ches 2003, Proceedings, vol. 2779, pp. 426–440, 2003.
115	N. J. AlFardan and K. G. Paterson, “Lucky thirteen: Breaking the TLS and DTLS record protocols,” Proceedings - IEEE Symposium on Security and Privacy, pp. 526–540, 2013.
116	M. Wang, “Understanding security flaws of IoT protocols through honeypot tech- nologies MengWang,” 2013.
117	P. Du, “IoT Message Protocols: The Next Security Challenge for Service Providers? The State of IoT,” pp. 2–4, 2017.
118	C. Rong, S. T. Nguyen, and M. G. Jaatun, “Beyond lightning: A survey on security challenges in cloud computing,” Computers & Electrical Engineering, vol. 39, no. 1, pp. 47–54, jan 2013.
119	Cloud Security Alliance, “Cloud Security Alliance,” 2010.
120	S. Chandna, R. Singh, and F. Akhtar, “Data scavenging threat in cloud computing,” no. August, pp. 17–22, 2014.
121	Webopedia, “PALM.”
122	G. Xiaopeng, W. Sumei, and C. Xianqin, “VNSS: A network security sandbox for virtual computing environment,” Proceedings - 2010 IEEE Youth Conference on Information, Computing and Telecommunica-tions, YC-ICT 2010, pp. 395–398, 2010.
123	SYBASE, “Dynamic credentia.”
124	Tenable, “Tenable.io Web Application Scanning — Tenable.”
125	Z. Wang and X. Jiang, “HyperSafe: A lightweight approach to pro-vide lifetime hypervisor control-flow integrity,” Proceedings - IEEE Symposium on Security and Privacy, pp. 380–395, 2010.
126	N. P. Smart and F. Vercauteren, “Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes,” springer, pp. 420–443, 2010.
127	Eric Z Goodnight, “What Is SHAttered? SHA-1 Collision Attacks, Explained.”
128	ALIEN VAULT, “Brute Force Attack Mitigation: Methods & Best Practices — AlienVault,” 2016.
129	N. Kaaniche and M. Laurent, “Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms,” Computer Communications, vol. 111, pp. 120–141, 2017.
130	Claudia Chandra, “Data Loss vs. Data Leakage Prevention: What’s the Difference?” 2017.
131	Cloud Security Alliance, “Top Threats to Cloud Computing V1.0,” 2010.
132	W. Dawoud, I. Takouna, and C. Meinel, “Infrastructure as a service security: Challenges and solutions,” Informatics and Systems (INFOS), 2010 The 7th International Conference on, pp. 1–8, 2010.
133	W. A. Jansen, “Cloud hooks: Security and privacy issues in cloud com-puting,” Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 1–10, 2012.
134	B. Grobauer, T. Walloschek, and E. Stocker,¨ “Understanding cloud computing vulnerabilities,” IEEE Security and Privacy, vol. 9, no. 2, pp. 50–57, 2011.
135	B. A. Sullivan, “Securing the cloud: Cloud computer security techniques and tactics,” Security Journal, vol. 27, no. 3, pp. 338–340, jul 2014.

136	J. Rittinghouse and J. Ransome, Cloud computingnnImplementation, Management, and Security, 2010.
137	Kelly Jackson, “Hacker’s Choice: Top Six Database Attacks.”
138	M. Stevens, A. Lenstra, and B. de Weger, “Chosen-prefix Collisions for MD5 and Colliding X.509 Certificates for Dierent Identities,” nov 2007.
139	R. Singh, J. Singh, and R. Singh, “ATTACKS IN WIRELESS SEN-SOR NETWORKS : A SURVEY,” vol. 5, no. 5, pp. 10–16, 2016.
140	U. Sabeel and N. Chandra, “Categorized Security Threats in the Wire-less Sensor Networks : Countermeasures and Security Management Schemes,” vol. 64, no. 16, pp. 19–28, 2013.
141	J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, p. 39, apr 2004.
142	A. Tsow, “Phishing with Consumer Electronics: Malicious Home Routers,” 2007.
143	SecurityWeek News, “IoT Devices Easily Hacked to be Backdoors: Experiment — SecurityWeek.Com,” 2016.
144	The OWASP Foundation, “Owasp top 10 - 2013 the ten most critical web applications security risks,” 2013.
145	J. S. SARA BODDY, “The Hunt for IoT: The Rise of Thingbots,” 2017.
146	D. Papp, Z. Ma, and L. Buttyan, “Embedded Systems Security : Threats , Vulnerabilities , and Attack Taxonomy,” ieee, pp. 145–152, 2015.
147	M. Msgna, K. Markantonakis, D. Naccache, and K. Mayes, “Verifying Software Integrity in Embedded Systems: A Side Channel Approach.” Springer, Cham, 2014, pp. 261–280.
148	M. Msgna, K. Markantonakis, and K. Mayes, “The B-Side of Side Channel Leakage: Control Flow Security in Embedded Systems,” springer, pp. 288–304, 2013.
149	W. L. W. Michael K. Bugenhagen, “Pin-hole firewall for communi-cating data packets on a packet network,” 2007.
150	The OWASP Foundation, “Owasp enterprise security api.”
151	OWASP, “Top 10 2013-A5-Security Misconfiguration - OWASP.”
152	M. Ongtang, S. Mclaughlin, W. Enck, and P. Mcdaniel, “Semantically Rich Application-Centric Security in Android,” 2009.
153	Kaspersky, “The Kaspersky IoT Scanner app helps you secure your smart home Kaspersky Lab official blog.”
154	S. V. Mahavidyalaya, “Wireless Sensor Networks: Security, Attacks and Challenges,” 2010.
155	M. Backes and C. Hricu, “Practical Aspects of Security Control Hijacking Attacks,” 2009.
156	G. Hoglund, G. Mcgraw, and A. Wesley, “Exploiting Software How to Break Code,” 2004.
157	D. Miessler, “Securing the Internet of Things: Mapping Attack Surface Areas Using the OWASP IoT Top 10.”
158	K. Angrishi, “Turning Internet of Things(IoT) into Internet of Vulner-abilities (IoV) : IoT Botnets,” pp. 1–17, 2017.

TEZ İZİN FORMU / THESIS PERMISSION FORM

ENSTİTÜ / INSTITUTE

Fen Bilimleri Enstitüsü / Graduate School of Natural and Applied Sciences ☐

Sosyal Bilimler Enstitüsü / Graduate School of Social Sciences ☐

Uygulamalı Matematik Enstitüsü / Graduate School of Applied Mathematics ☐

Enformatik Enstitüsü / Graduate School of Informatics ☒

Deniz Bilimleri Enstitüsü / Graduate School of Marine Sciences ☐

YAZARIN / AUTHOR

Soyadı / Surname :Erhan.....

Adı / Name : Mutlu.....

Bölümü/Department :Information Systems.....

TEZİN ADI / TITLE OF THE THESIS (**İngilizce** / English) : IT IT SECURITY AND PRIVACY GUIDANCE TOOL FOR IOT DESIGNS AND PRODUCTS

TEZİN TÜRÜ / DEGREE**:** **Yüksek Lisans** / Master ☒ **Doktora** / PhD ☐

1. **Tezin tamamı dünya çapında erişime açılacaktır. /** Release the entire work immediately for access worldwide. ☒
2. **Tez iki yıl süreyle erişime kapalı olacaktır.** / Secure the entire work for patent and/or proprietary purposes for a period of **two year. *** ☐
3. **Tez altı ay süreyle erişime kapalı olacaktır.** / Secure the entire work for period of **six months**. ***** ☐

***** *Enstitü Yönetim Kurulu Kararının basılı kopyası tezle birlikte kütüphaneye teslim edilecektir.*

A copy of the Decision of the Institute Administrative Committee will be delivered to the library together with the printed thesis.

Yazarın imzası / Signature ..... **Tarih** / Date .....