GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

IOT SECURITY REQUIREMENT CLASSIFICATION

Arafat MUKALAZI

Advisor
Asst. Prof. Dr. Ali BOYACI

MASTER'S THESIS
COMPUTER ENGINEERING DEPARTMENT
ISTANBUL - 2022

ACCEPTANCE AND APPROVAL PAGE

On 27/06/2022, **Arafat MUKALAZI** successfully defended the thesis, entitled "**IOT Security Requirement Classification**", which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are listed below. This thesis is accepted as a **MASTER'S THESIS** by Istanbul Commerce University, Graduate School of Natural and Applied Sciences, **Computer Engineering Department.**

Advisor	**Asst. Prof. Dr. Ali BOYACI** Istanbul Commerce University	.....
Jury Member	**Asst. Prof. Dr. Metin TURAN** Istanbul Commerce University	.....
Jury Member	**Assoc. Prof. Dr. Muhammed Ali AYDIN** Istanbul University - Cerrahpaşa	.....

Approval Date: **29.07.2022**

In accordance with Article 6 of the Board of Directors Decision No. 2022/353 dated 29.07.2022 of the Institute of Natural and Applied Sciences, Istanbul Commerce University, it was unanimously decided to graduate the student named "Arafat MUKALAZI" who was determined to have fulfilled his course loads and thesis obligation.

Prof. Dr. Necip ŞİMŞEK
Head of Graduate School of Natural and Applied Sciences

ACADEMIC AND ETHICAL RULES
DECLARATION OF CONFORMITY

In this thesis I prepared in accordance with the rules of thesis writing, Istanbul Commerce University, Graduate School of Natural and Applied Sciences,

- I obtained all the information and documents in the thesis within the framework of academic rules.
- I present all visual, audio and written information and results in accordance with scientific moral rules.
- I refer to the related works in accordance with scientific norms in case of using others' works.
- I cited all the works I cited as a source.
- I did not make any distortions in the data used.
- and that I do not present any part of this thesis as another thesis study at this university or another university.

I declare.

29.07.2022

Arafat MUKALAZI

CONTENTS

ABSTRACT

M.Sc. Thesis

IOT SECURITY REQUIREMENT CLASSIFICATION

Arafat MUKALAZI

Istanbul Commerce University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Asst. Prof. Dr. Ali BOYACI
2022, 63 pages

Societies all over the world are rapidly becoming more and more connected especially because of the huge growth in the number of intelligent things and smart applications (e.g, smart telephones, smart automobiles, smart wearable devices, etc.) that are being put to use. All these have come hand in hand with the new way of inter-connecting between the touchable and the virtual world, popularly known as the Internet Of Things. This is a new promising paradigm whereby every 'thing' can connect to anything via some communication solution, Internet. In IoT, most communication happens directly without requiring human intervention. However, with such systems being deployed even in large-scale, arises the concern of security amongst other challenges. Hence the need to allocate appropriate protection of resources (e.g; devices, applications, services etc.) from un-authorised access of any sorts. The realisation of secure IoT systems could only be accomplished with a comprehensive understanding of the particular needs of a certain system. This paradigm lacks a proper and exhaustive classification of security requirements as far as IoT is concerned. With motivation from here, in this thesis I present an approach towards understanding and classifying the security requirements of IoT. This will play role in the design of not only cost efficient but also purposefully secured future IoT systems. During the coming up with and the classification of the requirements, I present a variety of set-ups and define possible attacks and threats within the scope of IoT. With having the nature of IoT in mind and also considering security weaknesses as manifestations of unrealised security requirements, I put together the would-be attacks and threats in four categories i.e. communication, device/service, mobility, and user interface. I then assessed the existent IoT security requirements as seen in literature, added more in accordance with the applied domain of the IoT and then classified the security requirements. I claim that an IoT system can be secure and also give all its benefits like scalability and flexibility by abiding by the security requirement classification proposed.

Keywords: Architecture, Internet Of Things(IOT), security requirement classification, security, threats and attacks.

ÖZET

Yüksek Lisans Tezi

NESNELERİN İNTERNETİ GÜVENLİK GEREKSİNİM SINIFLANDIRMASI

Arafat MUKALAZI

İstanbul Ticaret Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Ali BOYACI
2022, 63 sayfa

Günlük hayatımızda kullanımda olan akıllı cihazların ve uygulamalarının (akıllı sensörler, giyilebilir cihazlar, akıllı telefonlar, akıllı arabalar vb.) sayısında muazzam bir artış olmuştur. Buna, genellikle Nesnelerin İnterneti (IoT) olarak bilinen fiziksel ve dijital dünyalar arasında yeni bir ara bağlantı biçimi eşlik ediyor. Her 'şeyin' İnternet aracılığıyla herhangi bir şeye bağlanabileceği yeni umut verici bir paradigmadır. Bu tür sistemlerde güvenlik en önemli husustur ve kaynakları (örn. uygulamalar ve hizmetler) yetkisiz erişimden korumak, uygun şekilde tasarlanmış güvenlik çözümlerine ihtiyaç duyar. IoT için güvenli sistemler oluşturmak, ancak bu tür sistemlerin özel ihtiyaçlarının kapsamlı bir şekilde anlaşılmasıyla başarılabilir.Ancak bu paradigma, güvenlik gereksinimlerinin uygun ve kapsamlı bir sınıflandırmasından yoksundur. Bu tez, IoT cihazlarının güvenlik gereksinimlerini anlamaya ve sınıflandırmaya yönelik sistematik bir yaklaşım sunmaktadır. Bu çabanın, uygun maliyetli ve amaca yönelik olarak güvenli geleceğin IoT sistemlerini tasarlamada rol oynaması bekleniyor. Gereksinimlerin belirlenmesi ve sınıflandırılması sırasında IoT kapsamında çeşitli senaryolar sunuyor ve IoT içindeki olası tehditleri ve saldırıları ana hatlarıyla tanımlıyoruz. IoT'nin doğasını ve güvenlik zafiyetlerini gerçekleşmemiş güvenlik gereksinimlerinin tezahürü olarak değerlendirerek, olası saldırı ve tehditleri kategoriler halinde bir araya getirdik, mevcut IoT güvenlik gereksinimlerini literatürde görüldüğü gibi değerlendirdik, IoT'nin uygulama alanına uygun olarak daha fazlasını ekledik ve ardından güvenlik gereksinimleri sınıflandırdık. Bir IoT sistemi, önerilen güvenlik gereksinimi sınıflandırmasını izleyerek, vaat edilen ölçeklenebilirlik, kullanılabilirlik, bağlanabilirlik ve esneklik faydalarının çoğunu pratik ve kapsamlı bir şekilde gerçekleştirerek güvenli bir şekilde tasarlanabilmektedir.

Anahtar Kelimeler: Güvenlik gereksinimlerinin sınıflandırılması, güvenlik, mimari, Nesnelerin İnterneti (IOT), tehditler ve saldırılar.

ACKNOWLEDGEMENTS

Firstly, I would like to say thank you so much to my thesis advisor Asst. Prof. Dr. Ali BOYACI. He is not only a bright lecturer but also great at what he puts hands on. He always motivated me and challenged my ideas with higher standards while at the same time also provided me with a lot of freedom to explore and research the area that intrigues me most. Without his continuous encouragement and always patiently checking on my progress. I would not be able to finish this thesis. I carried out most of the research I have presented with his help.

I'd also like to thank the University and team at the Graduate School of Natural and Applied Sciences too for their support. In particular let me thank Asst. Prof. Dr. Muhammed CEYLAN. I appreciate his research perspectives and willingness to always listen and support in any way possible. It's my privilege to learn from you.

Lastly, and most importantly, I'd like to say a big thank you to my parents and siblings for their endless support, faith and belief in me. Thank you.

Arafat MUKALAZI
ISTANBUL, 2022

LIST OF FIGURES

LIST OF TABLES

SYMBOLS AND ABBREVIATIONS LIST

AC	Air Conditioner
AD	Application Domain
AMI	Advanced Metering Infrastructure
AMQP	Advanced Message Queuing Protocol
AP	Application Interface
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
DDoS	Distributed Denial of Service
DG INFSO	**T**he Information Society and Media Directorate General of The European Commission
DoS	Denial of Service
eID	Electronic Identification
EPSOSS	The European Technology Platform on Smart Systems Integration
GSM	Global System for Mobile Communication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICSs	Information Communication Systems
ID	Identity
IIOT	Industrial Internet Of Things
IOS	Apple Mobile Operating System
IOT	Internet Of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
ITS	Intelligent Transport System
LoRaWAN	Low Power Wide Area Network
M2M	Machine to machine communication
MIMO	Massive Input Massive Output technology
MIT	Massachusetts Institute of Technology
MQTT	Message Queuing Telemetry Transport
MRI	Magnetic resonance imaging
NFC	Near-Field Communication
PC	Personal Computer
PHR	Personal Health Record
QOS	Quality Of Service
RFID	Radio Frequency Identification
RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks
RTLS	Real Time Location System
SCM	Supply Chain Management
UI	User Interface
V2I	Vehicle to Infrastructure communication
V2V	Vehicle to Vehicle communication
Wi-Fi	Wireless Fidelity
XMMP	Extensible Messaging and Presence Protocol
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks

1. INTRODUCTION

The Internet of Things (IoT) has seen rapid and inevitable advancement and has splendidly spread allover different societies enormously improving the way of living. (Baker and Nori, 2021) It promises a rise in connectivity and efficiency hence improved productivity and a decrease in the required effort to do plenty of things in our modern life. Even-though the number of 'things' deployed has potently been growing over the previous few years , the statistics are predicting even much much more increament in the near future with the number of Internet of Things(connected devices) in the world being more than 28 billion next year and 75 billion by the year 2025.(Statista, 2022) This enormous increase in the number of devices that are connected to the internet and at the same time can communiacte to each other (e.g; smartphones and wearables, smart home devices like smart meters, smart industrial machines with intelligent sensors and actuators) will come with opportunities but challenges too.(Cisco, 2022) The immense deployment of this technology to the extent of having 3,6 connected devices per individual by next year signals an increase in the global network traffic, of-which it's predicted to reach 4,8 zettabyte per year by then and the volume of data genearated by IoT connections is estimated to reach a huge total of 79.4 zettabytes by the year 2025.(Statista, 2022) With all this rise in the scale of deployment of IoT devices comes a growth in the value of the acquired , stored and processed data and the attacks towards them too. Speaking from a security perspective, greater security measures have to be devised for threats and attacks on the plethora of IoT are just going to continue getting more sophisticated and it isn't exaggerating to talk about potential security disaters like Mirai(Gopal et al., 2018). For this reason, I strongly believe that a clear and thorough analysis and classification of the security requirements of the Internet Of "things" is very vital to improve and guarantee the security of IOT.

NB: For the purpose of this thesis, "thing(s)" refers to a set of or one user, device(s), applications and services and any related entity.

1.1 Thesis

The word ''IoT'' got disseminated by the ground-breaking works of Massachusetts Institute of Technology(MIT) AutoID Center. The earliest recognised proof of the using of 'The Internet of Things' as a term was from Kevin Ashton who is amongst the founders of MIT AutoID Center in 1999.(Guillemin et al., 2010) IOT connect all physical domains via internet for communicating altogether for fast and easy services. IOT exemplifies a scene where our reknown internet reaches real world objects such as foods, clothings, furnitures, papers, land-marks, refrigerators etc. and makes them capable of gathering, processing and acting on the data smartly. Objects like sensors and actuators are capable of interacting with one another to attain mutual goals such as quality and service through linking all the smart 'things' to the present-day internet.(Internet, 2010) Hence, the vision for IOT is deploying a pervasive ecosystem in which the subject that is, people and the object that is, resources, that can be addressed and communicated to, shall be linked through the web for leveraging the gains to both societies and technologies in a wide range so that people(users) are unremarkaby aided by technologies while carrying out daily activities. (Kouicem et al., 2018)

Amongst the major setbacks hindering the pervasive deployment of IOT systems is : inadequate storage plus the limited processing capacities of the 'things', reliability concerns in performance, availability as regards communication channels, accessibility anytime anywhere, inter-operability while in a heterogeneous setting, information management performance and security (Tewari & Gupta, 2020). Beacuse of IOT devices being resource-constraint by nature, it's difficult to administer traditional hefty security mechanism throught such devices. Further more, because of the 'things' being mostly inadequately secured physically, they are prone to being effortlessly attacked.(Minshall, 2017) For example with the use of un-secured wireless connection, resources like services and network can be acessed without prior permission.(Dazine et al., 2018) Amongst the plethora of attacks include even those that disrupt our physical world in interesting ways as illustrated in (Figure 1.1) with even most

seen just in this previous year. In early 2019, hacked Lime Scooters spew profanity in Australia when those parked on roadsides unleashed filthy human speech (Smith, 2020). Smart ovens were reported to have been turning on themselves and pre-heating to upto 400 degrees(Sivanathan et al., 2018). In 2018, a newly installed MRI machine was noticed disabling all of the IOS devices in the hospital. It turned off only Iphones but not other devices due to the material in the clocks of new iphones(Hristozov et al., 2020). In May 2019, garage door openers and car key fobs mysteriously stopped working in a town in Ohio and the cause later was found to be a device used by someone to turn off own lights emitting a 315 MHz signal inadvertently jammed the key fobs(Smith, 2020). Another report stated that some smart cars would perceive the logo of a Japanese ramen chain as a 'Do Not Enter' sign hence confusing results(Dong et al., 2020). Hackers were able to cause a Tesla's self driving feature to go off-course into the wrong lane by just placing afew stickers along the road.(Marcus, 2022) Default or coded-in credentials in several critical GE healthcare products when hacked for example can alter the dosage of drugs administered to patients remotely(Y. Li et al., 2020). In 2019 MIT technology review reported that it had discovered the Triton malware that gives adversaries remote access in wide-spread ICSs that include installations like petro-chemical plants which can have a huge impact physically(Brass et al., 2018). Such proves that IOT devices have long been lagging behind in-terms of security with hacker's main entrypoints into many IOT devices even being the use of default hard-coded manufacturer usernames and passwords.(Rizvi et al., 2020) In 2019, another report showed that 'thousands of individually-exposed internet-connected Industrial fridges that could be easily remotely instructed to defrost' had been discovered. These can possibly lead to a number of physical consequences, all because of hardcoded credentials. (Radanliev et al., 2020).

This review has indicated that there is necessity of protecting IOT systems and all resources from possible attacks and threats of which these originate from both internal and external network precincts. Because of the dynamic characteristic and sensitiveness of IOT by nature, lots of these concerns can't be tackled simply via a software update or generally exercised security mechanisms (Abdelaziz et

al., 2013),(Xie et al., 2013),(Lu and Xu, 2019),(S. Yu et al., 2018). Security for IOT needs to be made with their intended application domain in mind. Enforcement of security via appropriately well-classified IOT security requirements isn't only a crucial matter but also a must. This thesis aims at investigating and classifying the security requirements that need to be met by an IOT system depending on it's area of application inorder for it to be deemed secure enough.

Figure 1.1. Due to the permiation of IOT throught the physical world, security negligences in IOT can mess up the physical world as we know it. (Smith, 2020)

1.2 Contribution

This thesis intends to provide an up to date and well structured classification of the IOT security requirements. Therefore my goal isn't to propose yet another endless analysis of security requirements in general but rather to disscuss and put forward a classification of security requirements of the broad IOT system when considered as per its domain of application(Neshenko et al., 2019), (Tabrizi and Ibrahim, 2016),(S. Yu et al., 2018),(Alfandi et al., 2021),(M. Yu et al., 2020). To the best of my knowledge, as of today there isn't a complete classification of the security requirements of IOT in attempt to fully tackle all the specific security

needs of an IoT system at a rather granular level with taking full account of its application domain. For this purpose, i am using a well-structured approach to try and synthesize the existing literature on security requirements for IOT in a singular manner. Firstly, I examined the significant security requirements for IOT mainly by assessing the existent relaevant literature out there after which compared and contrasted all of them and then did the classification. My approach in this thesis is three-fold; (1) I summarise the possible attacks and threats in an IOT system. (2) I look at the existing security requirements for IOT and (3) I scrutinize then classify these requirements in accordance with their application domain hence an optimumly secure IOT system. To the best of my knowledge, this thesis provides the most detailed classification of the security requirements of IOT systems as per their domain and i believe that this classification is crucial for understanding security of IOT systems.

In summary , the key contributions of this thesis are;

- I review and map numerous attacks and threats to an IOT system in five distinctive parts thats is communication, device/service, user, mobility and resource integration. This helps to guide the derivation of unique security requirements for the IoT.
- I present and discuss an all inclusive structured domain aware classification of IOT security requirements: differently from the existent literature out there, security requirements of IOT will be associatated to and classified with respective architectural IoT security layers in mind. My approach puts in consideration both the technology, architecture and application domain of an IOT system.

1.3 Organisation of the Thesis

The rest of this thesis here is organized in the following way: Section 2 motivates my thesis by reviewing close works and with the comparison of all these efforts with the rationale behind my thesis. Section 3 is establishing the ground by giving basic notions of IOT. It includes various descriptions of IOT. Section 4 defines a generic IOT Security Architcture adopted in this thesis, including the different

architecture layers involved. Section 5 lists and defines briefly various threats and attacks existing in a system of IOT systematically. Section 6 presents the literature as regards IOT security requirements. This is of vital importance for understanding the classification put forward in this thesis. Sections 7 discusses and presents my approach to IOT security requirement classification with Application domains of IOT put into consideration together with the different IOT architectural layers respectively. Section 8 finally wraps-up and concludes my thesis.

2. LITERATURE REVIEW

In this section I review relevant works that have inspired and motivated my research towards this thesis. To this aim, I focus this discussion on how my contribution will extend and complement the literature in this field.

The novelty heterogeneousness and complexiousness of IOT systems includes wide and un-explored attack surfaces ofwhich in the long run can result in solemn repercussions to those utilising them and also even to firms.(Neshenko et al., 2019) Examples of gaps in IOT Security are vast with some given in the previous section such as,(Ronen et al., 2018) showed how malign entities were able to switch off or on the smart-bulbs in an Internet-based light system and could even have bricked them. Such can cause un-expected electricity utilisation peaks especially in densely-populated areas. More critical incidents can be seen through (Smith, 2020) ,(Hackernews, 2020). (Martin et al., 2020) stated that with having the divergency of Internet of Things(IOT) systems at mind, having satisfactory standardizations security-wise was hard, therefore meaningfully comparing security in diverse IOT is difficult. I saw the gap as per security requirement classifiction for secure implementation of IOT as a system and took a shot at it.

(Yaqoob et al., 2019), (Salman et al., 2018) and (Sicari et al., 2015) grouped security requirements in-comparison to the service they affect. The authors reported various sorts of security requiremnts without being so clear on how and what to follow when classifying them. Their work resulted in a jumble of groupings that often over-lapped with each-other. I am claiming that this lacking in distinguishment between the requirements alongside the inherent complexity of IOT and where its applied doesn't let the readers to acquire a vivid picture of what security requiremets to consider where hence my work that classifies security requirements with-in the IOT at a much granular level.

(Mosenia and Jha, 2017) and (Tabrizi and Ibrahim, 2016) were the first authors that i came accross in the literature that proposed the differentiating of IOT-

specific from general security requirements of the Internet of Things. He focused on IOT-specific requirements and grouped them in accordance to the level in the architecture at which were desired. However they didn't focus at the security requirement each domain would look out for in particular. Similarly, (Approach, 2020) presents security requirements based on IOT architecture, not so different from the one that i have used in my thesis. However he doesn't specify which security requirement is most crucial in what domain of IOT hence my coming up with a new approach to bring to life a granular all emcompassing security requirement classification for the Internet of Things.

(Iqbal et al., 2020) in '' Internet Of Threats'' descibed the different kinds of threats that are currently out there as far as IoT devices are concerned. This work surveyed practical security threats in real IOT Devices in a multitude of different domains for which i have attempted classifying security requirements wise even-though in a much diiferent way. (Ahanger and Aljumah, 2019) This study provided a broad overview of the security risks in the IoT and mentioned possible counteractions too and also showed gaps as regards ZigBee, ZLL, BLE, 6LoWPAN ,LoRaWAN to the extent that some vulnerabilities have hindered use of IoT in critical applications. A thorough IOT Security Requirement classification will aid the securing of IOT in a foremost manner.

(Roman et al., 2013) ,(M. Yu et al., 2020)amalgamates the afew security requirements for IOT and gives a clear frame-work of security infrastructure in general basing on four layers. (Mohsin et al., 2017) Security requirements and potential threats are provided in his work However his coarsened-grained approach doesn't allow to achieve the desired level of detail as per up-to-date security requirements are concerned.

To the best of my knowledge, there isn't any study throught the literature that proposes a well-structured classification of security requirements of the IOT with the applied domain put in consideration too. This represents the main motivation behind my thesis.

3. BACKGROUND: THE IOT PARADIGM

Nowadays, Internet of Things is a quite well known paradigm. However inorder for my thesis to be easier to read and also for it to be self-contained, I considered it relevant to go over the unsophisticated notions of IOT. This background here also facilitates the definement of common terminologies that are to be used through-out the remainder of my thesis. It's for such reasons that back-ground notions regarding the Internet Of Things are presented throught this particular section.

IOT isn't just an individual system that is comprised of computation gadgets. It's more of an eco-system with inter-connected smart things that are both touchable and virtual. It incorporates every'thing' and any'thing' that is connected to internet (Atzori et al., 2017) .A couple of definitions of IOT have been put forward. For example, DG INFSO and EPOSS define IOT (Bassi and Horn, 2008) as: 'things that have identity and digital personality and can operate inside intelligent space via use of smart interfaces hence are connecting and communicating with-in Social, Environmental and User Contexts'. This IOT definition that sticks to 'things' oriented architecture is widely used. Additionally, Atzori et al. (Baker and Nori, 2021) defines 'things' through a three perspective view that is Sensors, Middle-ware services and Information.

(Gubbi et al., 2013) presented one user oriented definition of IOT irrespective of the underlying communication protocols and IOT ambiances: 'inter-connection of the sensing with the actuator devices giving the capability of sharing information from one platform to another platform via a joint framework of which develops a mutual operation image for the enabling inventive applications. All this can be achieved with faultless pervasive sensing, data analysis and information representations by use of cloud-computing as a uniting framework'.

In comparison to (Baker and Nori, 2021) and (Gubbi et al., 2013) , Tan and Wang (Chopra et al., 2019) defined IOT from a communication, societal, surrounding plus users context just as stated: 'things have identity and digital personality that

operates in intelligent space with utilisation of smart interface for connecting and communicating with-in societal, surrounding plus users contexts'. Alittle bit differently from (Baker and Nori, 2021) and (Gubbi et al., 2013), (Zimmermann et al., 2015) defines IOT stand-alone without considering technologies or even platform. Their definition comes from mobility and service inclusion view point.

Additionally, (Abu Waraga et al., 2020) deliberated IOT from a network perspective whereby touchable devices are connected together in a structure like that of the Internet itself. More IOT descriptions can be located in (Neshenko et al., 2019), (Zhao and Ge, 2013) and (Pal et al., 2019).

All in a nut shell, IOT isn't just comprised of cyber physical systems that measure situational data and then carry out automated computations. It is much more of network infrastructure which joins both the physical and virtual world altogether. Hence i claim that inorder to address security distinctiveness of IOT, broader facets of scenarios that combine architecture, user, communication, technology and various applications must be put into consideration.

Moreover, the interactings in IOT in-between entities might take place for just a limited amount of time but also could be for their whole life-time.(Al-Fuqaha et al., 2015) It's also hard to predict everything at once as regards what entity would be interacting with which entities and also being able to precisely single out the exact service via which accessing would be attempted.(Militano et al., 2015)

In any IOT system in which a user(s) might possess plenty of devices together with their concomitant ammenities, capability of identifying the user(s) in every situation is for ensuring the security the systems.

Therefore i strongly claim that within greatly dynamic and scalable systems like IOT, confirmation of entities shouldn't just depend on the special distinct identities of the entities. All attributes such as ages, names, locations don't have to be in systems and all entities, only what is required in what context can be provided for hence an efficient system. (Baktyan and Zahary, 2018).

4. IOT SECURITY ARCHITECTURE

The main aim in this particular section is discussing the IOT Security Architecture that's adopted in this thesis. Several IOT architecture have been put forward throught the literature such as (Manogaran et al., 2018), (Al-Fuqaha et al., 2015) and (Minoli et al., 2017). Most of the works suggested three layered architecture for example (Siegel et al., 2018), (Khan et al., 2012), (Z. Yang et al., 2011) was comprised of an application layer, a network layer and the perception layer. Even though very few, there are some like (S. Li et al., 2016) that proposed a four layered structure consisting of sensing layers, network layers, service layers and the application interface layers. Nonetheless, there isn't any universal structural design for IOT thats being widely used as the recommended standard as per security architecture is concerned. To the contrary of these four and three layered architecture by others, (Al-Fuqaha et al., 2015) urges that that five layered architectures of IOT application and service should be supported. Startting from lower to higher: the object, object abstraction, services management, applications and business, are the layers that are used in there. Even though i agree to the fact of numerous layers being necessarily vital for understanding the complexness of IOT, I say their representation is too detailed as per the physical infrastructure of systems like these.

(S. Li et al., 2016) however put forward an architecture that's multi-layered both ways. That is horizontally and vertically. They covered the elements of IOT, such as: the device(s), the network that's connected with, the service(s) being connected to, and up through the application(s) until the end-user(s), horizontally and vertically they covered security service(s) like verification, approval, identity(ID), trust and key(s) management amongst others.

I claim that the operational constituents of IOT architectures must capture the various Security Requirements and diverse security concerns too just like in (Radanliev et al., 2020) . With such an architectural inclusive classification of IOT security requirements, one can achieve the desired security, device(s) wise, network-wise, data repository-wise, service(s), application(s) and user(s) wise

too. Hence, after analysing quite a number of works, I used the five-layered, three-dimensional IOT Security Architecture depicted in (Figure 4.1). Unlike some other architecture such as (S. Li et al., 2016), in which the user(s) and application(s) are considered as single layer, The architecture adopted during my classification (Approach, 2020) of IOT Security requirements separates user(s) from the application(s) layer, situating these as the top-most. The extra user dedicated layer helps in the taking care of user specific security requirements especially in pervasive IOT systems that have plenty of users.

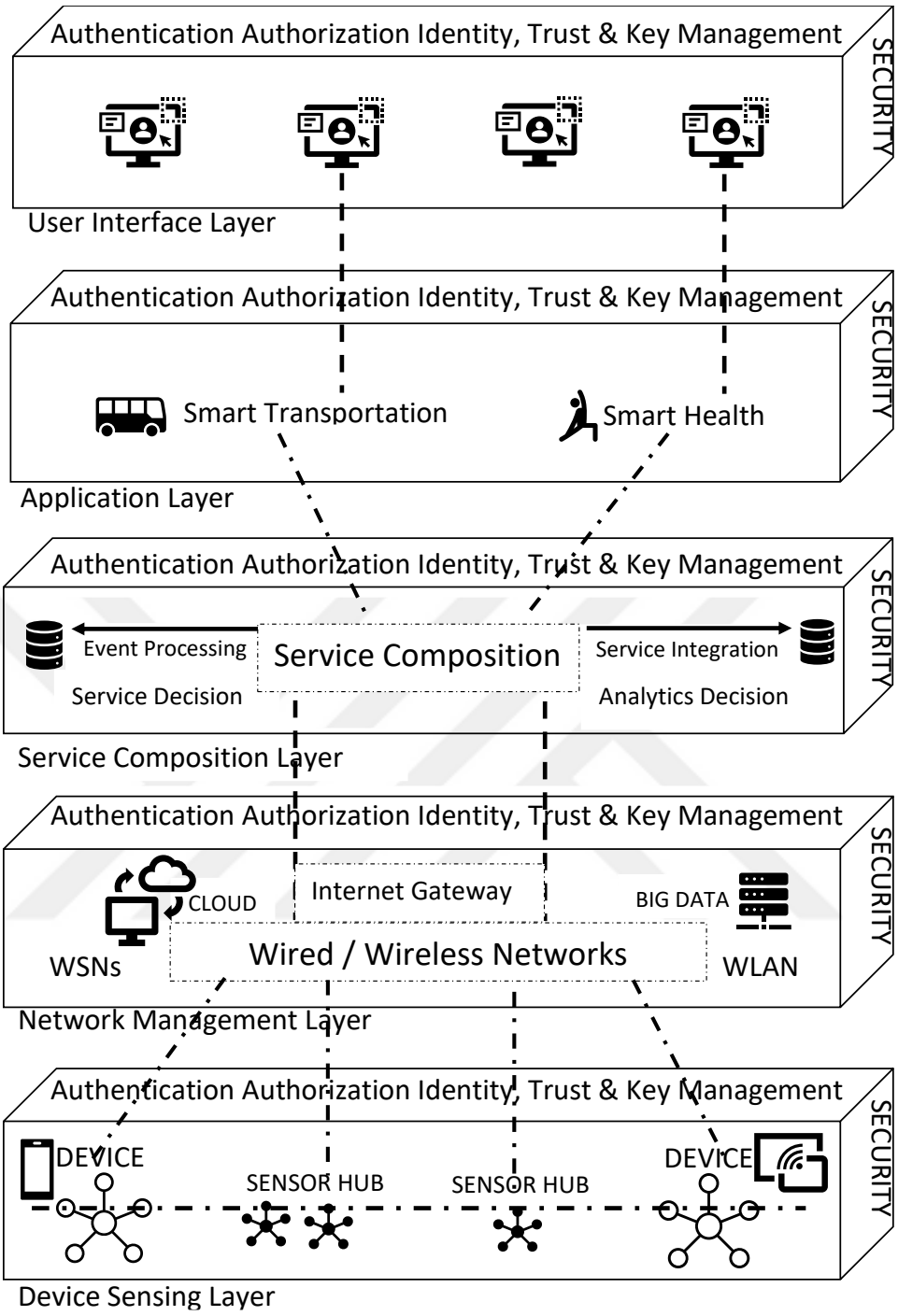

Figure 4.1. The Operational Layers of IOT Architecture

The above illustrated architecture is five layered i.e: the device-sensing layer, network-management, service-composition, application and user-interface layer(s). Each of the layers has the components which are needed for the collection, storage, computing, processing and communication of information amongst all architectue components plus in-between layers themselves. There is

also an added perspective comprising a few essential security requirements like verification, authority, ID, trust plus key(s) management but these are just a few, more are in the sections to follow. Security can be accounted for per level system-wide. Below, i describe the fundamental elements, main functions plus popular security concerns layer-by-layer.

4.1. The device sensing layer

This foremost level comprises Smart IOT gadgets such as smart-phones, RFID-tags, sensors plus actuators amongst others that are capable of sensing, collecting and measuring a range of substantial parameter(s) like: humidity, temperature, location and more automatically. These devices are capable of storing all accumulated data within them-selves where as the sensors do store their data in pre-defined sensor-hub for example in micro-controller unit(s) for the purpose of it being processed.(Perera et al., 2014) Data sensing and data attainment are the core functions carried out at this level. Regardless of where components of this layer are deployed, security is of key importantance always.

4.2. The network management layer

This layer comes just after the sensing one. Amongst this layers' components are; both wired-in and wireless networks, the services from the cloud and vast data depositories. Data clustering, QOS, scheduling amongst others are the main functions at this level. However the transmission of the data from this layer to the next one up in the IOT architecture is also this layer's responsibility and its done with the use of technologies such as 4G, 3G, GSM, WiFI, IPv6, 6LoWPAN, RPL, bluetooth and so forth.(Wang et al., 2017) With the utilisation of the cloud and big-data depositories, all the diverse technology is able to work in a seamless manner.

4.3. The service composition layer

This is the next layer after the network level. All the data passed on from the the network layer is processed and analysed here and this happens to be this layers' most important functionality. This layer mainly resides on middle ware technolojies that facilitate the exchanging of information for IOT applications amongst various entities without requiring any customized software or even hardware. This layer must meet demads of application(s), API(s) and a variety of service-protocols (Xu et al., 2014).

4.4. The application layer

This is the second last layer from the top of the architecture. It renders the Smart IOT service(s) to the user(s). This layer here is majorly comprised of the wide range of applications that can be grouped like e.g, smart-homes, smart-commerce, smart-cities, smart-transportation, smart-health and so on (Zaidan and Zaidan, 2020),(Risteska Stojkoska and Trivodaliev, 2017), with (more in section 5). This is the layer that caters for data-presentation(s), application-maintenance, application(s) access-control, software update and also chooses the suitable messaging protocol application-level wise. (Yassein et al., 2016) HTTP, HTTPS, CoAP, MQTT, AMQP, XMPP and so forth are amongst the commonly used in the application layer (Swamy, 2017).

4.5. The user interface layer

This is the top most level in the IOT architecture. It encompasses the interface(s) presented to the user(s). The user(s) them-selves are the most important element of this architectural level. Its through this layer that an IOT systems' functionality is moved from the latter layer(application layer) to the targeted users. At-times can use the well-known web-service(s) in the distribution of service(s) gotten from the layer below (Belkeziz & Jarir, 2017). It's noteworthy to mention that each and every layer has distinctive security requirement(s) as regards its' key security functionality. For example, The management of Identity

in the very first layer below(sensing layer) safeguards the privacy of service(s) but the same Identity Management it shields the privacy of user(s) this particular layer. The main functionality and key elements alongside the respective architectural layer are illustrated in Table 4.1

Table 4.1. The key elements, main functionality alondside respective layer as per the IOT security architecture shown in Fig. 2.1

Architecture Layers	**Key Elements**	**Main Functionality**
Layer for sensing of devices	Actuators, smart-sensors, RFIDs.	Sensing of data, acquiring of data.
Layer for control of the network	Wireless/wired network, Big-data storages.	Aggregating of data, Quality Of Service.
Layer composed of services	Miscellaneous entities, middleware technology.	Data analysis and Data handling.
Layer of applications	Varied application areas e.g, smart city, smart home.	Defines Message Passing Protocols
Layer for user interactions (UI)	The users.	Enable users to access services.

5. THREATS AND ATTACKS

The following section examines possible attacks and threats done to IOT. Most are in conjuction with the numerous IOT Application settings which have been put forward in the following main discussion section. Several work(s) regarding IOT Security have put forward the attacks and threats and also organised them differently with basing on the architecture of IOT(Alwarafy et al., 2021), (Makhdoom et al., 2019) some according to the security concerns such as access-control (Sadique et al., 2018)and also some even usage-scenario based (Mohamad Noor and Hassan, 2019). It's from all these that i derived an approach to group them as below as there isn't a one size fits all solution due to the diverse nature of IOT.

Attacks tend to be directed at the various weaknesses throughout any IOT system(Kouicem et al., 2018), Such weaknesses range from device(s) them-selves, thru the interaction amongst them that is for the services given. The user(s) plus the systems' being so dinamical and portable also presents attack windows. I found it essential to consider the IOT systems' architecture features while i was establishing suitable IOT security requirements with the wide range of could-be attacks and threats against IOT systems in mind. I argue that being able to put forward a usable classisification of the security reqirements of IOT goes thru examining the threats well too .

With the nature of IOT in mind, potential attacks and threats on IOT have been categorized in-to four arenas in this thesis i.e.: Communication(s), Device/Service(s), User(s) and Mobility. This categorisation has been illustrated in (Fig. 2). As per this thesis, IOT consisted of interacting user(s) with device(s), device(s) that provide variety of service(s). The devices together with own service(s) integrate hence meeting the requirements of the enduser. It is possible for the device(s) and user(s) to be mobile.

The potential attacks and threats through wireless and wired channels for example, data transfer channel threats, are covered under communication(s).

Physical IOT device(s) together with the related low level service(s) such as memory, battery and such are embraced under device/service(s). The user(s) encompassses the ones like Identity disclosure that are on the IOT user(s) and lastly mobility, just like the term itself, consists attacks and threats like tracking which takes advantage of the movability of IOT. A summary of all the mentioned classifications is presented in Table 5.1. I find it noteworthy to mention however that some attacks involve more than one aspect of an IOT as illustrated in Table 5.1.

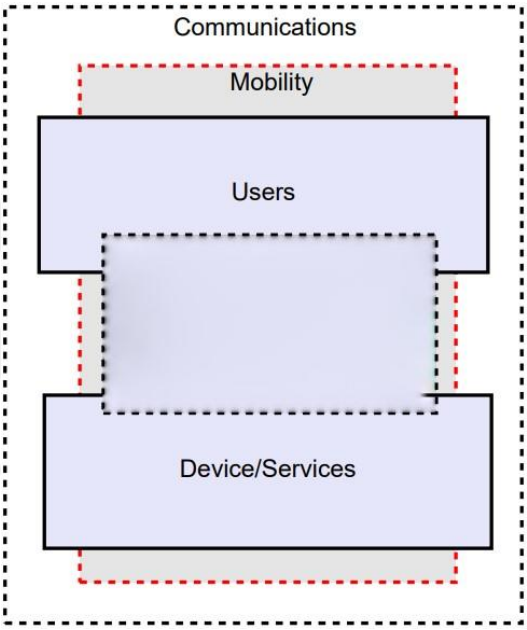

Figure 5.1. Suggested Threat and Attack Categories

Table 5.1. A Summary of the Concocted Threat and Attack Categories with a Precise Elucidation.

Categories	**Precise elucidation of threats and attacks**
Communication	Attacks and threats thru wireless and wired channels e.g, data transfer channel threats
Devices/Services	Attacks and threats on Physical IOT device(s) the related low level service(s) e.g, battery
Users	Atttacks and threats on the people in IOT systems e.g, disclosure of ones identity.
Mobility	Attacks and threats that take advantage of portability of IOT e.g, location-tracking

5.1 Communication

Communicating between entities that is to say the User(s) and device(s) is vey essential in IOT. However, such connectings bring with them threats too. The threats in communication are either a routing attack, an active or passive information or flooding.

The attacks refered to as routing ones take place by means of a hacker targetting the routing-protocols or the network-traffic for the purpose of either disrupting how data is flowing or for redicting paths to insecure destinations. No alteration of any kind is done to packet(s) in their transit and examples of such are black-hole, worm-hole and pharming (Pongle and Chavan, 2015).

Those attacks that change and delete info through aiming at good data packages in a direct manner instead of via sabotaging network-routing are refered to as the active attacks. Amongst these is channel-jamming together with any form of tampering or modifying of the data irrespective of the result. On ther hand lies those attacks in which the malicious beings retrieve info without having to change any of what is even being transmitted. These are refered to as passive and examples here are eavesdroping and traffic-analysis.

Where as for the case of flooding attacks, they are the ones in which brand-new packets are introduced to the network and an example here is the SYN Flooding attack(s)that are in most cases actually directly addressed as a DOS attacks(Hristozov et al., 2020).

5.2 Devices/Services

Physical attacks, Device subversion attacks, Device data-access and Device degradations are the four main categories under which the threats to IOT System device(s) and service(s) can be grouped. A big number of IOT gadgets resides in the open whereby they are so prone to being disconnected or even getting damaged. Attackers are capable of easily disconnecting a specific IOT Device such

as a PC, cell-phone or infact the AC off the internet physically and also are capable of damaging the IOT severely up to a point where it cannot be serviced anymore(Deogirikar, 2017).

In Device subversion-attacks such as a packet-capturing, attacker(s) gain the maximum or minimal hegemony of the device(s). They then if they wish make the device to stop working either fully or cause it to counterfeit its output. The malicious entitiy may either control one or even more devices.

Well, in the case of the so called device(s) data-access attacks, The attackers infect IOT device(s) that can later be used in the carrying out of malicious activity torwards the subtle personal information with-outeven the attacked user knowing at all. Identity spoofing is amongst the techniques that are used here by the attackers. In such attacks sometimes the device continues to work well as usual however all the information kept in the device is readily accesible by the hacker at any time.

The other category is device degradation. This happens to be some sort of DOS attack whose aim is to hinder the accessing of service(s) directly. It's carried out through attacking the device(s) itself instead of incapacitating the whole network itself from handling any traffic(Catarinucci et al., 2015).

5.3 The Users

For this category, all possible security threats related to the user(s) are also spread out in four wide types that is, the trust, data-confidentiality, identity-management and each and everyone's behaviour.

Because IOT is so vast, providing trust throughout it is really challenging. Amongst the attacks in conjuction with trust is: self promoting which is where a bad node recommends itself, bad mouthing that happens inform of some hacker negatively reccomending a a node that is good plus also good mouthing which

refers to when an infected node gives an awesome recommendation for an already comprised one. (Wright et al., 2004)

5.4 Mobilty

The security concerns that come hand in hand with the Mobility of IOT are split into three namely: Dynamic infrastructure, tracking plus location-privacy and many other dominions. It is possible to view some of the threats thru different perspectives: for instance;The capability of users to move from one place to another increases the attack terrain in terms of both active and passive attacks of which most have been elaborated on above.

6. IOT SECURITY REQUIREMENTS

This particular section provides a couple of the relevant works out there as far as the IOT security requirements area is concerned. I analysed a plethora of literature for the purpose of examining, explaining and later on classifying the various security requirements out there with especially keeping in mind the how and reason as to why the considered is are requirements. A-lot of work examines and addresses alot of issues regarding IOT but i noticed that there is close to none amongst the literature that puts focus around specifically classifying the security requirements of the Internet Of Things. Most the works i came across presented analysises of IOT Security needs plus architecture but always put the security requirements as an extra and none bothered classifying them. (J. C. Yang and Fang, 2011) stated that naming the IOT centric security requirements is essential but also not so easy.

(J. C. Yang and Fang, 2011) provided one IOT security architecture that was centered around the control, computing capability and comunnication viewpoints plus also discussed some primary IOT security concerns like verification, access-control plus identity but his work didn't specifically address what IOT requirements are neeeded where in an IOT system.

(Heer et al., 2011) and (Sain et al., 2017) proposed a couple of IOT security requirements in relation to their architecture layer like the network, application and physical layer plus. They did give major concerns like fault-tolerance, acess-control,confidentiality etc but they didn't try combining all the requirements to come up with a clear classification of their requirements if considered while securing any IOT system.

(Cirani et al., 2013) looked at IOT needs security-wise thru an IP viewpoint. This work examined the existent internet protocols being utilised in IOT and came up with security concerns plus requirements this way. They suggested that more lighter protocols for the diverse IOT are needed. However much i agree with their conclusion(Park and Shin, 2017), their work didn't present any strictly IOT

centric security requirements and not even a classification of them besides giving the well-known properties of security like integrity, confidentiality, authentication and availability for their case.

Other approaches in the literature for example (Tourani et al., 2018), (Ammar et al., 2018) and (Zhou et al., 2019) gave the authorizing, authenticating, control of access and management of identity as the major IOT system security requirements. As an addition to these, a couple of other work (Ning et al., 2013) suggested a couple of overall security needs like network-security, application-security, layer-wide security, configurations, encryptions, data-integrity and even anti-virusses amongst others. I put all of these in consideration while proposing my classification of all the IOT requirements (in section 6) as per their application domain for even these general requirements are needed in some specic area of an IOT system.

Nevertheless, there is much more literature that has been gone through however i have just included a-few of the reviewed studies above though a summary of all that i was able to get regarding the possible security requirements for IOT systems can be seen in Table 6.1 below. Requirements that i have colored green can be considered to be the 'usual' security requirements it is possible to see them even in other areas of application.

Table 6.1. The possible IOT security requirements as seen in literature. Those in green are the 'usual' security requirements

Requirements	(Gluhak et al., 2011)	(Babar et al., 2010)	(Kim, 2015)	(Singh et al., 2016)	(Abomhara and Koien, 2014)	(Yaqoob et al., 2017)	(Heer et al., 2011)	(Alam et al., 2011)	(Ciani et al., 2013)	(Ning et al., 2013)
Access control	+	+	+	+	+	+	+			
Confidentiality				+					+	+
Authorization		+		+				+	+	
Authentication		+		+				+	+	
Key-management	+		+		+		+		+	
Availability		+	+						+	
Trust	+			+				+		
Integrity				+				+		
Accountability										
Non-repudiation										
Usability							+			
Privacy	+	+	+	+	+	+				
Resilience-to-attacks		+		+				+		
Scalability		+			+					+
Secure-storage		+		+	+				+	-
Identity		+		+	+		+		+	+
Secure-communication				+	+					
Secure-content						+				
Manageability							+			
Location-privacy							+			
Energy-awareness					+		+			

Decentralization	+				+					
Real time						+		+		
Anonymity						+				
Quality-of-service			+			+				
Reliability	+									
Data freshness					+		+			
Load-balancing								+		
Fault Tolerance						+				
Mobility	+		+			+				

From Table 6.1, one can notice that a range of IOT centric security necesities are presented however the requirements here can be constricted and joined for better classsification of those that are more essential. A more concise and extended classification of IOT requirements is presented in Table 6,3 right after a short description of the added requirements is presented in Table 6,2. These added combination of latter requirements covers concerns of real time dependability, data-freshness, attack resilience and fault-tolerance as in shown in Table 6.1.

Table 6.2. The Enhanced IOT security requirement list with a short description.

Presented Security Requirements	**Brief description of Threats and Attacks**
End to end Security	Supporting of end to end security when Communication Path traverses multiple domain
Management of Identity	Incorporation of reliable and flexible Identity Management technique in thing(s) registration.
Lightweight Solutions	Considering of the resource constrained nature of thing(s) (Not only energy but also computing power.)
Decentralised Management	Supporting of adjustable provisioning of security in a decentralized manner.
Scalability or Incremental Deployment	Supporting of huge volumes of applications, data and services plus users
Robustness,	Supporting of security throughout various operating conditions, discovering of faults plus automatically correcting them.

Reliability, Selfhealing , Data-freshness, Real-time	
The privacy	Considering of data plus user privacy
Mobility or Dynamic	Supporting of mobility of thing(s), devices and users.
Heterogeneity, Composition, Inter-operability	Considering plus supporting of various security requirements of the diverse applications and services
Federation in Administration Domains	Enabling of relevant security policies for their enforcement in all involved domains.
Transiency or Ephemeral	Supporting of short interactions between thing(s) without any unnecessary overhead

Table 6.3. The added requirements and the joined entities from Table 6.2 above

Presented Security Requirements in 4.1	**Mapping to respective entities in 3,1**
Privacy	Privacy, Location-privacy.
End to end Security	Secure-storage, secure-content, secure communication, quality-of-service.
Decentralized Management	Decentralization, Manageability.
Identity Management	Anonymity, Identity.
Lightweight Solutions	Energy-awareness.
Dynamicity or Mobility	Mobility
Incremental-deployment or scalability	Load-balancing, scalability.
Robustness,Reliability,Selfhealing , Data-freshness, Real-time	Real-time,resilience to attacks, Freshness of data, fault tolerance and reliability.
Federation in Administration Domains	x
Heterogeneity, Composition, Inter-operability	x
Transiency or Ephemeral	X

Much of the other reviewed work also proposed how important IOT security is and discussed a couple of other security requirements that i found noteworthy discussing in short below. An attempt to classify the requirements depending on the IOT security architecture adopted in my thesis(in section 3) is also presented in Table 6.4 below. With utilisation of the IOT security architectural layers that i presented in Figure 1.1 of section 3, I am succinctly going over the prominent security concerns layer by layer line in line with the threats and attacks already put forward in section 6. With consideration of each and every layer in the IOT

architecture, an approach towards classification of the IOT requirements by the way they are applied is put forward below.

6.1 The Device Sensing Layer Security Requirements

This layers' most seen security concerns are: validation, approval, access-control together with the manageent of the identities of the device(s). When it comes to threats and attacks, this layer is mainly prone to device-subversion attacks, physical-attacks, device-degradations plus device(s)' data-access. The most significant security requirement(s) of this particular level are: light weight security, the capability to be heterogeneous ,interoperable, robust, reliable, do real-time, data-freshness and being able to heal ownself in an attack.

6.2 The Network Management Layer Security Requirements

The major set-backs of this partiacular layer includes concerns like the routing-attacks, active-data attacks, passive-data attacks, floodings, ever-changing topologies or infrastructures amongst others. This layers' principal security needs include: the capability of being heterogeneous, interoperable, scalable having of light weight security facilitating communication and mobility.

6.3 The Service- Composition Layer Security Requirements

The major security concerns that stick out at this layer are : confidentiality of data, floodings, device's data-access, resource-flow plus being interoperable. Furthermore, the key security needs of this level include: ability to self-heal and attain fresh data, be robust, reliable, scalable, heterogeneous and interoperable as regards management of service(s). It's such requirements that render the trust that is so dearly needed while managing data.

6.4 The Application Layer Security Requirements

This threats or attacks that are seen as the main concerns security-wise include surging resource, ability to be interoperable amonst others as shown in table 6.2. Interms of key security requirement(s), Having fresh data in real-time, being robust,self-heal capable, reliable, heterogenous and interoperable during application-maintenance, data-freshness when presenting data, possesion of light weight security in access-control plus the facilitating of end to end security throught the application(s) is crucial.

6.5 The User Layer Security Requirements

This layers' most seen security concerns are: authorizations, authentications, access-control plus the management of the identities of user(s). Outstandingly, amongst the most significant distresses of this particular layer is: the confidentiality of data, trustworthness, threats based on behaviour with tracking plus location-privacy. The most vital security requirement(s) tied to the user-interface layer include: all-around security, mobility/portability support, ability of being scalable, heterogeneous, interoperable and manageable in a disributed manner. Encryption is very important at this level for interactions in-between the user(s) of IOT at large.

In Table 6.4, we outline some notable security requirements in different layers of the IoT security architecture that we illustrated in Figure 1.

Table 6.4. Noteworthy IOT security requirements classified as per IOT security architecture depicted in Fig.2.1

Architecture Layer	Noteworthy Security Requirements
Layer for sensing of devices	Supporting of heterogeneity, composition, inter-operability. Lightweight Solutions. Self-healing, Robustness, Data-freshness, Reliability, Real-time, Identity-management, Dynamic, Mobility.
Layer for control of the network	Supporting of Heterogeneity, Composition, Inter-operability. Lightweight Solutions. Incremental-deployment, Scalability, Federation-of-Administration Domains, Dynamic, Mobility

Layer composed of services	Real-time, Self-healing, Robustness, Reliability, Data freshness. Incremental-deployment, Scalability. Inter-operability, Composition, Heterogeneity. Decentralised Management. Ephemeral, Transiency.
Layer for applications	Lightweight Solutions. Self-healing, Reliability, Robustness.Data-freshness, Real-time. Heterogeneity, Inter-operability, Composition. End to end security. Privacy
Layer for user interactions(UI)	Heterogeneity, Inter-operability, Composition. Privacy. End to end security. Dynamic, Mobility.

7. CLASSIFICATION OF IOT SECURITY REQUIREMENTS

Security requirements exist for the purpose of being met while considering the securing of any IOT system. The classification of these however is for efficiency and infact gives more granular security of IOT systems. I take this to another level by contributing a classification with putting the Appliaction domains too in the picture. I claim that this approach of classification of IOT requirements that i propose offers a way forward towards the securing of IOT which is already vast and diverse by nature.

Throught this section, i amalgamate the information from the aforementioned sections like the adopted IOT Security Architecture for the puropose of puttting forward an original classification of the IOT security requirements. With the information build-up from analyses done in the latter sections, I present my approach came up with for the classification of the requirements. Firstly, I succinctly describe the Application domain in which the IOT is applied. Then, with reference to the data in the prior sections, i classify the security requirements of a probable IOT system that could be in the domain.

The IOT security architecture described in section 2 and depicted in Fig.1 is adopted in the classification of the AD specific requirements. The prone threats and attacks are then also included in the classification after which the top-most necessary security requirements of an IOT system in the specific domain are presented. This is the brief explanation of how the classification of the AD specific IOT security requirements is organized. The over-all classification is also depicted in Fig. 7.1

APPLICATION DOMAIN	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
	DEVICE SENSING LAYER				
	NETWORK LAYER				
	SERVICE COMPOSITION LAYER				
	APPLICATION LAYER				
	USER INTERFACE LAYER				

Figure 7.1. The over-all AD-specific IOT Security Requirement Classification.

7.1 Application Domains of the Internet of Things(IOT)

The rationale of this particular section is discussing the wide range of domains in which IOT is applied. Quite a number of application(s) plus service(s) are deployable and infact are being deployed with IOT (Lin et al., 2017),(Al-Emran et al., 2020), (Ejaz and Anpalagan, 2019). From here on i lay out a good number of such conscisely for the purpose of giving a rough idea of where and how IOT is applied. After having discussed the IOT security attacks and threats plus numerous security requirements in-detail in the previous sections, I am aiming at presenting exemplary areas in which IOT is applied together with the attacks and threats that may happen in them and itt's from this that i derive a unique classsification of the relevant security requirements as far as each application domain is concerned.

7.1.1. Aviation and aerospace

The internet of things can be leveraged for the purpose of being able to improve the security and safety of products and services. The aviation sector is one of these industries that do use IOT to improve their security. For example for the sole purspose of meeting the high security standards, all air craft parts are RFID tagged for tracking of any changes to the original parts and before any installations, the part is automatically checked for origin and where-abouts hence a secure and green management of the lifecyle of air crafts in general thanks to technologies like this that are embeded in IOT. The 'on-condition'

wireless monitoring the airplane is only possible via the utilisation of smart devices with sensing capabilities available with in the cabin or even outside.These are connected to the airplanes' monitoring system . Nodes that are in a network like this are being used to detect numerous conditions like temperature, pressure and so forth. The data collected can be used for planned maintainance, saving energy and also for customizing the passenger experince hence efficiency. The wireless identifiables like RFID tags on crew/passenger luggage can be used in tracking of the cargo via sensors,cctv etc.All can be referred to as one wholesome IOT system.(Guillemin et al., 2010) The classification of the IOT security requirements of this application domain are summarized in Table 7,1

Table 7.1. Aviation-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
AVIATION AND AEROSPACE	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	PRIVACY INTEGRITY AVAILABILITY AUTHENTICATION CONFIDEENTIALITY
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, Self-healing, Reliability, Real time, Data freshness/Scalability, Incremental deployment/ composition, Heterogeneity, Interoperability Decentralized management, Transiency, Ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, Self-healing, Reliability, Real time, Data freshness/composition, Heterogeneity, Interoperability, Light-weight solutions, End-to-end security, Privacy.	
	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, Dynamic/Scalability, Incremental deployment/Composition, Heterogeneity, Interoperability/Decentralized management/Privacy.	

7.1.2 Automotive(V2V)

The automotive industry applies IOT in a couple of ways from the monitoring of the pressure in a specific tyre to proximity awareness of other vehicles or whatever could be around the vehicle. IOT technolojies like RFID are used in the conrtolling of the automobile production back at the factory inorder to maximise profits via efficiency. Items can be pinned down to their exact location with in the factory and info regarding their whereabouts too is on them. IOT is also leveraged in RLTS's hence improved vehicle tracking. This particularly important in shipments too. Vehicle recall processes and

Table 7.2. Auto-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
AUTOMOTIVE	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	NON-REPUDIATION AUTHENTICATION AVAILABILITY PRIVACY
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	
	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

Vehicle lifecycle management is easier for when the need arises, vehicle recall process are easier with IOT. V2V and V2I communications have advanced more

hence smarter vehicle and traffic management(Kouicem et al., 2018). Vehicles themselves have become 'things', in the case of emergencies they are capable of making the calls for assistance.

7.1.3 Smart buildings

Until today, automated tasks in both buildings and homes by use of technology has normally been just seen in luxury homes and high-end buildings. However, ever-since IOT took off, more and more smart home applications are appearing with the wireless technology having become cheaper. Amongst the applications under smart homes is smart metering where by energy consumption is tracked digitally by both the energy provider and the house owner. Sensors like those of temperature automatically increase the comfort of buildings. Intelligent homes are all about providing flexible likeable lifestyles with the help of IOT enabled house appliance(s) [ ]. Many real-life applications are even already out there with examples like CURB(Energycurb, 2021) and ''Philips Hue'' (Philips, 2020), a wireless lighting system in which user(s) are capable of controlling all lights with just their voices and things like adjusting of brightness, setting timers, creation of routines and even making changes in colour of the light is possible with just a swipe in the cellphone app.

Table 7.3. Smart building-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
SMART BUILDINGS	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/ Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	AUTHENTICATION CONFIDEENTIALITY AVAILABILITY INTEGRITY
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	
	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

7.1.4. Smart healthcare

With the advancements in IOT, there has been growth in the number of ways in which IOT is being used in the Health Sector. For example, sensors and actuators are embeddded in the patients' body for monitoring and tracking purposes(Shaikh et al., 2019). Possibilities like the use of a mobile phone that supports RFID to monitor and deliver drugs to patients is a reality nowadays.

The combining of different technolojies like sensors, RFID, NFC, Zigbee, Bluetooth and wifi amongst others will improve greatly the monitoring and measuring ways of things like blood pressure, temperature, heart-rate and much more. Eatable microchips could also be introduced into the bodies of Paralysed People and hence stimulated muscles via the implanted 'thing'(Baker et al., 2017). With IOT, health-care systems no longer reside in just the hospital network architecture, they are accesible anywhere with an example of (Catarinucci et al., 2015) in which Via the use of a wearable blood-pressure monitoring system, a patients' info such as blood-pressure is regularly being sent to the hospital's databases and is being viewed by the designated doctors. This constantly accumulated data could then potentially be utilised in the diagnosis and making of treatment-plans. A real-life example of such a system can be seen in Turkey as eNabiz(Turkish Ministry of Health, n.d.).

IOT also continues to play a big role in enabling of the old population to leave indepedently(Riahi Sfar et al., 2018). IOT supports the old by detecting their day to day activities via wearable sensors, monitoring of the vital signs via body sensors for those chronically ill and also due to the advanced algorithms in some IOT, catastrophies are prevented via pattern recognition enabled patient monitoring.

Table 7.4. Smart healthcare-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
SMART HEALTHCARE	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	AUTHENTICATION CONFIDEENTIALITY INTEGRITY PRIVACY
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	
	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

7.1.5. Smart supply chain(SCM)

With the implementing of IOT in the supply chain management, alot can be achieved. RFID tagged goods for example can be easily managed while at their point of sale where by a shop owner with smart shelves can effortlessly track the stocks, know whats out of stock or expired and even get notified of shoplifting in real-time thanks to IOT. Manufactures too can avoid over or under production via acquired fresh data from sellers. Logistics too is easier with IOT tracking technolojies and also just due to the fact that even pallets inside trucks are 'things' giving off data. Fast payments while shopping is an IOT plus too via automated check out in shops via bio metrics or so.

Food traceability can also be realised with IOT. In some areas of the world like in EU, food items should be able to be retraced to where they came from(Guillemin et al., 2010). An IOT technology like RFID tags are used for this purpose hence info regarding an item can always be updated digitally and even items can be called back where necessary. However, some producers aren't so happy with this due to privacy concerns since competitors can always get thiir Supply Chain insight. Security-wise what requirement is so essential can be derived from the classification regarding this application domain given in Table 7.5 below.

Table 7.5. Smart supplychain-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
SMART SUPLY CHAIN	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	AUTHENTICATION CONFIDEENTIALITY AVAILABILITY INTEGRITY PRIVACY
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	
	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

7.1.6 Smart manufacturing(PLM)

Through the linking of stuffs via the use of technology engraved deep down in the smart IOT gadgets, just by the use of Unique Identifiers data carriers can communicate through the intelligent network infrastructure and optimise the whole production processes. This is all with IIoT that takes use of new technology like M2M communications, WSN automation technologies and also Big-data for the creation of super-intelligent industrial

Table 7.6. Smart manufacturing-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
SMART MANUFACTURING	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	AUTHENTICATION CONFIDEENTIALITY AVAILABILITY INTEGRITY
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	

	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

ecosystems (M. Yu et al., 2020). The entire life cycle of products, that is from production to disposal can be managed too. Self-organising plus smart manufacturing solutions can be designed around the Identifiable Items i.e. IOT. The history of an item including the information encoded by manufaturer and its current status can always be monitered for objects have Identity with IOT. It's with such information that the end-of -life of an item can be known hence the safe and environmentally friendly disposing off or recycling of the products can be carried out.

7.1.7 Smart grid

Smart grid is amongst the application domains of the intelligent IOT backed-up infrastructure that attends to the distribution of electricity, it's management and consumption. With electrical energy having become a cherished resource of high-industrial value due to it's playing a key role in the economic development of societies, smart grids come in for the optimisation of the production and distribution of electricity with putting the day to day demands of users in consideration. This technology on which the electricity distribution lines are built on is comprised of a well connected network known as AMI that is situated in-between electricity generation centers and customers. Its major role the coordination of the generation of power with demand in consideration.. IOT is hugely deployed in this application domain with the chief goal of providing for QOS to the end-users. Further details about IOT in smart grids can be reached at (Firouzi et al., 2018). Nevertheless, a granular classsification of the security requirements for the smart grid is presented in Table 7.7 below.

Table 7.7. Smart grid-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
SMART GRID	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	NON-REPUDIATION CONFIDEENTIALITY AVAILABILITY INTEGRITY PRIVACY
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	
	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

7.1.8. Smart security systems

Wirelesssly identifiable device(s) are being put in use in different fields with the aim of increasing security and safety. Amongst the fields of application in this domain includes:

- Environmental Survaillance: Nature events like tsunamis, earthquakes, forest-fires, floodings and water or air pollution.

Table 7.8. Smart security-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
SMART SECURITY SYSTEMS	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	AUTHENTICATION CONFIDEENTIALITY AVAILABILITY INTEGRITY PRIVACY
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	

	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

- Buildings Monitoring: Gas- leaks, water-leaks, fire, vibratings, un-authorised entry,vandals.
- Personal: Payment systems, survailance, ID security.

While acquisition of information for the purpose security can pay off, it should be handled well too because in the event of the sensitive information databases being accessed by a malicous entity, meaningful relations might be made from the data which might even lead to potential damage.

7.1.9. Smart transportation systems

These also go by the term Intelligent Trasport Systems. These help with the monitoring and controlling of traffic data, computing it and then integrating this data in real time(Iqbal et al., 2020). The capability of monitoring traffic jam with just our mobile phones is amongst the enablers for smarter movement in cities. ITS are primarily comprised of RFID based tracking systems and GPS. The Internet of Things(IOT) puts forward more solutions for use in the collection of fares with road toll-systems. The screening of passengers and the luggage in movement from one place to another is also easily carried out accross the world with the help of IOT. With the connection and distribution of smart-processors throughout the transportation infrastructure and even with-in the vehicles themselves, it is possible to make transportation safe, green and more convinient. The unique classification of the security requirements for smart transport systems is presented in Table 7.9 below.

7.1.10. Smart farming systems

These can also be broken down as agriculture and breading. Due to the regulations that require the traceability of agrcultural animals together with their movements, the use of IOT technology is inevitable in this particular application domain. Real-time detection of the animals is done with IOT and this especially helps during the times when there is a disease out break on the farm. The fresh data gotten from real time IOT is also used by firms and governments while distributing incentives because it is calculated per number of cattle or sheep being looked after. Fraud is prevented that way thanks to IOT in farming(John et al., 2018). Animals are officially identified and vaccinationed at a national level and this even aids in the releasing of reports regarding the national animal health status on a country basis. Nevertheless, a very granular classsification of the security requirements for smart smart farming is presented in Table 7.10.

Table 7.9. Smart transport-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
SMART TRANSPORTATION SYSTEMS	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	PRIVACY AVAILABILITY AUTHENTICATION NON-REPUDIATION
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	
	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

Table 7.10. Smart farming-specific Layerwise IOT security requirement classification.

	IOT ARCHITECTURE LAYERS	POTENTIAL THREAT TARGETS		SECURITY REQUIREMENTS	TOP REQUIREMENTS (GENERIC)
		SECURITY CONCERN	THREATS AND ATTACKS	IOT SPECIFIC	
SMART FARMING SYSTEMS	DEVICE SENSING LAYER	Authentication, Authorization, Access control	Physical attacks Device-subversion attack Device-degradation Devices' data access	Light-weight solutions Heterogeneity, Interoperability/Robustness, Self-healing/Reliability, Real time, data freshness, Identity management	AVAILABILTY AUTHENTICATION
	NETWORK LAYER	Unauthorized Access, Modification of Routing Paths	Routing attack, Active data attack, Passive data attack, Flooding,	Support for composition, Heterogeneity, Interoperability, Light-weight solutions, Scalability, Incremental deployment, Mobility, dynamitic.	
	SERVICE COMPOSITION LAYER	Service (or Group) Authentication	Flooding, Device's data access, Data confidentiality, Cascading resources	Robustness, self-healing, reliability, real time, data freshness/Scalability, incremental deployment/ Composition, heterogeneity, interoperability/Decentralized management/Transiency, ephemeral.	
	APPLICATION LAYER	Unauthorized Access, Privacy Leakage, Integrity	Cascading resources, Interoperability, Multiple jurisdictions	Robustness, self-healing, reliability, real time, data freshness/Composition, heterogeneity, interoperability/Light-weight solutions/End-to-end security/Privacy.	
	USER INTERFACE LAYER	Authentication, Authorization, Access Control, Identity management for users	Trust, Behavioural threats, Tracking, Location privacy, Data Confidentiality	End-to-end security/Mobility, dynamic/Scalability, incremental deployment/Composition, heterogeneity, interoperability/Decentralized management/privacy.	

All the proposed security requirement classification tables in all the application domains of IOT mentioned above include a section tittled top requirements. All of these have been derived from a scoring system that assesed the risk factor of the identified possible threat and attack terrain in the particular domain. An illustration of the scoring of those in relation to the Smart Farming application domain is shown in Table 17 and further information is provided in Appendix regarding the terminology used in the assesment.

Table 7.11. Security requirement scoring system: the smart-farming case

SECURITY THREATS		TARGET	THREAT MATRIX						THREAT RATING					
			S	T	R	I	D	E	D	R	E	A	D	SCORE
Physical Attack	Device damage or disconnected	Devices/Services	x						7	3	2	3	8	4.6
Device subversion	Device capture or control						x		3	7	3	4	3	4
Device data access	Identity spoofing Replay attack			x					3	9	2	4	9	5.4
Device degradation	Battery exhaustion State manipulation DoS/DDoS		x					x	8	6	3	3	4	4.8
Routing Attack	Wormhole, Blackhole, Pharming	Communication		x	x		x		4	3	2	3	5	3.4
Active Data Attack	Channel Jamming							x	4	3	6	4	9	5.2
Passive Data Attack	Traffic analysis, Eaves-dropping			x					9	8	6	6	5	6.8
Flooding	DDoS, Routing table overflo, SYN flooding		x				x		5	3	6	8	2	4.8
Tracking and location privacy	Tag tracking, Device tracking	Mobility				x			3	6	2	5	7	4.6
Interoperability	Privacy of Data				x				8	3	6	3	4	4.8
Cascading resources	Malicious node manipulation		x				x		5	8	6	6	2	5.4
Multiple jurisdiction	Attacks on policy settings				x	x			3	7	2	4	9	5.0

Trust	Bad mounting, good mounting, self-promo	Users						x	4	8	6	6	7	6.2
Behavioural threats	Social engineering, Free-riding attack		x				x		6	3	9	4	6	5.6
Data confidentiality	User impersonation Phishing					x			5	3	8	2	3	4.2
Identity management	Subversion attacks						x	x	4	5	2	6	7	4.8

After having assigned risk ranking to the threats, it was then possible to sort the threats from the highest to the lowest risk and hence priotise mitigation through offering the top most security requirements to consider in a specific IOT systems.

8. CONCLUSIONS AND IMPLICATIONS

In this thesis, the security requirements of IOT have been analyzed and classified from a greatly wide perspective with consideration of the domain in which the IOT has been applied. The rationale behind this work resides on the evidence that, today IOT is applied in a wide range of areas due to its' cost effectiveness, efficiency and easy usability interms of the application(s) and service(s) rendered. Nonetheless, IOT sytems are currently not fully widely deployed because of key concerns in its security.

I've examined and classified the security requirements of IOT out there and presented a domain-aware classification of the security requirements after adopting an IOT security architecture that is well-explained in the respective section. After having realised that present-day IOT security requirements aren't well-structured for them to be able to cope with a wide range of attacks and threats out there that might come their way in an orderly manner. I noticed that a gap existed as per domain-specific IOT sequrity requirement classification is concerned. These are crucial while designing and keeping an IOT system secure. Differently from the rudimentary IOT security analysises, I did classify the numerous security concerns firstly in-to four definite groups that is attacks and threats in communication, devices/service, users(s) and mobility. Then, i did examine the possible attacks plus threats per layer. It's from these that i have come up with an up-to-date list of very significant IOT related security requirements. Furthermore, i amalgamated all of the requirements and classified them with the applied domain too in consideration. It should however be known that the requirements that i have classified and put forward aren't compulsory on IOT hundred percent but if taken into consideration, one can be able to give just the required security because various security needs of applications differ hence not all IOT nodes must necessesarily comply with the toughest security.

This work can be extended in different ways, for example by adding a more comprehensive security analysis or conducting a real world study on an IOT system practically with the security requirements presented in this thesis.

REFERENCES

Abdelaziz, A. K., Nafaa, M., Salim, G., 2013. Survey of routing attacks and countermeasures in mobile ad hoc networks. Proceedings - UKSim 15th International Conference on Computer Modelling and Simulation, UKSim 2013, 693–698. https://doi.org/10.1109/UKSim.2013.48

Abomhara, M., Koien, G. M., 2014. Security and privacy in the Internet of Things: Current status and open issues. 2014 International Conference on Privacy and Security in Mobile Systems, PRISMS 2014 - Co-Located with Global Wireless Summit. https://doi.org/10.1109/PRISMS.2014.6970594

Abu Waraga, O., Bettayeb, M., Nasir, Q., Abu Talib, M., 2020. Design and implementation of automated IoT security testbed. Computers and Security, 88. https://doi.org/10.1016/j.cose.2019.101648

Ahanger, T. A., Aljumah, A., 2019. Internet of things: A comprehensive study of security issues and defense mechanisms. IEEE Access, 7, 11020–11028. https://doi.org/10.1109/ACCESS.2018.2876939

Al-Emran, M., Malik, S. I., Al-Kabi, M. N., 2020. A Survey of Internet of Things (IoT) in Education: Opportunities and Challenges. In Studies in Computational Intelligence (Vol. 846, pp. 197–209). Springer Verlag. https://doi.org/10.1007/978-3-030-24513-9_12

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M., 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys and Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Alam, S., Chowdhury, M. M. R., Noll, J., 2011. Interoperability of security-enabled Internet of Things. Wireless Personal Communications, 61(3), 567–586. https://doi.org/10.1007/s11277-011-0384-6

Alfandi, O., Khanji, S., Ahmad, L., Khattak, A., 2021. A survey on boosting IoT security and privacy through blockchain Exploration , requirements , and open issues. Cluster Computing, 24(1), 37–55. https://doi.org/10.1007/s10586-020-03137-8

Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., Hamdi, M., 2021. A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. IEEE Internet of Things Journal, 8(6), 4004–4022. https://doi.org/10.1109/JIOT.2020.3015432

Ammar, M., Russello, G., Crispo, B., 2018. Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002

Approach, A. S., 2020. Security Requirements for the Internet of Things : 1–36. https://doi.org/10.3390/s20205897

Atzori, L., Iera, A., Morabito, G., 2017. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Networks, 56, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Babar, S., Mahalle, P., Stango, A., Prasad, N., Prasad, R., 2010. Proposed security model and threat taxonomy for the Internet of Things (IoT). Communications in Computer and Information Science, 89 CCIS, 420–429. https://doi.org/10.1007/978-3-642-14478-3_42

Baker, Nori, A. S., 2021. Internet of Things Security: A Survey. Communications in Computer and Information Science, 1347(December 2016), 95–117. https://doi.org/10.1007/978-981-33-6835-4_7

Baker, S. B., Xiang, W. E. I., Member, S., Atkinson, I. A. N., 2017. Internet of Things for Smart Healthcare.pdf. IEEE Access, 5, 26521–26544.

Baktyan, A., Zahary, A., 2018. A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective. EAI Endorsed Transactions on Internet of Things, 4(14), 156084. https://doi.org/10.4108/eai.20-12-2018.156084

Bassi, A., Horn, G., 2008. Internet of Things in 2020: Roadmap for the future.

Belkeziz, R., Jarir, Z., 2017. A survey on Internet of Things coordination. Proceedings - 2016 3rd International Conference on Systems of Collaboration, SysCo 2016, 4(3), 619–635. https://doi.org/10.1109/SYSCO.2016.7831328

Brass, I., Tanczer, L., Carr, M., Elsden, M., Blackstock, J., 2018. Standardising a moving target: The development and evolution of IoT security standards. IET Conference Publications, 2018(CP740), 1–9. https://doi.org/10.1049/cp.2018.0024

Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., Tarricone, L., 2015. An IoT-Aware Architecture for Smart Healthcare Systems. IEEE Internet of Things Journal, 2(6), 515–526. https://doi.org/10.1109/JIOT.2015.2417684

Chopra, K., Gupta, K., Lambora, A., 2019. Future Internet: The Internet of Things-A Literature Review. Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects, COMITCon 2019, 135–139. https://doi.org/10.1109/COMITCon.2019.8862269

Cirani, S., Ferrari, G., Veltri, L., 2013. Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview. Algorithms, 6, 197–226. https://doi.org/10.3390/a6020197

Cisco., 2022. Internet of Things (IoT) and our future - Cisco Blogs. Cisco. https://blogs.cisco.com/perspectives/internet-of-things-iot-and-our-future?dtid=osscdc000283

Dazine, J., Maizate, A., Hassouni, L., 2018. Internet of things security. 2018 IEEE International Conference on Technology Management, Operations and Decisions, ICTMOD 2018, 141, 137–141. https://doi.org/10.1109/ITMC.2018.8691239

Deogirikar, J., 2017. Security Attacks inIoT : A Survey. 32–37.

Dong, C., Wang, H., Ni, D., Liu, Y., Chen, Q., 2020. Impact Evaluation of Cyber-Attacks on Traffic Flow of Connected and Automated Vehicles. IEEE Access, 8, 86824–86835. https://doi.org/10.1109/ACCESS.2020.2993254

Ejaz, W., Anpalagan, A., 2019. Internet of Things for Smart Cities: Overview and Key Challenges (pp. 1–15). Springer, Cham. https://doi.org/10.1007/978-3-319-95037-2_1

Energycurb., 2021. Product - Curb. https://energycurb.com/product/

Firouzi, F., Rahmani, A. M., Mankodiya, K., Badaroglu, M., Merrett, G. V., Wong, P., Farahani, B., 2018. Internet-of-Things and big data for smarter healthcare: From device to architecture, applications and analytics. In Future Generation Computer Systems (Vol. 78, pp. 583–586). Elsevier B.V. https://doi.org/10.1016/j.future.2017.09.016

Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., Razafindralambo, T., 2011. A survey on facilities for experimental internet of things research. In IEEE Communications Magazine (Vol. 49, Issue 11, pp. 58–67). https://doi.org/10.1109/MCOM.2011.6069710

Gopal, T. S., Meerolla, M., Jyostna, G., Reddy Lakshmi Eswari, P., Magesh, E., 2018. Mitigating Mirai Malware Spreading in IoT Environment. 2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018, 2226–2230. https://doi.org/10.1109/ICACCI.2018.8554643

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Guillemin, P., Friess, P., Woelfflé, S., 2010. Vision and Challenges for Realising the Internet of Things Edited by Harald Sundmaeker. Europian Comission. https://op.europa.eu/en/publication-detail/-/publication/ed079554-72c3-4b4e-98f3-34d2780c28fc

Hackernews., 2020. Cyber Attack — learn more about it — The Hacker News. https://thehackernews.com/search/label/Cyber Attack

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., Wehrle, K., 2011. Security challenges in the IP-based Internet of Things. Wireless Personal Communications, 61(3), 527–542. https://doi.org/10.1007/s11277-011-0385-5

Hristozov, S., Huber, M., Sigl, G., 2020. Protecting RESTful IoT Devices from Battery Exhaustion DoS Attacks. Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2020, 316–327. https://doi.org/10.1109/HOST45689.2020.9300290

Internet, X. F., 2010. Future Internet Strategic Research Agenda. Internet Research, January, 1–73. https://doi.org/10.2759/26127

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., Bangash, Y. A., 2020. An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. IEEE Internet of Things Journal, 7(10), 10250–10276. https://doi.org/10.1109/JIOT.2020.2997651

John, J., Kasbekar, G., Sharma, D., Ramulu, V., Baghini, M., 2018. Design and Implementation of a Wireless Sensor Network for Agricultural Applications. EAI Endorsed Transactions on Internet of Things, 4(16), 158420. https://doi.org/10.4108/eai.13-7-2018.158420

Khan, R., Khan, S. U., Zaheer, R., Khan, S., 2012. Future internet: The internet of things architecture, possible applications and key challenges. Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012, 257–260. https://doi.org/10.1109/FIT.2012.53

Kim, J. T., 2015. Requirement of security for IoT application based on gateway. International Journal of Security and Its Applications, 9(10), 201–208. https://doi.org/10.14257/ijsia.2015.9.10.18

Kouicem, D. E., Bouabdallah, A., Lakhlef, H., 2018. Internet of things security: A top-down survey. In Computer Networks (Vol. 141, pp. 199–221). Elsevier B.V. https://doi.org/10.1016/j.comnet.2018.03.012

Li, S., Tryfonas, T., Li, H., 2016. The Internet of Things: a security point of view. Internet Research, 26(2), 337–359. https://doi.org/10.1108/IntR-07-2014-0173

Li, Y., Gao, M., Yang, L., Zhang, C., Zhang, B., Zhao, X., 2020. Design of and research on industrial measuring devices based on Internet of Things technology. Ad Hoc Networks, 102, 102072. https://doi.org/10.1016/j.adhoc.2020.102072

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W., 2017. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 4(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

Lu, Y., Xu, L. Da., 2019. Internet of things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103–2115. https://doi.org/10.1109/JIOT.2018.2869847

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., Ni, W., 2019. Anatomy of Threats to the Internet of Things. IEEE Communications Surveys and Tutorials, 21(2), 1636–1675. https://doi.org/10.1109/COMST.2018.2874978

Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P. M., Sundarasekar, R., Thota, C., 2018. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. Future Generation Computer Systems, 82, 375–387. https://doi.org/10.1016/j.future.2017.10.045

Marcus, H., 2022. How the Internet of Things Got Hacked | WIRED. Wired. https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/

Martin, T., Geneiatakis, D., Kounelis, I., Kerckhof, S., Fovino, I. N., 2020. Towards a formal iot security model. Symmetry, 12(8), 1–16. https://doi.org/10.3390/sym12081305

Militano, L., Araniti, G., Condoluci, M., Farris, I., Iera, A., 2015. Device-to-Device Communications for 5G Internet of Things. EAI Endorsed Transactions on Internet of Things, 1(1), 150598. https://doi.org/10.4108/eai.26-10-2015.150598

Minoli, D., Sohraby, K., Kouns, J., 2017. IoT security (IoTSec) considerations, requirements, and architectures. 2017 14th IEEE Annual Consumer Communications and Networking Conference, CCNC 2017, 1006–1007. https://doi.org/10.1109/CCNC.2017.7983271

Minshall, K., 2017. P olicing and the I nternet of T hings. IEEE Internet of Things Magazine, 2(October), 17–23.

Mohamad Noor, M. binti, Hassan, W. H., 2019. Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025

Mohsin, M., Anwar, Z., Zaman, F., Al-Shaer, E., 2017. IoTChecker: A data-driven framework for security analytics of Internet of Things configurations. Computers and Security, 70(2017), 199–223. https://doi.org/10.1016/j.cose.2017.05.012

Mosenia, A., Jha, N. K., 2017. A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586–602. https://doi.org/10.1109/TETC.2016.2606384

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N., 2019. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Communications Surveys and Tutorials, 21(3), 2702–2733. https://doi.org/10.1109/COMST.2019.2910750

Ning, H., Liu, H., Yang, L. T., 2013. Cyberentity security in the internet of things. Computer, 46(4), 46–53. https://doi.org/10.1109/MC.2013.74

Pal, S., Hitchens, M., Varadharajan, V., 2019. Modeling identity for the internet of things: Survey, classification and trends. Proceedings of the International Conference on Sensing Technology, ICST, 2018-Decem, 45–51. https://doi.org/10.1109/ICSensT.2018.8603595

Park, K. C., Shin, D. H., 2017. Security assessment framework for IoT service. Telecommunication Systems, 64(1), 193–209. https://doi.org/10.1007/s11235-016-0168-0

Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D., 2014. Context aware computing for the internet of things: A survey. IEEE Communications Surveys and Tutorials, 16(1), 414–454. https://doi.org/10.1109/SURV.2013.042313.00197

Philips., 2020. Ambiance with smart light: Bluetooth Bridge | Philips Hue. https://www.philips-hue.com/en-us/explore-hue/propositions/personal-mood-lighting

Pongle, P., Chavan, G., 2015. A survey: Attacks on RPL and 6LoWPAN in IoT. 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015, 00(c), 12–17. https://doi.org/10.1109/PERVASIVE.2015.7087034

Radanliev, P., De Roure, D., Page, K., Nurse, J. R. C., Mantilla Montalvo, R., Santos, O., Maddox, L. T., Burnap, P., 2020. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. In Cybersecurity (Vol. 3, Issue 1). https://doi.org/10.1186/s42400-020-00052-8

Riahi Sfar, A., Natalizio, E., Challal, Y., Chtourou, Z., 2018. A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118–137. https://doi.org/10.1016/j.dcan.2017.04.003

Risteska Stojkoska, B. L., Trivodaliev, K. V., 2017. A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.006

Rizvi, S., Orr, R., Cox, A., Ashokkumar, P., Rizvi, M. R., 2020. Identifying the attack surface for IoT network. Internet of Things, 9, 100162. https://doi.org/10.1016/j.iot.2020.100162

Roman, R., Zhou, J., Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Ronen, E., Shamir, A., Weingarten, A. O., Oflynn, C., 2018. IoT Goes Nuclear: Creating a Zigbee Chain Reaction. IEEE Security and Privacy, 16(1), 54–62. https://doi.org/10.1109/MSP.2018.1331033

Sadique, K. M., Rahmani, R., Johannesson, P., 2018. Towards security on internet of things: Applications and challenges in technology. Procedia Computer Science, 141, 199–206. https://doi.org/10.1016/j.procs.2018.10.168

Sain, M., Kang, Y. J., Lee, H. J., 2017. Survey on security in Internet of Things: State of the art and challenges. International Conference on Advanced Communication Technology, ICACT, 699–704. https://doi.org/10.23919/ICACT.2017.7890183

Salman, O., Elhajj, I., Chehab, A., Kayssi, A., 2018. IoT survey: An SDN and fog computing perspective. Computer Networks, 143(2018), 221–246. https://doi.org/10.1016/j.comnet.2018.07.020

Shaikh, Y., Parvati, V. K., Biradar, S. R., 2019. Survey of smart healthcare systems using internet of things (IoT) : (Invited paper). Proceedings of the 2018 International Conference On Communication, Computing and Internet of Things, IC3IoT 2018, 508–513. https://doi.org/10.1109/IC3IoT.2018.8668128

Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini, A., 2015. Security, privacy and trust in Internet of things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Siegel, J. E., Erb, D. C., Sarma, S. E., 2018. A survey of the connected vehicle Landscape - Architectures, enabling technologies, applications, and development areas. IEEE Transactions on Intelligent Transportation Systems, 19(8), 2391–2406. https://doi.org/10.1109/TITS.2017.2749459

Singh, J., Pasquier, T., Bacon, J., Ko, H., Eyers, D., 2016. Twenty Security Considerations for Cloud-Supported Internet of Things. IEEE Internet of Things Journal, 3(3), 269–284. https://doi.org/10.1109/JIOT.2015.2460333

Sivanathan, A., Gharakheili, H. H., Sivaraman, V., 2018. Can We Classify an IoT Device using TCP Port Scan? 2018 IEEE 9th International Conference on Information and Automation for Sustainability, ICIAfS 2018. https://doi.org/10.1109/ICIAFS.2018.8913346

Smith, S. W., 2020. Securing the Internet of Things : IEEE Computer Society, 4. https://doi.org/10.1109/MC.2020.2984254

Statista., 2022. Number of IoT devices 2015-2025. Statista. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Swamy, S. N., 2017. Security Threats in the Application layer in IOT Applications. 477–480.

Tabrizi, S. S., Ibrahim, D., 2016. Security of the internet of things: An overview. ACM International Conference Proceeding Series, 22(1), 146–150. https://doi.org/10.1145/3023924.3023943

Tewari, A., Gupta, B. B., 2020. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems, 108, 909–920. https://doi.org/10.1016/j.future.2018.04.027

Tourani, R., Misra, S., Mick, T., Panwar, G., 2018. Security, Privacy, and Access Control in Information-Centric Networking: A Survey. In IEEE Communications Surveys and Tutorials (Vol. 20, Issue 1, pp. 556–600). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/COMST.2017.2749508

Turkish Ministry of Health., n.d.. e-Nabız | Turkish Ministry of Health. Retrieved May 30, 2021, from https://enabiz.gov.tr/

Wang, F., Hu, L., Hu, J., Zhou, J., Zhao, K., 2017. Recent Advances in the Internet of Things: Multiple Perspectives. In IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India) (Vol. 34, Issue 2, pp. 122–132). Taylor and Francis Ltd. https://doi.org/10.1080/02564602.2016.1155419

Wright, M. K., Adler, M., Levine, B. N., Shields, C., 2004. The predecessor attack: An analysis of a threat to anonymous communications systems. ACM Transactions on Information and System Security, 7(4), 489–522. https://doi.org/10.1145/1042031.1042032

Xie, B., Kumar, A., Chen, C. M., 2013. Taxonomy and analysis of security protocols for Internet of Things. Future Generation Computer Systems, 29(7), 1680–1681. https://doi.org/10.1016/j.future.2013.04.025

Xu, L. Da, He, W., Li, S., 2014. Internet of things in industries: A survey. In IEEE Transactions on Industrial Informatics (Vol. 10, Issue 4, pp. 2233–2243). IEEE Computer Society. https://doi.org/10.1109/TII.2014.2300753

Yang, J. C., Fang, B. X., 2011. Security model and key technologies for the Internet of things. Journal of China Universities of Posts and Telecommunications, 18(SUPPL.2), 109–112. https://doi.org/10.1016/S1005-8885(10)60159-8

Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., Liu, W., 2011. Study and application on the architecture and key technologies for IOT. 2011 International

Conference on Multimedia Technology, ICMT 2011, 747–751. https://doi.org/10.1109/ICMT.2011.6002149

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., Guizani, M., 2017. Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Communications, 24(3), 10–16. https://doi.org/10.1109/MWC.2017.1600421

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. M. A., Hong, C. S., 2019. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems, 92(May 2018), 265–275. https://doi.org/10.1016/j.future.2018.09.058

Yassein, M. B., Shatnawi, M. Q., Al-Zoubi, D., 2016. Application layer protocols for the Internet of Things: A survey. Proceedings - 2016 International Conference on Engineering and MIS, ICEMIS 2016. https://doi.org/10.1109/ICEMIS.2016.7745303

Yu, M., Zhuge, J., Cao, M., Shi, Z., Jiang, L., 2020. A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. Future Internet, 12(2). https://doi.org/10.3390/fi12020027

Yu, S., Wang, G., Liu, X., Niu, J., 2018. Security and Privacy in the Age of the Smart Internet of Things: An Overview from a Networking Perspective. IEEE Communications Magazine, 56(9), 14–18. https://doi.org/10.1109/MCOM.2018.1701204

Zaidan, A. A., Zaidan, B. B., 2020. A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. Artificial Intelligence Review, 53(1), 141–165. https://doi.org/10.1007/s10462-018-9648-9

Zhao, K., Ge, L., 2013. A survey on the internet of things security. Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013, 663–667. https://doi.org/10.1109/CIS.2013.145

Zhou, W., Jia, Y., Peng, A., Zhang, Y., Liu, P., 2019. The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733

Zimmermann, A., Schmidt, R., Sandkuhl, K., Wißotzki, M., Jugel, D., Möhring, M., 2015. Digital enterprise architecture-transformation for the internet of things. Proceedings of the 2015 IEEE 19th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations, EDOCW 2015, 130–138. https://doi.org/10.1109/EDOCW.2015.16

APPENDIX

Appendix A. STRIDE

Appendix B. DREAD

Appendix A. STRIDE

The following table shows the STRIDE threat model together with meanings for each.

Table A.1. STRIDE threat model

Threat	Desired Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Appendix B. DREAD

The following table shows DREAD which is a risk assessment model for security purpose.

Table B.1. DREAD risk assessment model

Category	Description
Damage	How big would the damage be if the attack succeeded?
Reproducibility	How easy is it to reproduce this specific attack?
Exploitability	How much time, effort, and expertise is needed to exploit this threat?
Affected users	If this threat was exploited, what percentage of users would be affected?
Discoverability	How easy is it for an attacker to discover this threat?

A point system of numbers 1-10, representing low to high severity, is used in the calculation of a DREAD score which possibly helps while comparing one threat to another. While ranking threats, the questions above that encompass all the factor of risk are answered in the process.

BIBLIOGRAPHY

Name Surname : Arafat MUKALAZI

Education

High School : International Anatolian School, 2014

Bachelors : Istanbul Zaim University,
Faculty of Engineering and Natural Sciences,
Computer Engineering Department.

Publications

Mukalazi, A., Boyacı, A., 2022. The Internet of Things: a domain-specific security requirement classification. 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, June 9-11, 2022 Ankara, Türkiye.