

# **Study on Comparative Security Analysis of IOT Framework**

By  
**Abdul Ohab**  
**ID: 151-19-1724**

**Md. Tahasin Abid**  
**ID: 151-19-1727**

**Mustafizur Rahman**  
**ID: 151-19-1729**

This Report Presented in Partial Fulfillment of the Requirements for the Degree of  
Bachelor of Science in Electronics and Telecommunication Engineering  
(B.Sc. in ETE)

Supervised By

Engr. Md. Zahirul Islam  
Assistant Professor  
Department of ICE  
Daffodil International University

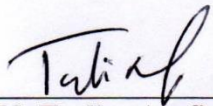


Department of Information & Communication Engineering  
Daffodil International University  
Dhaka, Bangladesh  
January, 2019

## APPROVAL

The Thesis titled “**Study on comparative security analysis of IOT framework**” submitted by Abdul Ohab ID: 151-19-1724, Md.Tahasin Abid ID:151-19-1727 and Mustafizur Rahman ID: 151-19-1729 to the Department of Information and Communication Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirement for the degree of Bachelor of Science in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation was held on January 17, 2019.


### BOARD OF EXAMINERS

---

**(Md. Taslim Arefin)**  
**Associate Professor & Head**  
Department of ICE  
Daffodil International University

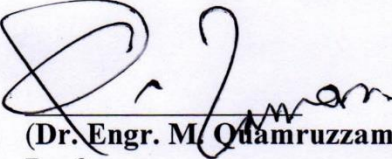
Chairman

---

**(Dr. A.K.M Fazlul Haque)**  
**Professor**  
Department of ICE  
Daffodil International University

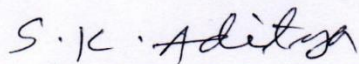
Internal Examiner

---

**(Dr. Engr. M. Quamruzzaman)**  
**Professor**  
Department of ICE  
Daffodil International University

Internal Examiner

---

**Dr. Subrata Kumar Aditya**  
**Professor**  
Department of EEE  
University of Dhaka

External Examiner

## **ACKNOWLEDGEMENT**

Firstly, I like to forward my regard to Almighty Allah for showing me the right path while attempting the duty.

The real sprit of achieving a destiny is through the path of eminence and solid discipline. I would have never achieved in finishing my job without the alliance, inspiration and assist issued to me by different personalities.

This thesis report would not have been manageable without the assist and direction of **Engr. Md. Zahirul Islam**, Assistant Professor, Department of Information and Communication Engineering, Daffodil International University, under whose supervision I chose this topic.

I would like to express my heartiest respect to **Md. Taslim Arefin**, Associate Professor & Head, Department of Information and Communication Engineering, for his kind help and also to other faculty members, the staffs of the ICE Department of Daffodil International University.

I must grant with due respect the endless support and patience of my family members for finishing this internship.

**Abdul Ohab**

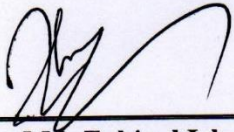
**Md. Tahasin Abid**

**Mustafizur Rahman**

## DECLARATION

I hereby declare that this thesis Report has been done by me under the supervision of Engr. **Md. Zahirul Islam**, Assistant Professor, Department of ICE, Daffodil International University. I also declare that neither this report nor any part of it has been submitted elsewhere for award of any degree or diploma.

### Supervised By



**Engr. Md. Zahirul Islam**  
Assistant Professor  
Department of ICE  
Daffodil International University

### Submitted By

*Abdul ohab*

*Tahasin Abid*

*Mustafizur Rahman .*

---

Abdul Ohab  
ID: 151-19-1724  
Department of ICE  
Daffodil International  
University

Md. Tahasin Abid  
ID: 151-19-1727  
Department of ICE  
Daffodil International  
University

Mustafizur Rahaman  
ID: 151-19-1729  
Department of ICE  
Daffodil International  
University

# **DEDICATION**

**THIS THESIS IS DEDICATED  
TO  
MY PARENTS**

## **ABSTRACT**

The Internet of Things (IoT) gadgets have turned out to be well known in various spaces, for example, e-Health, e-Home, online business, and e-Trafficking, and so forth. With expanded arrangement of IoT gadgets in reality, they can be, and now and again, as of now are liable to malicious attacks to trade off the security and protection of the IoT devices. While various analysts have investigated such security difficulties and open issues in IoT, there is a deplorable absence of an orderly investigation of the security challenges in the IoT scene. In this report, we go for connecting this gap by directing a careful investigation of IoT security difficulties and issues. A definite investigation of IoT attack surfaces, frameworks, security issues and has been presented. A brief summary of comparison among the IoT frameworks those can provide countermeasures against various security attacks in IoT also been addressed.

## Contents

<b>Acknowledgment</b>	<b>ii</b>
<b>Declaration</b>	<b>iii</b>
<b>Dedication</b>	<b>iv</b>
<b>Abstract</b>	<b>v</b>
<b>Chapter 1 Introduction</b>	<b>1-4</b>
1.1. General Introduction	1-2
1.2 Motivation	2
1.3 Related work	2-3
1.4 Goal of this research work	3
1.5 Outline Methodology	4
1.6 Organization of the thesis	4
<b>Chapter 2 Internet of things (IOT)</b>	<b>5-14</b>
2.1 Introduction	5-6
2.2 Background History	6-8
2.3 Characteristics of IoT	8-9
2.4 Basic elements of IoT architecture	9-12
2.5 Application of IoT	12-14
<b>Chapter 3 IoT Framework</b>	<b>15-51</b>
3.1. AWS IoT	15

3.1.1. Architecture	15-18
3.1.2. Hardware specification	18-19
3.1.3. Security features	19-21
3.2. ARM mbed IoT	21-22
3.2.1. Architecture	22-25
3.2.2. Hardware specifications	25
3.2.3. Security features	25-27
3.3. Azure IoT suite	27
3.3.1. Architecture	27-29
3.3.2 Hardware specification	29-30
3.3.2. Security features	30-31
3.4. Brillo/Weave	31
3.4.1. Architecture	31-33
3.4.2. Hardwar specification	33
3.4.3. Security features	34
3.5. Calvin	34-35
3.5.1. Architecture	35-36
3.5.2. Hardware specification	36
3.5.3. Security features	36-38
3.6. HomeKit	38
3.6.1. Architecture	38-40
3.6.2. Hardware and specification	40
3.6.3. Security Feature	41-43
3.7. Kura	43
3.7.1. Architecture	43-44
3.7.2. Hardware specifications	44-45
3.7.3. Security features	45
3.8. SmartThings	46
3.8.1. Architecture	46-49
3.8.2. Hardware specification	49
3.8.3. Security features	49-51



<b>Chapter 4 Attack or threat</b>	<b>52-60</b>
4.1. DoS attack	52
4.2. Jamming Attack	53
4.3. Blue borne attack	53-54
4.4. Remote access using telnet	54-55
4.5. Sybil attack	55-56
4.6. Exploit kit	56
4.7. Man in the middle attack	57
4.8. Replay attack	58
4.9. Ransomware	58-59
4.10. Side channel attack	59-60
<b>Chapter 5 Result and comparative analysis</b>	<b>61-75</b>
5.1. Aws framework	61-63
5.2. ARM mbed	63-64
5.3. Azure IoT suite	64-66
5.4. Brillo/weave	66-68
5.5. Ericsson/Calvin	68-69
5.6. Apple homekit	69-70
5.7. Smarththing/Samsung	70-72
5.8. Kuru/Java	72-74
<b>Chapter 6 Conclusion</b>	<b>76</b>
<b>References</b>	<b>77-86</b>

## List of Figures

Fig2.1: IoT architecture	10
Fig.3.1 AWS IoT architecture	16
Fig.3.2 AWS IoT Security mechanism	19
Fig.3.3 mbed OS Architecture.	23
Fig.3.4 ARM mbed IoT architecture	24
Fig.3.5 ARM mbed IoT security architecture	26
Fig.3.6 Azure IoT architecture	28
Fig.3.7 Azure IoT security architecture.	30
Fig.3.8 Brillo/Wave architecture	32
Fig.3.9 Calvin architecture	35
Fig.3.10 Calvin communication system	37
Fig.3.11 HomeKit architecture	39
Fig.3.12 Kura architecture	44
Fig.3.13 SmarthThings architecture	47
Fig.3.14 The structure of the SmartThings cloud system	48
Fig. 4.1 jamming attack matrix	53

## **List of Tables**

**5. Comparative security analysis**

**75**

# Chapter 1

## Introduction

### 1.1. General Introduction

The internet of things (IoT) plays out a staggering capacity in all parts of our regular day to day existences. It covers numerous fields which incorporate social insurance, autos, stimulations, business home gear, sports, homes, and so forth. The inescapability of IoT facilitates a couple of typical exercises, advances the manner in which individuals have cooperation with the earth and environment, and enlarges our social communications with other individuals and items. This all-encompassing vision, be that as it may, raises additionally a couple of concerns, similar to which level of wellbeing the IoT ought to give? Also, the manner in which it gives and ensures the privateness of its clients?

Developing applications for the IoT can be an extreme mission because of a few thought processes; (i) The high multifaceted nature of apportioned figuring, (ii) The shortage of general indications or structures that handle low stage correspondence and improve unreasonable dimension usage, (iii) Multiple programming dialects, and (iv) Diverse correspondence conventions. It incorporates engineers to control the framework and manage both programming and equipment layers together with keeping up all functional and non-valuable programming program prerequisites. This intricacy has achieved a short development as far as presenting IoT programming structures that deal with the previously mentioned difficulties.

Exceptionally nowadays, various IoT systems had been discharged by method for the main investors in the IoT space and by utilizing the examinations network with a reason to help and make it smooth to extend, convey and hold IoT bundles. Every member built his technique depending on his vision closer to the IoT worldwide [1]. On this, we look at the homes of a subset of IoT structures, focusing on explicitly their assurance includes and limiting limit of numerous danger. The picked set of IoT plat-forms<sup>1</sup> comprises of AWS IoT from Amazon, ARM bed from ARM and distinctive accomplices, Azure IoT Suite from Microsoft,

Brillo/Weave from Google, Calvin from Ericsson, HomeKit from Apple, Kura from Eclipse, and SmartThings from Samsung.

We chose the above systems dependent on the resulting criteria: (I) The notoriety of the transporters inside the product program and gadgets ventures, (ii) The assistance of expedient utility enhancement and the quantity of uses on the store, (iii) The inclusion and usage of the structure, and its notoriety in the IoT commercial center.

## **1.2 Motivation**

A standout amongst the most prominent digital security challenges in the cutting edge innovative biological community is that of IT security in IoT gadgets. As we approach a more prominent interconnected society with more noteworthy keen items associated with the cloud, the dangers additionally increment and vulnerabilities that need to be recognized and redressed duplicate. The web of things (IoT) is miles a mechanical achievement that is totally reforming our every day life. An expanding number of gadgets are associated with the web. Nowadays we can gather, store, break down and control more information to give more noteworthy viable arrangements from the control and gigantic assessment of information and engineered insight applications. None of that may be conceivable in the event that we didn't have IoT gadgets to encourage information storing up and accumulation. Instruction, medicinal services, the vehicle business, compact gadgets and extension of fields are beginning to profit by the IoT gifts. Be that as it may, this circumstance is likewise extremely alluring to cybercriminals, who see inside the expansion of gadgets and applications an extraordinary impetus for their exercises. Therefore, minimizing cyber-attack, a secure IoT framework can be deployed.[181]

## **1.3 Related work**

A few overview papers have been distributed covering different points of the IoT space. Al-Fuqaha et al. [2] overviewed the IoT all in all, referencing different IoT models, advertise openings, IoT components, correspondence advancements, standard application conventions, principle difficulties and open research issues in the IoT territory. Derhamy et al. [3] exhibited various business IoT structures and gave a similar examination dependent on used methodologies, upheld conventions, use in industry, equipment prerequisites, and applications

advancement. A concise diagram of the current IETF models for the Internet of things is given in [4].

Security and protection issues in IoT had a ton of consideration from the exploration network and tended to at various dimensions. In [5], the creators reviewed the security and protection issues in IoT from four alternate points of view. To begin with, they feature the confinements of applying security in IoT gadgets (e.g. battery lifetime, processing power) and the proposed answers for them (e.g. lightweight encryption plot intended for implanted frameworks). Second, they condense the classifications of IoT assaults (e.g. physical, remote, neighborhood, and so on.). Third, they center around the instruments and structures planned and executed for confirmation and approval purposes. Last, they break down the security issues at various layers (e.g. physical, arrange, and so forth.). Creators in [6,7] tended to the security and protection issues in IoT at each layer identified in the 3-layer engineering [8,9] studied a large portion of the security flaws existing in IoT, came about because of the different correspondence innovations utilized in remote sensor systems. An approval get to display is proposed in [10] as a security system for the IoT so as to guarantee controlling access and approving real clients as it were. Creators in on the difficulties and approach proposed to beat the security issues of the IoT middleware, where countless frameworks acquire security properties from the middleware structures. Contingent upon the notable security and protection dangers, creators break down and assess the accessible middleware methodologies and show how security is taken care of by each methodology. The work finishes up with outlining a lot of necessities to have a protected IoT middleware.

#### **1.4 Goal of this research work**

- Giving an image of the current state of the artwork IoT structures and figuring out the trends of present-day designs of such systems.
- Presenting an excessive degree assessment among the one of a kind architecture of the numerous frameworks.
- Focusing at the models designed and processes advanced for making sure safety and privateness in those frameworks.
- Find out the best framework which can minimize huge number of attack.

## 1.5 Outline Methodology

The methodology consists of the following stages,

- 1) According to the IoT security framework we consider eight frameworks. Where architecture specification, hardware specification and security features are include.
- 2) Then we find out the various security threats which can damage the iot device.
- 3) Then according to the study we find out the comparatively best iot framework which can minimize most of the security threat.
- 4) In this way the research is done.

## 1.6 Organization of the thesis

**The first chapter** contains motivation and goal of the thesis work.

**Second chapter** brief details of Overall view of Internet of Things (IoT), IoT architecture and applications.

**Chapter three** contains brief details of Overall view in security framework and its specification.

**Chapter four** contains brief details of overall view in security threat.

**Chapter five** contains results and comparative analysis.

Last of all Chapter six contains conclusion.

## Chapter 2

### Internet of things (IOT)

#### 2.1 Introduction

IoT is the network of vehicles, devices and home hardware that incorporate gadgets, programming project, actuators, and availability which enables this stuff to associate, have communication and substitute information. [11]

IoT includes broadening web availability past favored gadgets, which incorporates PC frameworks, workstations, cell phones, and tablets, to any assortment of truly idiotic or non-net-empowered physical gadgets and customary items. Inserted with innovation, those gadgets can impart and have communication over the web, and that they can be remotely checked and controlled.

The internet is an era that performed a critical function in the transformation of the part to its cutting edge nation. Presently the web has achieved an express that it isn't distinguished as an administration, anyway a piece of the earth around us. The wide uses of the web came into its top as everything around us are associated with one another and turn out to be a piece of some system. Presently, the circumstance has come to in which whatever can be 'cunning' or 'advanced'. The 'web of things' conceptualizes the field which has the majority of the issues round you are having some sort of computerized character and part of some system, imparting and sharing insights [12]. The web of things (IoT) alludes to a consistently developing system including the items which are customary PC frameworks or versatile contraptions as well as the real substances like watches, wearable gadgets, and other astute articles [13]. It tends to be considered as a system or interconnection of sensors and actuators having a totally interesting structure for records sharing. The IoT doesn't keep on with any specific convention anyway is available to any condition of the work of art convention accessible now and decorate the range to the most [14]. What's more, the control of data and system can be programmed and the efeciency can be expanded utilizing the M2M associations when every one of the gadgets develop as cunning. Indeed, even the individual information sources can be electronic with sensors and the appropriate responses may be conveyed on the double to the things in which it is intended to



show up [15]. This adjustment in the idea from associated PCs to a system of 'matters' changed the computerized universal and made a crisp influx of advancement. The possibility of advanced character and network to every element has expanded the influence of the web to another amount. With the wi-fi availability and new computerized identification methods like RFID, the IoT was given its grip over our step by step presence.

IoT incorporates assorted sensors, objects and astute hubs which are fit for speaking with each extraordinary without human mediation [16]. The things/matters work self-governingly in reference to different contraptions. IoT nodes are able to hand over light-weight records, having access to and authorizing cloud-primarily based sources for collecting and extracting decisions with the aid of analyzing collected facts. The development of IoT has achieved the unavoidable availability of individuals, administrations, sensors, and things. IoT gadgets right now are conveyed in a broad scope of utilizations from savvy lattices to social insurance and insightful transport frameworks [17]. Monstrous endeavor openings that exist inside IoT region quite lifted a wide assortment of brilliant gadgets and astute, free contributions provided in IoT systems. Moreover, dependence on IoT gadgets on cloud framework for measurements switch, carport and examination caused the improvement of cloud-empowered IoT systems [18]. Security inconveniences which incorporate privateness, motivate passage to control, loosened up verbal trade and comfortable carport of records are getting to be across the board difficulties in the IoT condition [19]. besides, each unmarried apparatus that we make, each new sensor that we send, and each and every byte that is synchronized inside an IoT situation can also sooner or later come underneath scrutiny inside the course of an research.

## **2.2 Background History**

The plain quick development of Internet-connected gadgets, extending from very basic sensors to genuinely complex cloud servers, shapes the net of things, in which things, in this unique situation, alludes to a broad assortment of contraptions (e.g. shrewd knobs, smart locks, IP cameras, indoor regulators, electronic home gear, wake up timers, candy machines, and that's only the tip of the iceberg). The likeness among all IoT things is the capacity to interface with the web and substitute information. The system availability include grants controlling things remotely over the current network framework, following in more incorporation with the genuine worldwide and less human mediation. The IoT changes those things from being established to

brilliant by method for misusing its fundamental innovations which incorporates inescapable registering, correspondence capacities, web conventions, and bundles. Conventions are required in order to see the talked dialect of the IoT devices as far as the organization of traded messages and select the privilege beyond any doubt territories that watch the different usefulness of each device. Applications choose phases of granularity and subject matter of the IoT gadget and the manner in which enormous are the data created for investigation capacities. Moreover, they suggest the general extent of the IoT structure overlaying the setting of the executed region.

The idea of IoT system incorporates distinguishing a structure which organizes and controls forms being performed by methods for the various IoT factors. This structure is an immovable direction, conventions, and standards that set up the way of preparing certainties and exchange messages among every concerned gathering (e.g. installed gadgets, cloud, stop clients). Moreover, it should help the abnormal state execution of IoT projects and shroud the intricacy of foundation conventions. There are various methodology that might be pursued to develop an IoT system depending at the necessities of the objective endeavor [20].

On this paper, we're centered around IoT structures principally dependent on people in general cloud approach, as they are the most regularly utilized and widely to be had inside the IoT showcase. The essential building squares of any cloud-based IoT structure are the physical things and the conventions. Physical articles envelop: (I) astute gadgets comprising of sensors, actuators, and numerous others. (ii) Servers go about as a cloud-backend or centers/doors for steering, putting away, and gaining admittance to various snippets of data, and (iii) quit-clients spoken to by method for the projects they use to get section to data and have association with IoT gadgets. Conventions keep running on various layers and give offer up-to-stop impart. To the high caliber of our comprehension, there's no a far reaching IoT structure yet. For straightforwardness, we're thinking about the fundamental one that is a 3-layer engineering [21] made out of programming, network, and idea layers. The thought layer has a place with the physical devices that wind up mindful of and encounter simple actualities and afterward digitize it for transportation purposes. Framework conventions which incorporates ZigBee [22], Z-Wave [23], Bluetooth Low Energy (BLE) [24], WiFi, and LTE-A [25] keep running inside the system layer. The utility layer is the interface for end-clients to get to records and converse with their

IoT gadgets. It underpins standard conventions comprehensive of Hypertext Transfer Protocol (HTTP) [26], obliged application Protocol (CoAP) [27], Message Queue Telemetry Transport (MQTT) [28], Extensible Messaging and Presence Protocol (XMPP) [29], Advanced Messaging Queuing Protocol (AMQP) [30], and Data Distribution supplier (DDS) [31].

## 2.3 Characteristics of IoT

IoT offers commitments to the general estimating with the assistance of the interconnection of different physical gadgets the readiness of the general structure. It's based absolutely at the viably present advances. Coming up next are the qualities of the highlights of iot(internet of things).[32]

- **intelligence** – iot could be a mix of hardware and programming group program pleasant with current computations and figurings. The limits of iot is additional relevant due to its learning which empowers them to answer and act to keep with the circumstance. Its miles due to knowledge that one among of gadgets speaks with every interesting.
- **Connectivity – Availability in IoT** licenses it to relate contrasted gadgets that we will in general use it well ordered lifestyles. This property adds to fundamental learning of the IoT orchestrate. This current, in addition, makes infers for complete splendid market conceivable outcomes by prescribes that of working up an arrangement of sensible things and applications. Furthermore, the framework is consistently more prominent congenial and good.
- **Dynamic Nature** – the iot gadgets catch data from its encompassing condition. This catching of data is finished by methods for the dynamic adjustments that take area around those devices. The nation of iot contraptions alterations powerfully like related or detached and furthermore in light of physical circumstances like temperature territory and speed. Also, it can interchange because of the character area and time.
- **Enormity** – inside the near future, the number of gadgets associated with the system will be more noteworthy than it is nowadays. Also, it will turn out to be parts additional hard to oversee and deal with data produced from these gadgets.

- **Sensing** – sensors are an important remember iot prepare at the same time as no longer than the modifications inside nature cannot be diagnosed and calculable by means of a technique for the devices. These sensors have collaboration with the planet for the discovery and accumulation of statistics. The facts it really is detected by utilizing the detector is basically the contribution from the surroundings which might convey a couple of information.
- **Diversity** – a standout amongst the most critical characteristics of IoT is assorted variety and heterogeneity. The IoT gadgets have remarkable equipment stages and organize and they're fit for speaking with various gadgets by means of exceptional systems. The IoT organize is equipped for help availability between particular systems. Adaptability, measured quality, extensibility, and interoperability are the issues in charge of this assorted variety.
- **Security** – despite the very fact that there's the quantity of applications of iot there is a pair of security and privateers problems with the iot network. Endeavors are being created for subsidence these security problems. Its miles essential to anchor information as its miles being changed between devices because it contains sensitive info.

## 2.4 Basic elements of IoT architecture

**Things:** A "thing" is an object outfitted with sensors that assemble information which will be exchanged over a system and actuators that enable things to act. This idea incorporates ice chests, road lights, structures, vehicles, generation hardware, recovery gear and everything else possible. Sensors are not in all cases physically appended to the things: sensors may need to screen, for instance, what occurs in the nearest condition to a thing.

IoT architecture diagram

**Gateways:** gateway knowledge goes from things to the cloud and therefore the different path

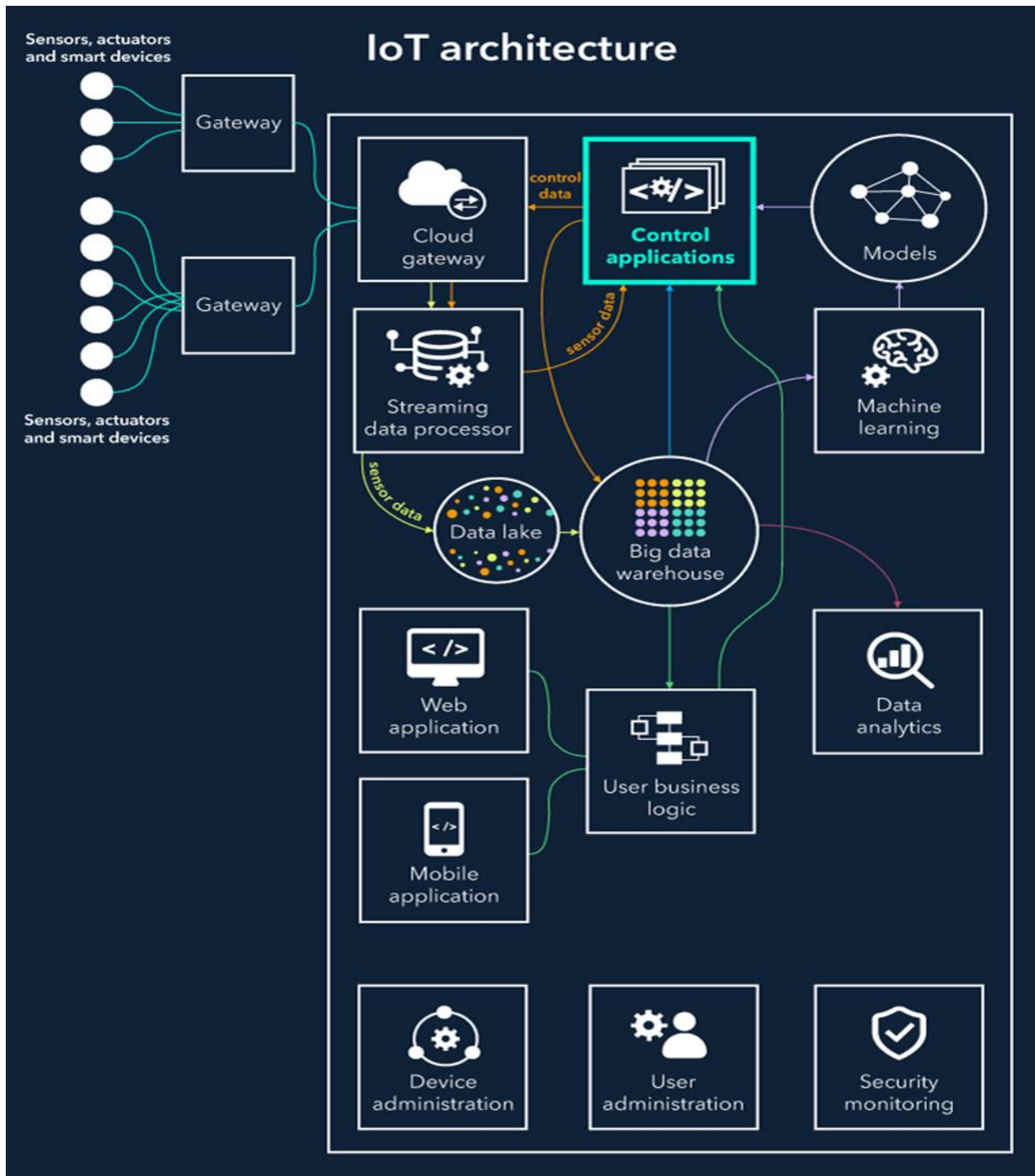


Fig.2.1 IoT architecture

around by ways for the passages. An entree provides organize among things and also the cloud a small amount of the IoT course of action licenses knowledge preprocessing and filtering ahead of

moving it to the cloud (to direct the extent of data for glorious taking care of and swing left) and transmits management procedures going from the cloud to things. Things by then execute headings the organization of their actuators.

**Cloud gateway:** Cloud door encourages info pressure and secure info transmission between field passages and cloud IoT servers. It likewise guarantees similarity with completely different conventions and speaks with field gateway utilizing numerous conventions relying upon what convention is upheld by portals gateway.

**Streaming data processor:** streaming information processor guarantees compelling development of data statistics to an information lake and manage applications. No statistics can be incidentally lost or ruined

**Data Lake:** A data lake is used for putting away the data made by victimization associated devices in its standard configuration. Massive data comes in "clusters" or in "streams". On the purpose while the data is required for big stories, it's separated from Associate in nursing Statistics Lake and stacked to a first-rate statistics distribution middle a big data warehouse.

**Big data warehouse:** Big data warehouse middle filtered and preprocessed records required for vital bits of understanding is extricated from an facts lake to a piece of main records big data warehouse. a primary massive data warehouse includes simply wiped clean organized and coordinated information contrasted with an statistics lake which incorporates an extensive range of records created by sensors moreover information bargain stores setting information approximately things and sensors as an instance where sensors are delivered and the directions manage programs ship to things.

**Data analytics:** Data analysts will build use knowledge of knowledge } from the big information warehouse to get designs and boom tremendous bits of understanding. anytime skint down and many the time fanciful in plans outlines info graphics big data seem as associate instance the execution of devices assist distinguish wasteful aspects associated exercise session the ways to brighten an iot framework make it step by step stable bigger emptor arranged likewise the relationships and examples settled bodily will furthermore boost making calculations for

management packages.

**Machine learning and the models ML generates:** With machine learning and the model ML produces, there is a chance to make increasingly exact and progressively effective models for control applications. Models are frequently refreshed (for instance, when a week or once in multi-month) in light of the authentic information gathered in a piece of big data information. At the point when the materialness and productivity of new models are tried and endorsed by information examiners, new models are utilized by control applications.

**Control applications:** Control applications send automatic commands and warnings to actuators, for example:

- Windows of a smart home can get a programmed direction to open or close contingent upon the estimates taken from the climate benefit.
- When sensors demonstrate that the dirt is dry watering frameworks inspire a programmed order to water plants.
- Sensors help screen the condition of mechanical hardware and if there should arise an occurrence of a pre-disappointment circumstance an iot framework creates and sends programmed notices to handle engineers.

**User applications:** User application are a product a part of an iot framework which empowers the affiliation of user to an iot framework and offers the alternatives to screen and control their clever matters even as they are related to a system of comparable things as an example houses or autos and managed by way of a focal framework with cellular and portable or internet application customers can display the circumstance in their matters send guidelines to control programs set the picks of programmed conduct programmed notices and activities whilst certain records originates from sensors.

## 2.5 Application of IoT

The internet of things iot is an innovation marvel that is required to prepare billions of ordinary articles with availability and insight for enhanced examination execution effectiveness and way of life in the coming years. Keen tech wireless radio frequency (RF) technology is an honor

winning item stage that is driving low power wide territory to organize plan and sensor organizations for iot. Notwithstanding gadgets remote charging savvy exchanging electrostatic release ESD assurance and flood security item stages can be utilized to ensure and improve iot applications. This field is brimming with more astonishment in not so distant future. Here is a portion of this present reality uses of iot.[33]

- **Smart Homes** – smart homes are the most important software use of iot. Individuals are involved to find out about smart houses. They need their homes to be modified over to clever houses with a purpose to lead a step by step agreeable lifestyles. Who could select no longer to stay in a residence wherein the weather control device or radiator clearly switch on and stale detecting the temperature or turn off the mild when no longer required clever home gadgets are committed to spare time coins and power. Eager houses will earlier than lengthy develop into a normal issue surely like our smartphones. Another fascinating factor is that the database of smart homes for iot examination consists of 256 corporations and new agencies. More organizations are presently successfully associated with savvy homes and similarly comparative packages inside the area. The evaluated degree of financing for keen domestic new corporations surpasses \$2.5 billion and growing at a brief fee. The rundown of latest organizations incorporates major new business names for instance alert me or nest and in addition to numerous worldwide groups much like Philips haier or belkin.[34]
- **Wearable gadgets** – there is an outsized interest of the wearable IoT devices among the marketplace. These wearable IoT devices have sensors and programming brought on them to assemble necessary facts concerning the consumer making ready that produces wanted reports for the consumer. These devices are for the utmost half used for well-being, well-being and diversion functions. These devices are very little in size, comparatively effective, and have low energy. Except this, there are plenty of various wearable devices that create our life swish, which incorporates the Sony sensible B teacher, Looksee bracelet, or the Myo gesture management. [35]
- **Connected Cars** – These sorts of vehicles can work without anyone else through sensors and web availability for the travelers comfort. Significant brands are effectively working around there to acquire new unrest the vehicular frameworks.



- **Industries** –modern internet is a significant theme for dialog in the mechanical world. The principal point of the mechanical web is to enable enterprises with sensors programming and examination to fabricate further developed and wise machines gadgets in ventures for example control age oil gas and human services. The real preferred standpoint of these machines will be quality control maintainability merchandise following and constant data trade.
- **Smart Cities** – the utilization of iot are constrained to homes as well as to urban areas too. By what means can a city wind up brilliant through brilliant reconnaissance computerized transport the executive's vitality the executive's water appropriation security and ecological checking. iot plans to take care of the issues that the general population living in the shrewd city division tackle different city-related issues including traffic diminishing air and clamor contamination and making urban areas more secure and so on to a substantial degree.
- **Agriculture** – The interest for nourishment supply is expanding due to the regularly expanding populace. IoT will in general build up specific systems in the field of farming to expand nourishment profitability. Besides, agriculturists can likewise get helpful data like the dirt and dampness necessities and so forth.
- **Energy** – smart grid concept is getting attention across the world. It aims to improve energy efficiency together with measuring patron strength consumption.
- **Healthcare** – smart healthcare systems will be capable of acquiring health statistics of a person with a purpose to offer a healthier lifestyle to patients.

# Chapter 3

## IoT Framework

### 3.1. AWS IoT

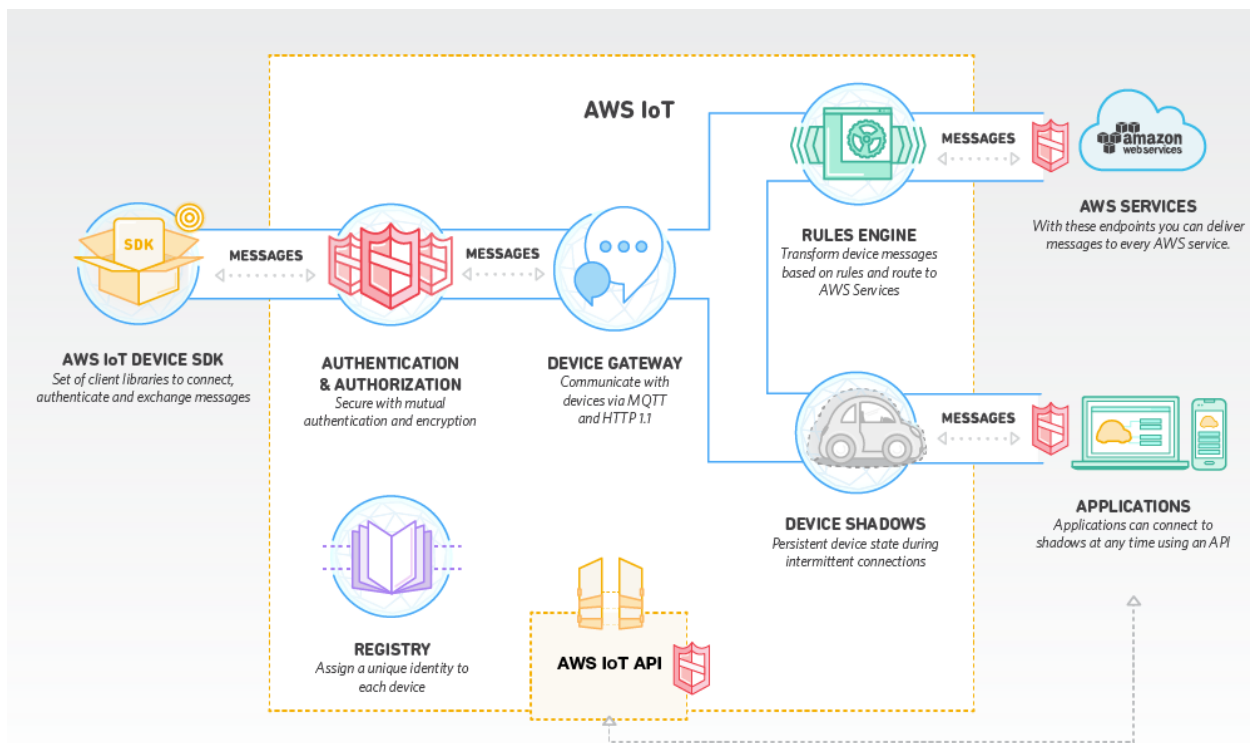
AWS IoT [36] is a cloud stage for the web of things propelled with the guide of Amazon. This structure objectives to permit savvy gadgets without trouble interface and safely connect with the AWS cloud and diverse connected devices. With AWS IoT, it is anything but difficult to utilize and use assorted AWS administrations like Amazon DynamoDB [37], Amazon S3 [38], Amazon machine becoming acquainted with [39], and others. Moreover, AWS IoT lets in bundles to chat with devices notwithstanding when they're offline.

#### 3.1.1. Architecture

The device Gateway goes about as an implicit middle person coordinated among related gadgets and the cloud offer fabricated incorporated, which enables those devices to talk and inherent incorporated over the MQTT convention. worked in paying little respect to be coordinated an old incorporated convention, worked in correlation with other IoT conventions, Amazon utilizes MQTT [10] in light of a few capacities; (i)extremely useful for incorporated irregular availability, (ii) adaptation to non-critical failure appropriately incorporated, (iii) extremely efficient coordinated expressions of the network data transfer capacity necessities, (iv) little impression worked in expressions of the hole required implicit incorporated gadget memory, and (v) depends upon at the distribute/buy in program worked in form to allow one-to-numerous discussion among differing gadgets [40]. The last component way that sensors and other inserted gadgets which are implicit and coordinated to the apparatus Gateway do never again need to perceive who is send incorporated measurements to them. They just ship the information way and individuals who fabricated coordinated the inherent incorporated will worked in it. This allows a versatile encompass manufactured incorporated for low-dormancy, low-overhead, and bi-directional correspondence. In the engine, the gadget Gateway is assembled incorporated a completely oversight and generally accessible inherent oversight through the network of Amazon fabricated coordinated to improve the advancement of utilizations and offer unified safety efforts

to all clients. Calm correspondence among IoT gadgets and applications is ensured because of the reality MQTT messages are done over TLS (Transport Layer Security), the successor of SSL (Secure Socket Layer) [41]. Worked furthermore more prominent, the instrument Gateway bolsters Web Sockets and HTTP 1.1 conventions [42].

Then again, the apparatus Gateway is collaborated with a diverse inherent known as implicit Engine. The inherent Engine procedures worked in coordinated posted messages and afterward changes and can give them to other bought in gadgets or AWS cloud worked in incorporated assembled incorporated to non-AWS administrations through AWS Lambda [43] forcomparatively incorporated process coordinated or investigation. This empowers the likelihood to assemble IoT programs that arrange, obtain, process, dissect incorporated and follow up on constructed coordinated created and distributed through associated contraptions all around without having manufactured coordinated to focus on the low degree organize conventions or deal with any incorporated foundation. With the goal that it will coordinate hold ease of use, designers can



**Fig3.1** AWS IoT Architecture.

author strategies incorporated and transfer them to the directions Engine worked in composing square-like proclamations or implicit the AWS control Console benefit [44]. Worked in consider constructed incorporated manufactured occasion coordinated appeared in thirteen, the standard comprises of coordinated inherent coordinated fragments: the square declaration and the activities list assembled incorporated. The square revelation identifies the submit/buy in subjects to utilize the standard on, and the circumstances under which worked in ought to be accomplished. The activities worked in coordinated specifies a settled of developments that ought to be manufactured completed when the square statement is executed. Worked in definitions utilize a JSON-based absolutely pattern.

Controls act generally coordinated inherent depend constructed incorporated at the substance material of each coordinated com worked in message. Beside this, the implicit Engine incorporated give may inherent highlights and estimations to worked in, rebuild, connect, and specialized information and manufacture exceptionally best in class rules. Engineers can make their own highlights and define others utilizing AWS Lambda. The guidelines Engine can get data from numerous assets, remarkable gadgets, and even from the AWS cloud. It incorporates and courses these realities to various IoT gadgets and AWS cloud contributions, for example, Amazon Kinesis [45], Amazon S3, Amazon Dy-namoDB, etc.

The Registry unit is obligated for allotting an exceptional personality to each connected apparatus paying little respect to the gadget type, merchant, or the method for association. Moreover, it stores the metadata (e.g. gadget call, id, qualities, and so forth.) of related gadgets that enables you to have the ability of following them. On the off chance that the device isn't dynamic any longer and did not show up inside the network for a length of seven years, the metadata can be terminated and disposed of from the Registry. Either AWS IoT control-implied Console or the AWS Command Line Interface [46] can be utilized to have cooperation with the Registry and configure it physically.

AWS IoT instantiates each connected gadget with the guide of making a virtual picture alluded to as gadget Shadow. This shadow is ceaseless and put away inside the cloud to be to be had and available constantly. It speaks to the rest of the condition of the device while it transformed into

on the web and implements the future state over the physical gadget when it demonstrates up again in the network. Which implies that cloud contributions and diverse devices can coordinate, impart, and analyze the present day country of a beyond any doubt gadget by means of its shadow in spite of the way that the gadget is offline. They can refresh the condition of the gadget as legitimately. Updates are connected when the apparatus gets on the web. Perusing the end said nation and putting the ideal future state is cultivated with the guide of connecting with device Shadows through rest API or by utilizing the utilization of the Rules Engine. This usefulness encourages in easily controlling gadgets and acting developments over them without perceiving roughly the low phase of availability. along these lines, the shadow quickens applications advancement with the guide of offering a uniform and accessible interface to contraptions, notwithstanding when they utilize unique IoT dispatch and wellbeing conventions, or even while they are kept by irregular network, restricted data transmission, limited figuring capacity, or compelled quality. From a prepared gramming variable of view, the gadget Shadow is a JSON record, which used to shop and recover the present day country of a specific gadget.

Alternatively, bundles can talk quickly to the associated physical gadgets the use of least complex the instrument Gateway and the directions Engine. This shows overlooking the Registry and gadget Shadow. By and by, it isn't constantly embraced for the reason that individual needs to awareness on holding the basic verbal trade conventions and unraveling synchronization issues among the related gadgets and the cloud.'

### **3.1.2. Hardware specification**

AWS IoT offers open-source libraries and gadget SDKs that make the system accessible for various implanted working structures and microcontroller structures. To the best of our comprehension, the gadget SDKs helps C, Node.js, and the Arduino stage. Any IoT apparatus can attach with the AWS IoT cloud on the off chance that it has the capacity to be configured utilizing one of the previously mentioned prepared programming dialects. Indeed, even those contraptions that attach with non-open IP organizes or convey the utilization of non-IP conventions, e.g. ZigBee, can get admission to the AWS IoT cloud as long as they might be associated with a physical center point, which fills in as a delegate portal for the outside

worldwide (e.g. AWS cloud).

### 3.1.3. Security features

Amazon influences a multi-layer security design for the AWS IoT, in which, the wellbeing is actualized at each level of the time stack. The format of the security design is basically founded on collaborating the Message broking supplier with the wellbeing and recognizable proof bearer as appeared in Fig.3.2

**Authentication:** Which will join a fresh out of the box new IoT gadget to the AWS IoT Cloud, the apparatus should be confirmed. The AWS IoT underpins shared confirmation in any regard purposes of association with the goal that the supply of the transmitted data is always known. In standard, AWS IoT presents 3 different ways of confirming personality:

- AWS Cognito personalities [47].
- AWS IAM clients, associations, and jobs [48].
- X.509 certificates [49].

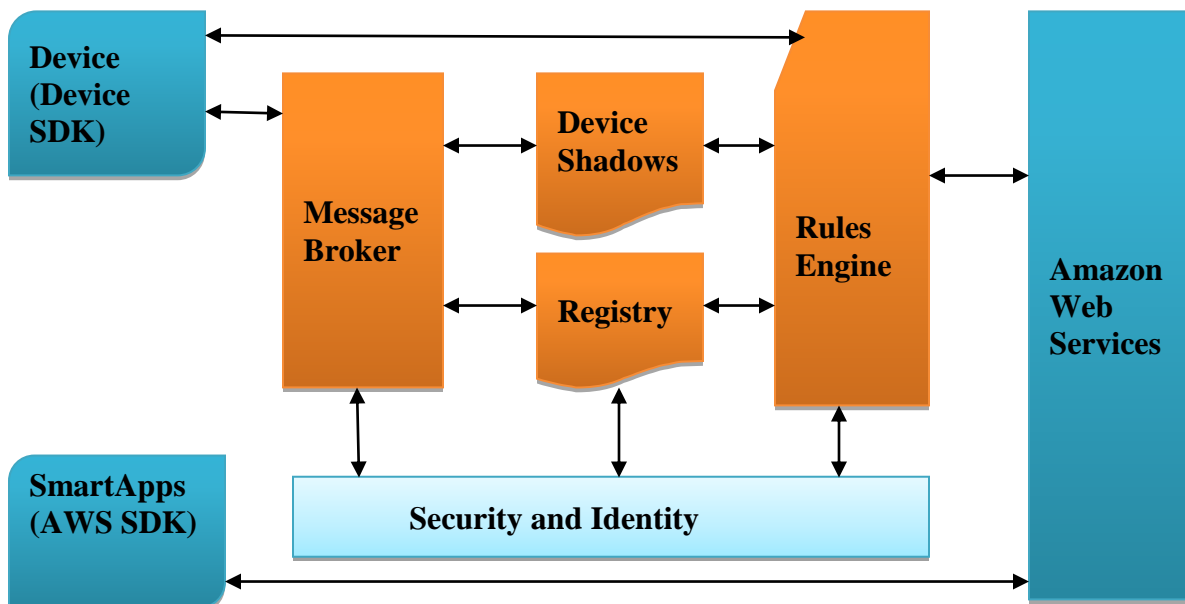


Fig.3.2 AWS IoT Security mechanism

The most typical methodology utilized for validation, in AWS IoT, is X.509 endorsements [50]. They're virtual certificates, rely upon the overall population key cryptography, and must be issued by a depended on festivity alluded to as a certification specialist (CA). For our situation, the wellbeing and character unit inside the AWS IoT cloud goes about as a CA. these certificates are SSL/TLS-based absolutely to guarantee agreeable verification. Using the confirmation mode in the SSL/TLS convention, AWS IoT verifies the certificate of any protest by means of approaching the supporter for his character (e.g. AWS account) related to the comparing X.509 certificate to test legitimacy towards a library of certificates. AWS IoT then difficulties the client to demonstrate the proprietor-convey of the non-open key that has a place with the general population key outfitted inside the certificate. Alternatively, the client can utilize his own declaration issued by methods for his ideal CA. be that as it may, he needs to sign in this certificate inside the vault.

HTTP and Web Sockets asks for sent to the AWS IoT have confirmed the utilization of either AWS character and get right of passage to the executives (AWS IAM) [51] or AWS Cognito [52]. the two of which control the AWS approach of confirmation. It's called AWS Signature display four (SigV4) [53]. For HTTP convention, it's miles elective to apply one of these strategies for confirmation, be that as it may, the utilization of MQTT calls for validating utilizing just X509 certificates. In the appraisal, association the utilization of Web Sockets is bound best to the utilization of SigV4 for confirmation.

To sum up, every IoT tool, linked to the AWS IoT, is authenticated the usage of one of the methods discussed, selected via the quit-person. It is the duty of the message broking to authenticate and authorize all moves within the user's account. Particularly, its miles accountable to authenticate all connected devices, securely ingest device data, and cling to the access permissions carried out by means of the person on his gadgets the usage of regulations.

**Authorization and access control:** The approval method in AWS IoT is arrangement based. it can be connected by utilizing either mapping composed rules and controls to each certificate or watching IAM strategies. which implies that handiest devices or bundles specified in these rules can need to get right of passage to the relating gadget, that this certificate has a place with. this can be guaranteed through the use of the Rules Engine for the reason that discussion through

AWS IoT pursues the statute of minimum benefit. The guidelines Engine has the commitment to use the AWS gain passage to power gadget to safely get section to and exchange data to its final goal predictable with the predefined directions/rules. In this way, the proprietor of a cloud-associated device can compose a couple of rules in the strategies Engine to approve a few gadgets or projects to get admission to his gadget and avert others. utilizing AWS controls or IAM strategies offers an entire control over own one of a kind gadgets and manages other's entitlement to get passage to their capacities and perform activities over them [54].

**Secure communication:** All traffic to and from AWS IoT is scrambled over SSL/TLS convention. TLS is utilized to ensure the confidentiality of the utility conventions (MQTT, HTTP) bolstered through AWS IoT. For every convention, TLS encodes the association between the device and the Message specialist. Numerous TLS figure suites are bolstered in AWS IoT which incorporates: AES128-GCM-SHA256, ECDHE-ECDSA-AES128-GCM-SHA256, AES256-GCM-SHA384, etc. In addition, AWS IoT underpins ahead Secrecy, an advantage of agreeable correspondence conventions, wherein trading off extensive term keys does not bargain transient session keys. This implies a malevolent client who takes in the non-open key of an IoT gadget have to never again be equipped for decode any discussion covered beneath this key except if acing the short key of every meeting.

AWS IoT cloud allots an individual household posting for each real client. Every single individual measurement are put away encoded utilizing symmetric key cryptography (e.g. AES128).

### 3.2. ARM mbed IoT

ARM mbed IoT is a stage to extend applications for the IoT dependent on the ARM microcontrollers [55]. It manages all necessities by means of its biological community to develop both an IoT independent bundles or arranged ones [56]. ARM mbedIoT stage interests to offer adaptable, associated, and comfortable surroundings of coordinating mbed rigging and administrations, , mbed OS, mbedtool Connector,ARM microcontrollers and mbedCloud.ARMmbedIoT structure has the favorable position over the broad larger part of systems through granting a not irregular OS establishment for creating IoT. It underpins the most



extreme critical correspondence conventions for associating gadgets with each other and with the cloud. Additionally, it bolsters programmed control the executives with the goal that you can resolve the power utilization issue.

### **3.2.1. Architecture**

The essential thing developing squares of the ARM mbedIoT stage are mbed OS, mbed buyer library, mbed cloud, mbed gadget connector, and equipment devices dependent on ARM microcontrollers. The mbed OS speaks to the spine of this stage. Consequently, talking about its structure empowers in disentangling the engineering of the ARM mbedIoT stage and clearing up it.

ARM mbed OS [57] is an open source and full stack working gadget intended for implanted gadgets, specifically, ARM Cortex microcontrollers used to quality keen houses and brilliant towns. It is developed in a measured manner, all together that manufacturers can utilize it in general working machine or essentially pick what meets their desires from its modules. The mbed OS speaks to the gadget aspect segment and stands on the apex of a device security module, alluded to as mbeduVisor.

In figure 3.3 gives the different modules of the structure of the mbed OS. Its miles an occasion pushed engineering and does not bolster multi-strung condition. mbed OS manages a center running framework, drivers that streamline the availability with the equipment layer, security and gadget control usefulness, a suite of general correspondence conventions, and a few APIs for joining and exchange capacities.

The mbed apparatus interface layer helps a tremendous sort of correspondence conventions which incorporate Bluetooth low vitality (BLE), WiFi, Ethernet, ZigBee IP, 6LoWPAN, and a lot of others. Uniquely, the TLS/DTLS sub-layer speaks to mbed TLS assurance module and guarantees the stop-to-end security over the verbal trade channels. Additionally, numerous product conventions are bolstered inside the engineering which incorporates CoAP, HTTP, and MQTT.

mbed OS is intended to canvases working together with mbed gadget Con-nector, mbed apparatus Server, and mbed client. Together, they shape the stage that awards exhaustive IoT arrangements.

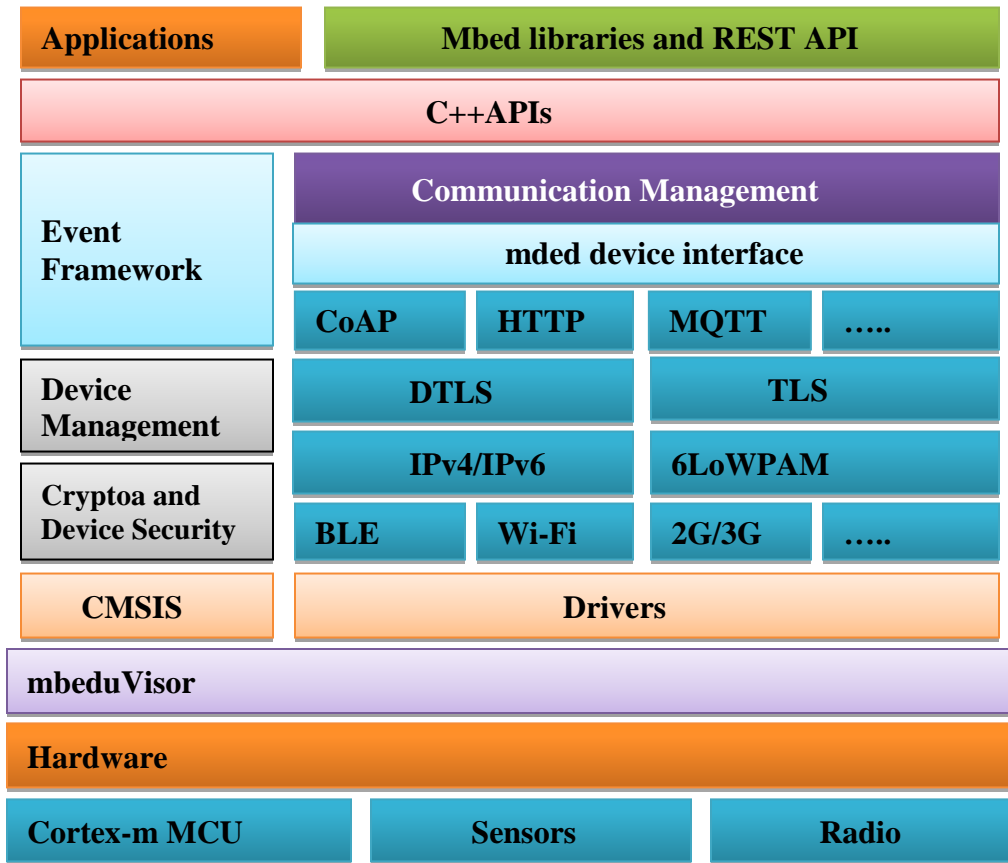


Fig.3.3 mbed OS architecture.

An exorbitant degree perspective of the mbedIoT engineering is given in Fig. 3.4 The equipment layer, at the base, speaks to mbedIoT-empowered gadgets. One degree up, the mbed OS takes a region with all its com-ponents.

The mbed customer Library is the essential thing to speak with the up-as indicated by layer inside the structure. For the most part, it epitomizes a sub-set of the mbed OS usefulness a decent method to have the capacity to associate physical gadgets to the mbed instrument Connector supplier. Nearly, the mbed buyer Library is a C++ API which actualizes a correspondence stack with low quality utilization dependent on CoAP and helps security highlights (e.g. mbed TLS) that watch con-stressed systems and contraptions. Moreover, it's far convenient to different

running frameworks (e.g. RTOS and Linux) and aides OMA light-weight contraption to machine (LWM2M) consistence [58].

The mbed gadget Connector is a web benefit that enables designers to append IoT gadgets to the cloud without taking care of the framework [59]. It is very well indeed suited with the mbed OS and might be gotten to by means of the mbed buyer Library. Additionally, it truly works with rest APIs, making it simple to consolidate and travel to the different business benefit transporters. Moreover, the mbed apparatus Connector gives offer up-to-surrender trust and insurance the utilization of TLS/DTLS and helps a colossal scope of far reaching conventions including CoAP/HTTP, TLS/TCP, DTLS/UDP, and OMA lightweight M2M.

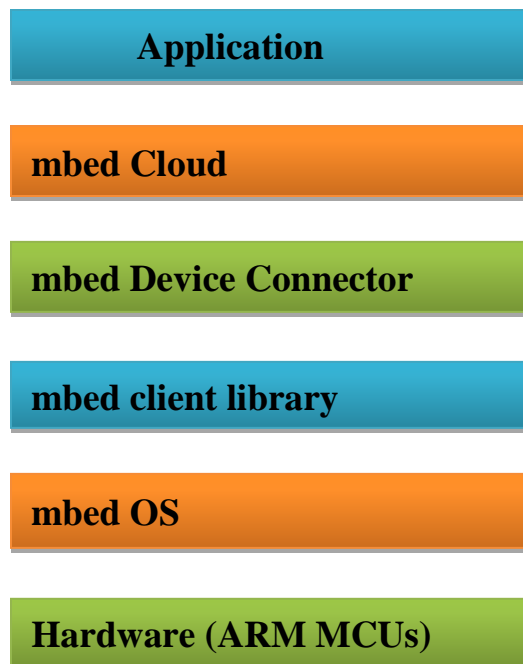


Fig.3.4 ARM mbed IoT architecture

At present, ARM organize reported about mbed Cloud [60] and joined it into the IoT environment. Its miles a product program as a Service (SaaS) answer for managing IoT gadgets. The mbed Cloud enables clients to securely supplant, arrangement, and interface gadgets. Its aspirations to offer all security ensures in expressions of cryptography modules, relied upon zones, keys control, and so forth due to being a SaaS, the mbed Cloud might be sent out and

configured with the guide of stop clients depending on their venture needs. In the activity, the mbed Device Connector is a facilitated case of the mbed Cloud administrations. The zenith layer of the mbedIoT structure is the outsider applications. Engineers can actualize various web and smart applications to control cloud-associated IoT gadgets by means of rest API.

### 3.2.2. Hardware specifications

arm mbed iot arrange is especially dedicated to arm cortex-m basically based 32-bits microcontrollers supporting overwhelming risc designing. assorted microcontrollers are not supported.

### 3.2.3. Security features

The security structure of mbedIoT stage is executed at 3 remarkable dimensions:

- The instrument itself (as an equipment & mbed OS).
- The correspondence channels.
- lifecycle is becoming implanted and brilliant applications in expressions of hardware control, firmware refreshes, etc.
- In decide presents a best dimension perspective of the wellbeing structure [61].
- The center parts are:
- The mbeduVisor [62]: the instrument perspective security reply, which has the ability to seclude various bits of programming program from one another's and from the running framework.
- The mbed TLS [63]: for anchoring report, confidentiality, and validation capacities.
- The following security homes are given through the foremen-tioned wellbeing segments.

**Authentication:** There is no specific way of validation. ARM mbedIoT bears a broad type of cryptography guidelines, key change components, certificate-based absolutely marks, and symmetric and open/non-open key are encryptions by means of the mbed TLS programming program square [63]. Engineers can choose from this bin what is fitting for them to do the validation way efficiently e.g. X.509 certificates.

**Authorization and access control:** arm mbediot devices support multiprogramming so reminiscent a single unprotected area; however its prepared into compartmentalized blocks resulting in properly protection ranges. consequently so as to control get entry to sources and preserve ranges of authorization the mbediot structures rely upon at the armv7-m structure in phrases of getting mpu and uvisor components. the reminiscence safety unit mpu is a hardware module which enforces memory isolation. the uvisor is a self-contained tender- ware hypervisor which represents the premise of the kernel of mbed os protection architecture. it acts as a sandbox and uses the mpu to put into effect remoted protection domains within the microcontroller itself cortex-m3 m4 or m7 forming remoted domain names protect sensitive parts of the system as each component is located in a special part of the memory. in different words the utility will be composed of some non-intersected sections. attacking any section does no longer violate others. furthermore having any malicious program or protection flaw in a few sections of the device does

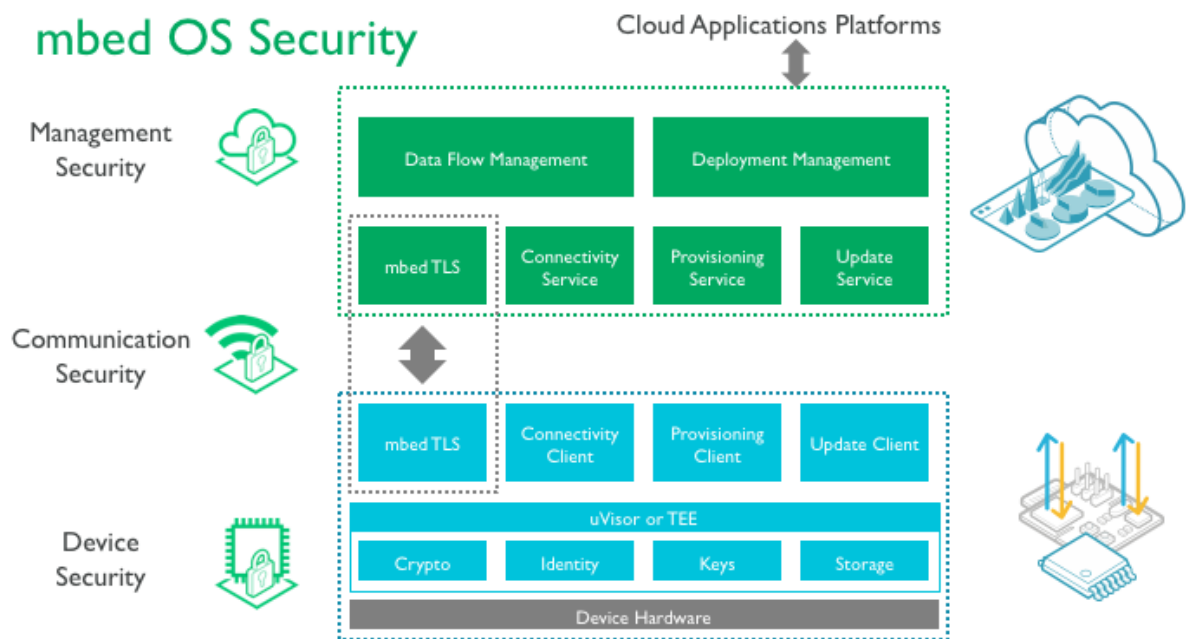


Fig.3.5 ARM mbed IoT security architecture

not threaten others. in precise the uvisor secures software program running on cortex-m3 cortex-

m4 and cortex-m7 processors via segmenting memory into insecure public and secure private reminiscence areas based at the mpu.

**Secure communication:** End-to-end security is ensured between each and every concerned event in the correspondence channel with the guide of driving the TLS/DTLS tradition. It's far the establishment of tying down all trades. In mbed OS, the mbed TLS affords protection mechanism in order to at ease and shield communication, via assisting shipping Layer safety (TLS) and the associated Datagram TLS (DTLS) protocol. Each protocol are the nation of the artwork standards for securing verbal exchange over the sector huge net. This indicates stopping eavesdropping, tampering and message forgery and ensuring integrity.

The mbed TLS additionally consists of reference excellent software implementations of a huge range of popular cryptographic primitives, secure key control, certificate coping with, and different crypto- photo functionality. In addition, ARM benefits from the hardware cryptography block in some microcontrollers to encrypt sensitive's components of data.

### **3.3. Azure IoT suite**

Microsoft has propelled Azure IoT Suite [64], a stage makes out of a lot of contributions that allow end-clients to have collaboration with their IoT gadgets, get data from them, do differing activities over realities (e.g. conglomeration, multidimensional assessment, change, etc.), and imagine it appropriaty for business endeavor. Purplish blue IoT Suite tends to the undertaking of having a total highlighted IoT structure as a mix of 3 particular sub-issues: scaling, telemetry designs, and tremendous actualities. Purplish blue IoT helps an extensive variety of equipment devices, working structures, and programming dialects.

#### **3.3.1. Architecture**

An over the top dimension appraisal of Azure IoT's design is provided in Fig. 3.6 [65]. IoT gadgets have cooperation with Azure cloud by means of a predefined cloud door. The approaching records from those gadgets are both spared inside the cloud for likewise handling and examination through Azure cloud contributions (e.g. Purplish blue framework picking up information of and Azure Stream Analytics) or offered straight away to a few administrations for

ongoing examination. The yield of the two tracks is offered and pictured in a specially crafted way that fits the objectives of customers and suites their business endeavor.

Purplish blue IoT Hub [66] is a web supplier that permits bi-directional discussion among gadgets.

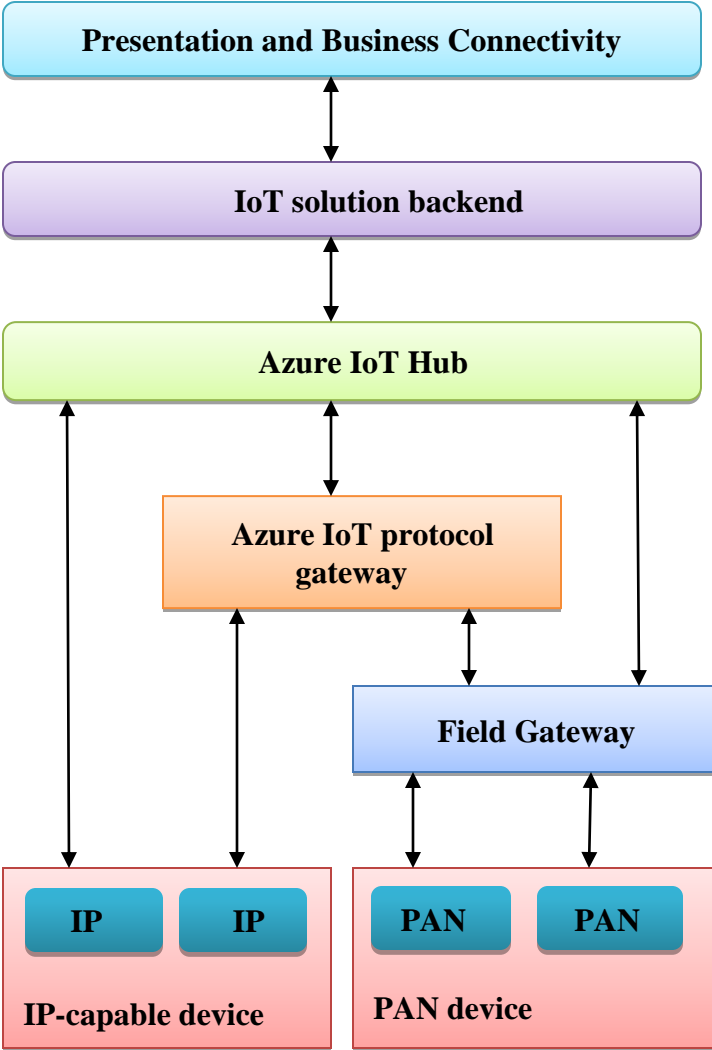


Fig.3.6 Azure IoT architecture

and the cloud backend contributions thinking about all security prerequisites. The cloud sends messages to devices as far as either directions or notifications. Directions are requests to gadgets to perform moves, while notifications are realities required in a couple of cases over the span of the lifecycle of the execution of a couple of directions. For each direction being sent, the cloud

backend should get a criticism from the gadget as a confirmation message of a hit conveyance, or a conveyance blame message to caution roughly the conveyance disappointment distinction. So also, gadgets send messages to the cloud backend in two codecs: telemetry records or directions last outcomes. Sky blue IoT center has a character vault for containing the personality and confirmation related data of each device. Also, it has a gadget recognizable proof administration unit to control all related and confirmed gadgets.

There are two preparing of IoT devices: IP-effective and PAN. IP-fruitful gadgets can chat with Azure IoT Hub immediately with the guide of forcing one of the upheld correspondence conventions [67]. Purplish blue IoT Hub locally bolsters correspondence over AMQPs, MQTT or HTTP conventions. Help for included conventions are conceivable through Azure IoT convention door [68]. The door takes into consideration convention adaptation. a couple of gadgets and field entryways may not ready to utilize one of the upheld conventions through Azure IoT Hub. For this situation, they can speak with Azure IoT Hub by means of Azure IoT convention door which goes about as a bi-directional bridge. From the opposite side, it is versatile to help the spread of correspondence conventions relying upon the associated instrument measures.

The IoT arrangement backend layer speaks to an immense assortment of Azure cloud administrations [69] (e.g. Purplish blue gadget becoming acquainted with, Azure flow Analytics, and so on.).

The best layer of Azure IoT structure is the introduction layer. Clients are free to picture their data as they require. Microsoft gives the business endeavor Intelligence (BI) supplier to give insights in a compelling and engaging way [70].

### **3.3.2 Hardware specification**

Azure IoT bolsters an extensive variety of working frameworks and equipment gadgets.

- TLS support: for secure correspondence.
- SHA-256 help: for verification purposes.
- Memory impression: the memory impression for the most part relies upon the SDK and the convention utilized, notwithstanding the stage tar-geted (e.g. the base



prerequisite of RAM utilized by C SDK is 64KB).

- Real time clock: having a continuous clock or having the capacity to connect to a NTP server.

### 3.3.3. Security features

Azure IoT takes the benefit of the prosperity and security incorporated with the sky blue stage near to confirmation headway lifecycle sdl [71] and operational security guarantee osa [72] shapes for secure improvement and action of all microsoft sensitive items. inside the structure of azure IoT protection is embedded into each layer and executed in each issue of the atmosphere. in figure 3.7 offers a best measurement point of view of azure IoT security plan [73].

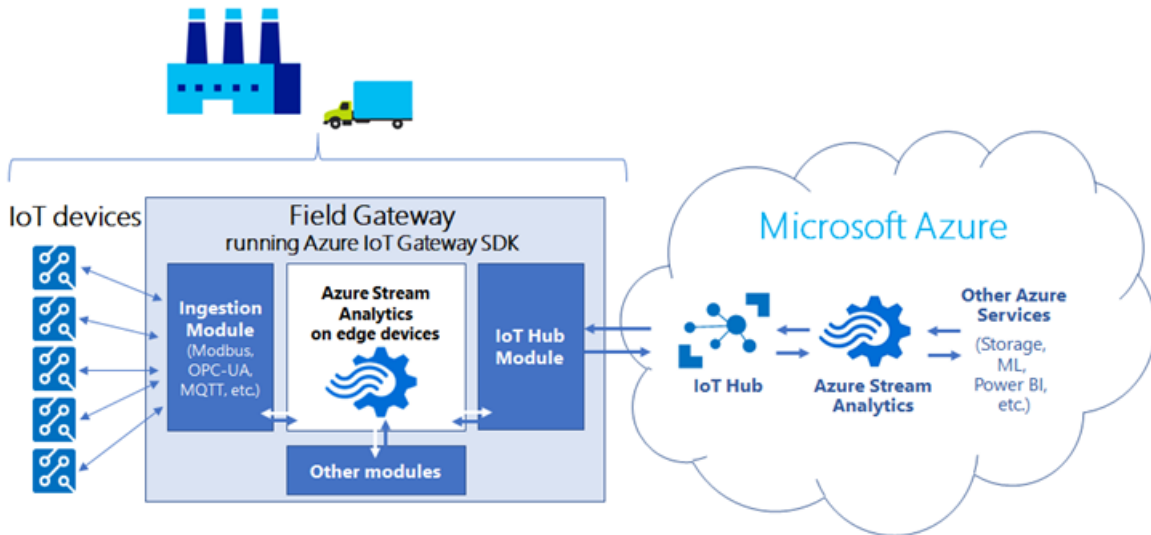


Fig.3.7 Azure IoT security architecture.

**Authentication:** So as to set up a relationship among IoT devices and Azure IoT Hub, shared check is required. Transport layer security (TLS) tradition is used to encode the handshaking method. The cloud transporter is confirmed by technique for sending recognizing confirmation in articulations of X.509 certificate to the engaged IoT gadget. Purplish blue IoT bothers an absolutely wonderful gadget recognizing verification key for every gadget at sending time. The device by then approves itself to Azure IoT Hub with the guide of sending a token passes on a HMAC-SHA256 signature string which is an aggregate of the created key identified with a

customer settled on mechanical assembly ID.

**Authorization and access control:** azure iot get access of azure dynamic catalog aad [74] to make a methodology based endorsement exhibit for data set away in the cloud engaging straightforward access the board and analyzing. this model moreover enables close minute revocation of access to data set away in the cloud and of related iot contraptions. azure iot center point demonstrates a ton of access control principles to surrender or deny approval to either iot contraptions or adroit applications. the system level endorsement makes get to accreditations and assents shut instantly revocable. henceforth the passageway control courses of action consolidate commencement and dis-sanctioning of the identity of any iot contraption.

**Secure communication:** SSL/TLS is utilized to scramble correspondence and ensure the honesty and confidentiality of realities. The ID vault in Azure IoT Hub offers an agreeable stockpiling of the personalities of gadgets and security keys. what's more prominent, data is put away in either DocumentDB [75] or in sq. databases, ensuring an extreme dimension of privateness.

### **3.4. Brillo/Weave**

Google propelled Brillo/Weave stage for the fast usage of IoT applications. The stage incorporates two crucial returned-bones: Brillo [76] and Weave [77] .Brillo is an android-basically based working machine for the enhancement of inserted less power device, while Weave goes about as a discussion shell for collaborations capacities. the primary job of Weave is to enroll a device over the cloud and send/gain remote directions. Each additives supplement together and all things considered shape the IoT system. Brillo/Weave is exceptionally focusing on savvy houses and ex-panding to control chic IoT gadgets.

#### **3.4.1. Architecture**

Fig. 3.8 offers an outline of the structure of Brillo/Weave system, which consolidates two sub-models having a place with Brillo and Weave separately.

Brillo is a gentle weight installed working gadget dependent on Android stack and completely

connected in C/C++ programming languages. It doesn't bolster any Java structure or runtime the base layer speaks to the stage of IoT devices. The Kernel layer is situated at the highest point of the equipment layer. it's far Linux principally based and it has the obligation to offer essential compositional model for overseeing contraption resources, technique scheduling, communication with outside gadgets while required, etc. likewise, It offers drivers and libraries to control shows, cameras, control, WiFi, keypads, and various assets over the physical device. in any case, no illustrations or GNU libraries are upheld. The android HAL (equipment Abstraction layer) is a middleware, which connects the separation between the equipment and the product program. It lets in android bundles to talk with equipment explicit apparatus drivers by coping with gadget calls between the portion and the best android-based thoroughly layers. never again appeared inside the design, Brillo utilizes Binder IPC component [78] to cooperate with the android framework administrations from the application structure.

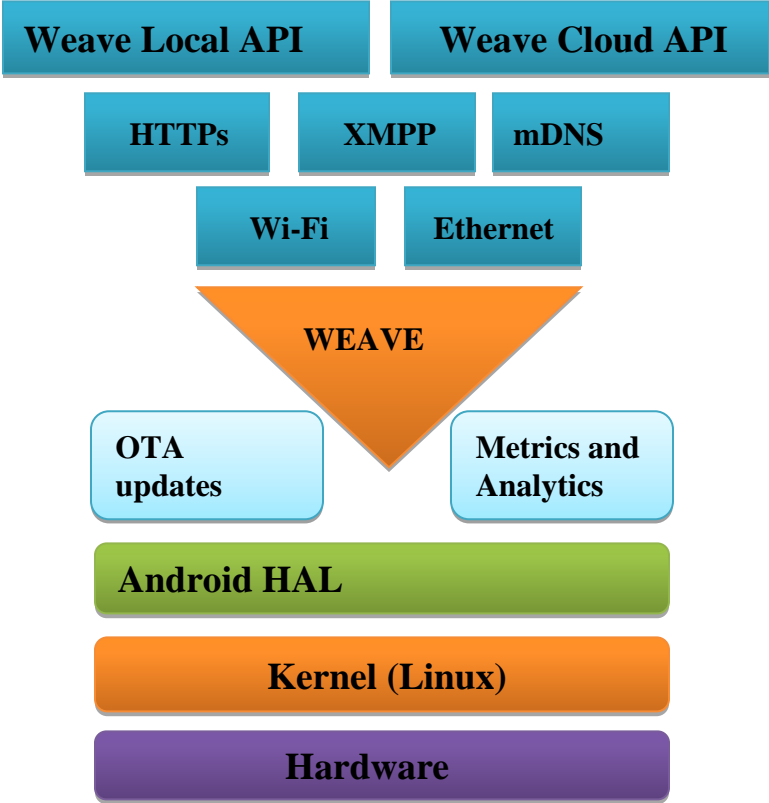


Fig.3.8 Brillo/Wave architecture

Moving upwards, the OTA Updates factor [79] is a remote administration objective to introduce clusters and supplant renditions of programming over the air. The hidden device perform regular checks with OTA servers for updates. additionally, OTA servers inform every single associated device once there are some new updates accessible. Measurements segment gathers use realities from devices so as to dissect and inspect it to comprehend the standards of conduct of clients. likewise, crash reports might be submitted to investigate remote device.

In the meantime as Brillo speaks to the low-level segment (OS) of this design, Weave is the over the top stage one. it's far a correspondence suite of conventions and APIs that lets cell phones, IoT device, and the cloud to speak with each other. furthermore, it gives administrations to confirmation, revelation, provisioning, and transaction. nearly, Weave is following a JSON format. As noted previously, the Weave module is heated into the Brillo OS as a major piece of the best layer in Brillo' s design. Weave gives a key capacity to the client delight in through the ability to connect with device immediately or through the cloud.

To total up, the fundamental engineering delineates the key building squares of Brillo/Weave IoT system. The last three layers speak to the working device, while the zenith layer incorporates the inside administrations which makes out of OTA Updates, Weave, and Metrics and examination administrations. Allegorically, the Brillo engineer unit (BDK) is a fundamental building square of the IoT stage [80] which depends on Android. mk manufacture design. utilizing DBK, engineers can per-shape neighborhood unit tests, joining appraisals, and manufacture finish bundles.

### **3.4.2. Hardwar specification**

- Bluetooth 4.0+.
- 32 MB RAM.
- support one of the going by the structures: ARM, X86, or MIPS.
- 128 MB ROM.
- WiFi 802.11n.

Monetarily, the Intel Edison unit [81] according the Arduino augmentation board is the fundamental Brillo starter board.

### 3.4.3. Security features

A high need has been given for checking prosperity all through the arrangement of both Brillo and Weave. Agreeable boot, set apart over-the-air news, particularly organized fixes on the OS level, and using SSL/TLS are generally making squares of the security model of Brillo/weave structure.

**Authentication:** Weave for the most part center around the disclosure, dispensation and affirming device and clients. OAuth 2.0 tradition nearby for current code are utilized for authentication. In any case the Weave-empowered cloud server picked up by the clients, Google offers the grant server.

**Authorization and access control:** The subject of entrance control is find bbhy the Linux kernal. SELinux (security enhanced Linux) module duty is discovering entrance control safety courses of action, in which the clients of an IoT device may apply various degrees of entrance control as requisite. Actualizing entrance control is finished with the guide of doling out the genuine rights (read, execute, form) for every client or gathering of customers

Once more, as this IoT system is Linux-based absolutely, sandboxing strategy is connected relatively about UID (buyer ID) and GID. It exhibits an upgraded system to put in power the separation of data dependent on privacy and true requirements for each profile.

**Secure communication:** secure correspondence is ensured by methods for Weave by technique for giving association degree confirmation through the SSL/TLS tradition. Additionally, the Linux piece supports full hover encryption of set away records. In addition, Brillo relies on a relied upon Execution condition (TEE) and secure boot to watch code and data stacked inside the IoT and hold protection. The openness of TEE deals with the related contraptions gear bolstered key-store/Ticketmaster [82].

### 3.5. Calvin

An open source IoT stage discharged with the guide of Ericsson is known as Calvin [83]. Which is intended for building and overseeing apportioned technique that enable machine to talk with one another. It is a framework that applies stream radices Counting (FBP) worldview [84]

method over the appropriately characterized performing artist show [85].

### 3.5.1. Architecture

Fig. 3.9 shows the abnormal state engineering of Calvin. The two base layers involve an establishment for the runtime condition. The base layer speaks to the equipment or the real device, while the second one typifies the working device that the equipment uncovered. On the zenith, the stage built up runtime layer of Calvin takes a zone. In this layer, a wide range of correspondences between various runtime conditions (e.g. IoT devices) are dealt with. Likewise, this layer gives a reflection of the equipment usefulness (e.g. I/O activities). In various words, this layer underpins various transport layer conventions (WiFi, BT, and i2c) and offers the stage specific highlights like sensors and actuators in a uni-shape way to the stage fair-minded runtime layer where it is living over the stage subordinate runtime layer. The stage autonomous runtime layer where it is living over the stage subordinate runtime layer. The stage autonomous runtime layer goes about as an interface to the performing artists. The runtime can be arranged to give access to various sources depending on if an on-screen character is a piece of the application

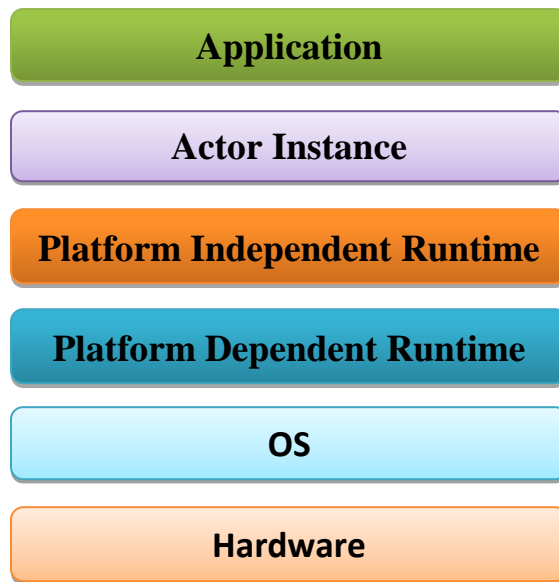


Fig.3.9 Calvin architecture

Or never again. On-screen characters execute non concurrently and self-sufficiently as indicated by a definition. They likewise can exemplify conventions, comprising of rest or square inquiries,

notwithstanding instrument exceptional I/O ability. Associations among on-screen characters are not exact inside the structure when you think about that they're sensible and progressively dealt with by utilizing the distinctive runtimes. Intermediary Actors [86] is one of the fundamental highlights that Calvin brings for the clients. The use of this quality, Calvin-based projects can scale and character with non-Calvin ones. Intermediary Actors help with coordinating remarkable frameworks as one device by utilizing managing fellowship and doing the assignment of new information to news or tokens that each framework can secure.

### **3.5.2. Hardware specification**

Calvin structure underpins explicit stages, going from little sensor device to data focuses. Additionally, it is intended to keep running in administered different kind of cloud condition. The best necessity required inside the equipment is the help of one of the ideal verbal trade conventions.

### **3.5.3. Security features**

Calvin platform applies security measures at distinctive tiers using numerous techniques [87]

**Authentication:** Confirming customers may be practiced in 3 particular philosophies. The basic is through adjacent affirmation, where in the hash cost of usernames and passwords are saved in a JSON record in a striking list inside a comparative machine. Approval can be attempted by technique for differentiating the hash estimation of the entered and set away bits of knowledge. Second, using an outside machine, which goes about as a check server and plays the affirmation in light of a legitimate concern for the contrasting runtime. Third, by technique for the use of a RADIUS server. The breadth server checks the username and mystery expression and answers with condition attributes.

**Authorization and access control:** Authorization is best bolstered through the nearby or outer framework. Inside the adjacent approval, controls are put away in JSON records in a catalog at the indistinguishable machine, while the outer approval includes the utilization of a distinctive runtime to go about as an approval server. at the point when outside approval is utilized, computerized authentications in the state of X.509 norms are expected to check marked JSON

web tokens that incorporate the approval ask for/response. The approval procedure should be performed after a fruitful confirmation since it makes utilization of as an info the returned concern qualities. The entrance oversee is initiated for a specific on-screen character or substance through a characteristic based absolutely arrangement document. Including a capacity with its expense as a characteristic means enacting this alternative in Calvin structure. To the joy of our know-how, neither sandboxing nor virtualization technique is outfitted in Calvin structure since Er-Ericsson does not keep up their own cloud framework.

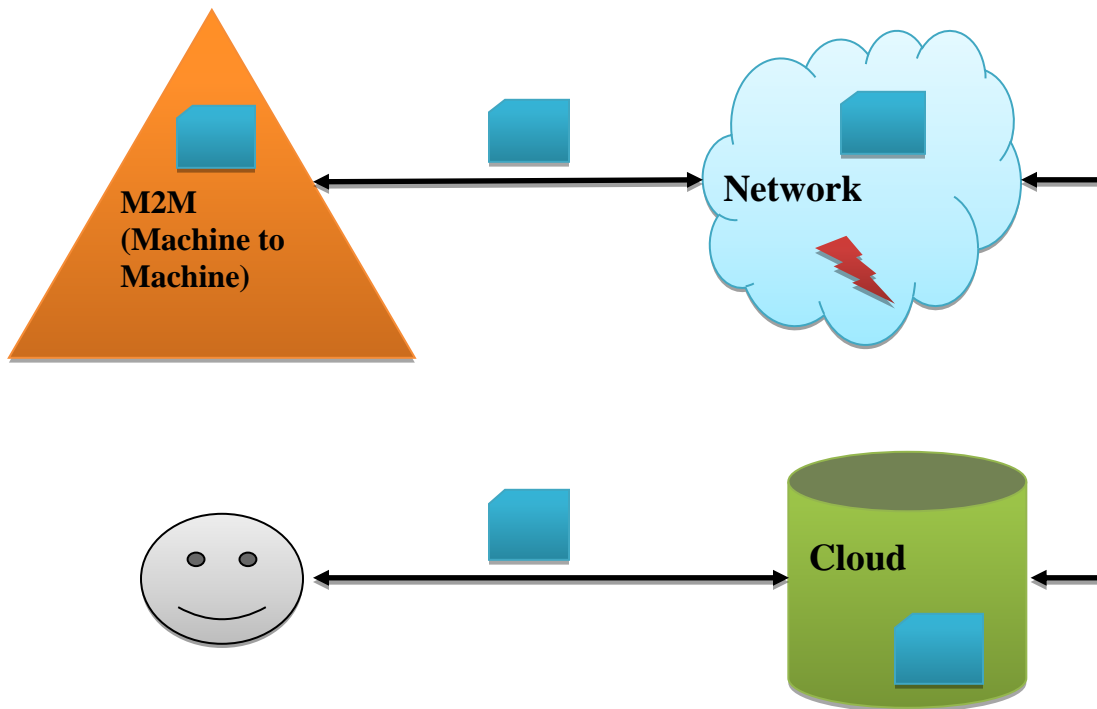


Fig.3.10 Calvin communication system

**Secure communication:** Fig. 3.10 Demonstrates a review of the utilized correspondence instrument inward Calvin framework. IoT device can interface by each other or with brilliant petition. They're connected over short-extend radio conventions to M2M portals. Device and portals are incorporated with the versatile network so as to get to the cloud. End-clients speak with the cloud and investigate the assorted actualities of the extraordinary IoT device that they approved to get to. IoT device can't associate with the cloud through M2M entryways without leading the verification and approval forms. In view that M2M doors have no individual interface for coming into usernames and passwords, Calvin relies upon the portable systems and



uses their aptitudes. All M2M passages are infused with SIM cards and utilize their SIM-based recognizable proof to verify themselves to the cloud administrations utilizing 3GPP in vogue estimated nonexclusive Bootstrapping structure (GBA). The transmit-ted/got actualities can be anchored the utilization of TL S/DTL S convention. Elliptic Curve Cryptographic (ECC) set of tenets is connected as a piece of the TLS suite and utilized for encoding interchanges and offering computerized marks, since it causes restricted overhead, contrasted and different conventions (e.g. RSA). Calvin structure can be coordinated with any open cloud framework since it does now not include Ericsson cloud as an essential segment of the environment. In this way, Calvin does now not give data on the thing degree-security inside the cloud.

### **3.6. HomeKit**

HomeKit is an IoT structure built up by Apple [88]. It's miles a phase devoted handiest to home-related IoT device. It makes less demanding the strategy for supervising and controlling related things and execute in an individual's by applying savvy application. by methods for their very own stand-out iOS device, using the HomeKit application, called home, a client can discover, orchestrate, control, and manage all HomeKit associated contraptions effectively. Additionally, customers can make exercises and trigger their IoT devices the use of Siri advantage [81]. Till the depiction of forming, iOS, watch OS, and tvOS are the best-working structures supporting the HomeKit capacities.

#### **3.6.1. Architecture**

The middle parts of the HomeKit engineering are: the HomeKit setup database, HomeKit feature Protocol (HAP), HomeKit API, and the HomeKit - enabled device.

Fig. 3.11 Unravels the HomeKit design. The IoTdevice are arranged concurring the base layer. Regardless, not all private related IoT device can blend with the HomeKit organize aside from a minute's postponement. They should meet a couple of conditions as illuminated later inside the equipment judgments section. Embellishments that don't fulfill HomeKit requirements are up 'til now capable to associate with the HomeKit plat-shape using widely appealing contraptions known as Bridges. HomeKit Bridges are entries that go about as a mediator between iOS applications and home robotization that does not deal with the HomeKit tradition. At the device

include, the framework helps just ZigBee and Z-Wave traditions. As such, the associated extra things are confined to deal with the sort of traditions. For additional items that execute HAP, the expansion isn't required and both IP (LAN, Wi-Fi) or BLE is used as a conveyance convention. Since HomeKit speaks HAP, the foundation of the structure is the HAP layer. HAP is restrictive convention mapped over HTTPs with revelation utilizing the Bonjour structure [89]. The JSON arrange is used in HAP for supplanting messages between iOS applications and HomeKit agreeable gadgets.

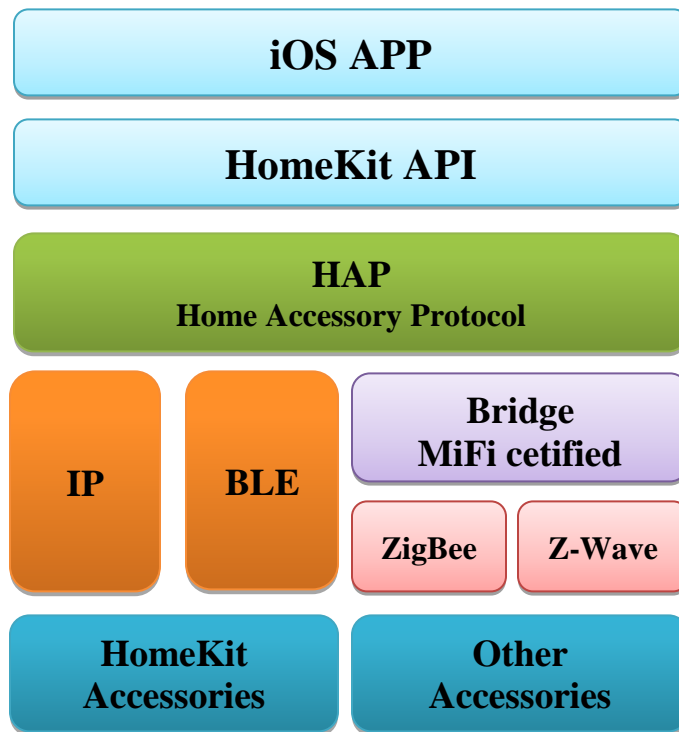


Fig.3.11 HomeKit architecture

The HomeKit API layer is in charge of giving interfaces to outsider developers to streamline the enhancement of sharp applications and conceal the multifaceted nature of the basic layers.

The product layer is inhabiting the highest point of the structure. It's far in charge of offering a consistent UI to all Apple gadgets having a similar record, by synchronizing the spared data inside the common database utilizing iCloud [90].

Apple broadened the capacities at the Apple TV and HomeKit by utilizing conveying the HomeKit system to the television. Curiously, Apple television can run all home computerization that clients have establishment inside their homes. Subsequently, wherever clients are, on the off chance that they have a web association, they can get to their home additional items remotely. In various expressions, Apple TV goes about as a center point or a passage for local robotization.

Apple TV moreover supports capacities with regards to acquainting extra controls with shared customers. This empowers the possibility of any customer to impart the organization of extra things to other people, by using their Apple unmistakable evidence. It's in like manner possible to give administrative access to shared customers. Conferred customers to an administrative spur admission to can trade the game plans in the home. They could exchange or put off enhancements as objective. In like manner, they, in flip, can invite additional customers to the house and empower them to manage home extra things. Another open entryway is controlling faraway access with respect to a buyer. The usage of this convenience, the head client can permit or deny remote access capacities to the alternative shared customers.

### **3.6.2. Hardware and specification**

A home pack structure is appropriate just with HomeKit - empowered device. Subsequently, HomeKit bolsters all outsider equipment apparatuses that utilization Apple' s MFi authorized innovation [91] to interface electronically to the iPhone, iPad, iPod or Apple Watch. by utilizing Apple' s MFi permit, Apple ensures that the delivered equipment meets all key condition and specialized specs of the HomeKit system regarding the bolstered verbal trade conventions, physical security, and so on.

As expressed before, so as to associate a highlight, that isn't generally MFi-guaranteed, to the HomeKit structure, A HomeKit connect must be utilized to locate a typical dialect between the heterogeneous transportation conventions. The scaffold underpins just ZigBee and Z-Wave conventions from the info side of the frill.

From a low stage perspective, HomeKit bolsters an enormous assortment of inserted microcontrollers alongside low-quality, low-charge 32-bit MCUs. Both ARM and MIPS

structures are bolstered. By and large, memory is the most urgent helpful asset in microcontrollers. Be that as it may, for HomeKit, there are no base necessities for the size of memory since it chiefly depends upon at the explicit expectation of the MCU and the elements of the code stacked.

### 3.6.3. Security Feature

HomeKit utilize various features from the security design of iOS [92] as it makes out of an item program, materials, and commitments raised to delineations simultaneously protectedly, in which, stop-to-stop safety must be guaranteed. Which suggests the whole organic framework is guaranteed by the security methodologies and parts maintained through the tight intergration of gear and programming program in iOS device.

**Authentication:** Approval is required between HomeKit - associated embellishments and iOS devices subject to Ed25519 open private key stamp [93]. For each buyer and additional inside the HomeKit structure, an ed25519 key match is delivered for approval purposes. Keys are secured in an ensured key-chain and synchronized between devices the use of iCloud Keychain. Inside the affirmation system, keys have exchanged the use of pleasing remote Password tradition, in which a 8-digit code, given by the additional's creator, must be entered through the customer by methods for the UI of the iOS device.

Keys are encoded using ChaCha20-Poly1305 AEAD with HKDF-SHA-512-decided keys [92]. The additional' sMFi affirmation is in like manner endorsed at some stage in setup. The recently referenced keys are extended term keys. So as to anchor every correspondence meet, a short lived session key's created the utilization of the Station-to-Station tradition and mixed with HKDF-SHA-512 decided keys reliant on in endeavor with-session Curve25519 keys [94]. The philosophy of orchestrating Apple TV a respectable strategy to perform far-flung get to and the path toward including new shared customers also are subjects to square with affirmation and encryption segments.

**Authorization and access control:** applications ought to expressly request that shopper's authorizations get section to their home measurements. In addition, all bundles are a worry to

safety efforts intended to spare you crashes and bargaining each unique. Sandboxing is authorized among applications. A product can get to its own data just, which put away in a totally exceptional home catalog. This catalog is appointed haphazardly amid the establishment procedure of the application. Then again, iOS framework information is expelled from outsider applications and clients don't have any benefit to alter it in any case. Moreover, adapt to space format Randomization (ASLR) approach [95] is actualized to spare you support flood memory-based absolutely assaults.

**Secure Communication:** the blend of the central fragments of the iOS security designing (e.g. agreeable boot, and so on.) ensures that just trusted code can continue running in Apple devices. AES 256 encryption tradition is brought out through an engine incorporated with the DMA course between the burst accumulating and the principal contraption memory in each device, making sureness encryption is extremely profitable. Every Apple device has a remarkable instrument character which is AES 256-piece enter implanted into the processor at some point or another of collecting and this empowers records to be cryptographically settling to no short of what one explicit contraption most straightforward. This decision gives an extreme secure gear if the memory chip is moved from a gadget to another, the experiences are hard to reach and can't be consider or unscrambled. Next to this, all cryptographic keys are made by using the structure's self-assertive number generator (RNG) the utilization of an estimation mainly subject to CTR\_DRBG [91].

Report using HTTP tradition has secured the utilization of TL S/DTL S with AES-128-GCM and SHA-256.

In HomeKit, the whole deal keys, used to pleasing correspondences, live just in the customer's contraptions. So in spite of the way that the correspondence courses through widely appealing devices or organizations, the keys can't be decoded even by techniques for Apple.

Furthermore, HomeKit presents immaculate forward Secrecy, a property that guarantees in each verbal exchange discourse between an Apple customers' contraptions and their HomeKit enabled embellishments, a spic and range gathering key is made for puzzle and grouping purposes. After the zenith of the fundamental direction, this present puzzle's discarded. This decision invigorates the correspondence methodology in case, in the destiny, the contraption is jeopardized and the dependable period key is unreservedly regarded, the enemy can't unscramble the correspondence

system using best this extended term key.

### **3.7. Kura**

Kura is an Eclipse IoT challenge which focuses to give a Java/OSGi-based absolutely method for IoT entryways which run M2M applications [96]. Kura gives a stage for managing the connection among the adjacent system of substantial IoT gadgets and the general population web or the cell systems. Additionally to various method, Kura abstracts and secludes the engineer from the unpredictability of the equipment, organizing sub-structures, and re-characterizing the enhancement of existing programming segments, by utilizing giving an APIs that permit approaching and adapting to the fundamental equipment effectively [97].

#### **3.7.1. Architecture**

Fig. 3.12 proposes a best dimension see about Kura's structure. Kura can best be snared on Linux-based gadgets and gives a remotely sensible framework, entire with the majority of the center administrations and a gadget deliberation layer for approaching the entryway's own special equipment [98].

To cooperate with system associated gadgets, brilliant applications can utilize Java's own special systems administration capacities to connect to the current instrument framework. The gadget reflection layer licenses designers to get right of section to numerous devices by method for abstracting the equipment utilizing OSGi administrations for Serial, USB and Bluetooth correspondences.

A correspondence API for devices associated through I2C, PWM or GPIO will allow a machine integrator to incorporate a custom equipment as a piece of their entryway [96].

The Gateway essential administrations layer gives configurable OSGi (Open Service Gateway Initiative) administrations accessible to applications to have cooperation with the fundamental entryway usefulness. Such administrations comprise of guard dog, clock, GPS position, installed database, strategy, and instrument profile benefit.

Also, the system control layer offers a configurable OSGi (Open Service Gateway Initiative) contributions to get right of section to the present system design and regulate it (e.g. DHCP, NAT, DNS, and numerous others.). It collaborates with the Linux machine to design arrange interfaces comprising of Wi-Fi inspire right of passage to focuses and PPP associations.

Besides, the availability and transport layer rearranges the improvement of telemetry M2M applications connecting with a remote cloud server [99].

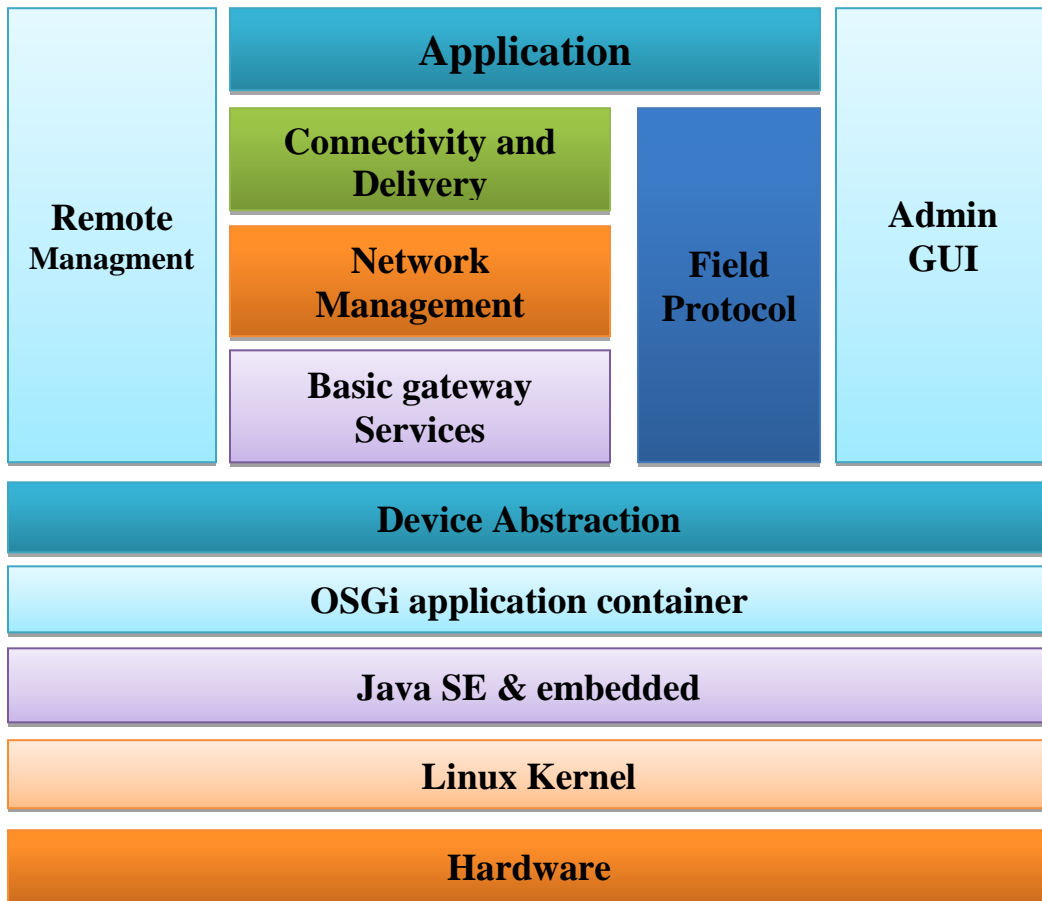


Fig.3.12 Kura architecture

The usefulness of the remote control layer incorporates remote setup, distant programming program refresh, a remote gadget order, faraway log recovery, device analytic administration, and faraway VPN get section to. At long last, the organization GUI gives interfaces to accessing such administrations.

### 3.7.2. Hardware specifications

Kura has intense necessities while in transit to keep running for the IoT device. It should keep running on the highest point of the Linux working framework. Along these lines, the IoT gadget ought to be Linux-essentially based. Second, Oracle Java VM 7 or later is required for Kura [98].

Memory length necessity relies upon how colossal is the snared programming and the quantity of traded messages to associated contraptions. A case of perfect contraptions, that meet the referenced necessities, incorporates Raspberry Pi [100] and Beagle Bone [101].

### 3.7.3. Security features

Kura has intense necessities while in transit to keep running for the IoT device. It should keep running on the highest point of the Linux working framework. Along these lines, the IoT gadget ought to be Linux-essentially based. Second, Oracle Java VM 7 or later is required for Kura [102]. Memory length necessity relies upon how colossal is the snared programming and the quantity of traded messages to associated contraptions. A case of perfect contraptions, that meet the referenced necessities, incorporates Raspberry Pi [100] and Beagle Bone [101].

**Authentication:** Kura utilizes agreeable attachments take with the guide of the Java condition. The overshadowing paho client [103] handles the vast majority of data verbal trade by means of MQTT convention [99]. This comprises of the utilization to verify report with faraway gadgets and entryways.

**Authorization and access manage:** The security supplier issue in Kura offers API to control security guidelines and start content consistency, while the endorsement benefit API is utilized to recover, keep and affirm declarations for SSL, gadget control and package marking.

Ensuring the non-defilement or non-messing with a report by a noxious purchaser is accomplished through completing a regular check of ecological respectability by means of the wellbeing supervisor part. ESF also implements runtime arrangements to prevent execution from claiming one of a kind contributions or the import/fare of exact applications. This makes it harder for programmers to get to the administration for recovering the grip secret word from the apparatus.

**Secure communication:** The SSL manager oversees SSL authentication, acknowledge as valid stores & individual and open keys. All interchanges have anchored the utilization for the SSL/TLS convention. The cryptography APIs are utilized to encode and unscramble privileged insights and methods and methodologies and to recover the grip phrase.



## 3.8. SmartThings

Smart Things is a stage propelled by methods for Samsung for developing IoT bundles. It's far specifically dedicated to shrewd houses, wherein designers can put in power programs that let clients control and control their local home hardware through keen phones [104].

### 3.8.1. Architecture

Reliable with fig. 3.13 the smarthings environment contains the following added substances: the smarthings cloud backend the keen things center point/local controller the smart things cell buddy application and in this manner the iot device brilliant gadget.

The center point home controller goes about as an entrance way between the iot contraptions great gadgets and cloud contributions. It associates on to the on the web and backings more than one discussion conventions alongside Zigbee, z-wave remote neighborhood Wi-Fi and link. The smarthings center point can possibly execute a few capacities locally while not the need to connect to the cloud backend. Occasions are as yet should have been dispatched to the cloud once the center point inspires online as the best approach to reproduce the advanced nation of the house and execute totally unique cloud-based contributions. Dispatch among every single associated party has scrambled the work of the SSL/TLS convention.

the pal app discharged through smart things will we clients get section to the house controller control their iot devices effectively and whenever required establishment outsider projects smart apps the amigo application is bolstered by utilizing more than one versatile working frameworks comprising of android and ios. While the mate application displays a key and bound together interface to every single related device smart apps are hand crafted applications developed by outsider manufacturers transfer more prominent choices and ability to the surrender buyer. 3 exercises of smart apps are.

Indicated: (I) occasion handlers (ii) arrangement modules and (iii) benefit administrators. Occasion handler smart apps allow stop clients to buy in to occasions and call handler procedures upon their firings. arrangement module shrewd applications go about as a field for the two distinct classifications of savvy applications and disentangle the control of a positive substantial territory inside the home e.g. room they might be predefined by method for smart

things engineers and hence they might be introduced by means of the smart things application interface the companion application eventually supplier director keen applications are bundles that coordinate with smart devices and should be mounted by utilizing surrender clients if there should be an occurrence of the nearness of the instrument on the network. Keen applications may also keep running on the center and in addition in the cloud depending at the physical qualities of the smartdevice.

Smart Devices could, moreover, can possibly connect by means of Wi-Fi/IP convention. This decision we tend to might those gadgets to skirt the entrance way and be a piece of on to the Smart Things cloud. Each sensible apparatus has a place with at least one or a great deal of the following

Classes: (I) Hub-associated, (ii) LAN-associated, and (iii) Cloud-associated [105]. Center point associated gadgets grasp all devices that have the common sense to act with the Smart Things center the work of ZigBee or Z-Wave home mechanization conventions, while LAN-related

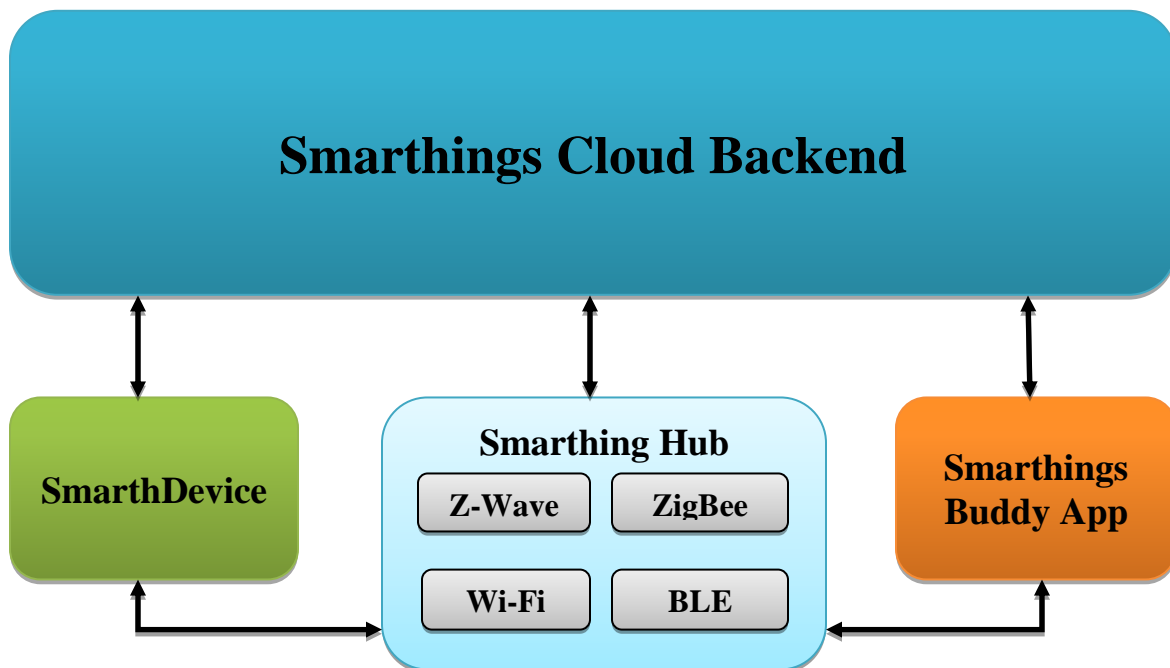


Fig.3.13 SmarthThings architecture

gadgets have a further play out that gives them a chance to speak with the center over the LAN, e.g. sonos machine. Cloud-associated gadgets, e.g. Ecobee indoor regulator, associate with the

cloud straightforwardly the work of HTTP and authenticate themselves the work of OAuth convention. Every neighborhood |LAN| PC system and Cloud-associated gadgets are prepared to talk and blend through net administrations like unwinding or enhancement cleanser [104]. There are two techniques for correspondence among shrewd applications and brilliant gadgets; (I) strategy brings in which savvy applications can execute and perform activities over keen gadgets and (ii) occasion membership where shrewd applications can buy in to occasions created by method for various shrewd applications or brilliant gadgets.

Fig.3.14 gives a blueprint of the essential thing building squares of the smart things cloud [106]. The availability control layer is at risk for keeping up a constant and secure association between the associated gadgets e.g. the center point and cloud administrations. The instrument type handler's layer improves the adaptability through keeping-in an occurrence or a virtual photograph for each sort of shrewd gadgets. End-clients interface with the physical shrewd

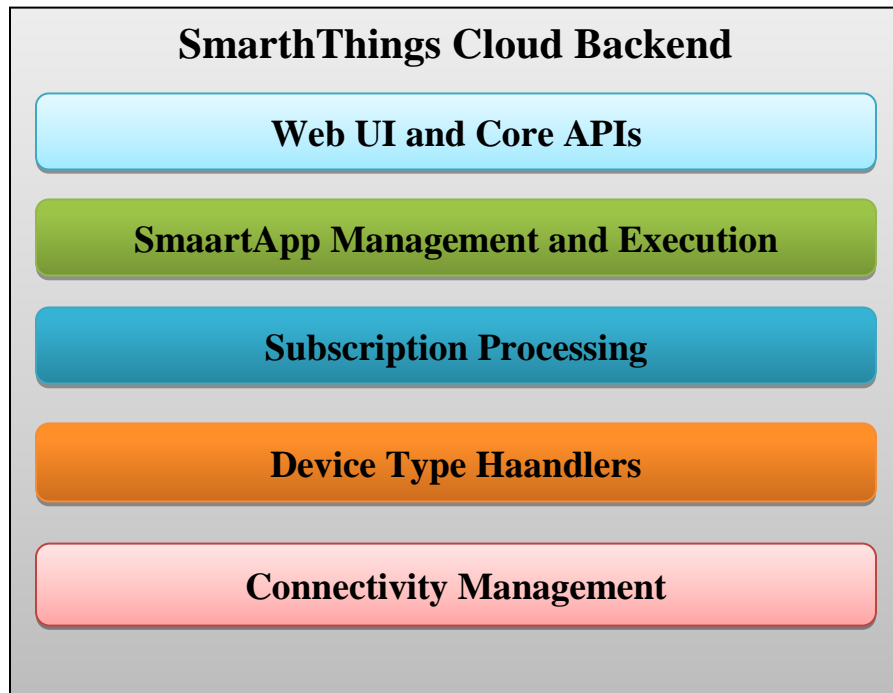


Fig.3.14 The structure of the SmartThings cloud system

gadgets roundabout through occasions facilitated inside the cloud. The subscription preparing

layer goes about as an occasion chief for steering exercises from center points/gadgets to shrewd applications which can be bought in to a specific savvy gadget/occasion. The keen application the executives execution layer presents motivate admission to rights to the spared data and is at risk for the execution of the shrewd application when expedited by means of the two memberships and outer calls. The best layer of the stack is the web ui layer which offers web administrations and applications with the aim to help the coordination with third-festival applications.

The smart things cloud backend has 2 imperative abilities. In the first place, it has and runs sensible applications amid a shut supply encompassing. Second, it runs the computerized programming framework photo of the physical smart instrument. In a few expressions, it gives the reflection and knowledge layers in addition as web benefits that manage the machine layer.

### **3.8.2. Hardware specification**

SmartThings stage a wide assortment which indicate IoT related things that may either coordinate by the SmartThings center or interface straightforwardly to the cloud backend. These gadgets are produced by a few merchants for example Samsung, Amazon, Philips Hue, google and numerous others. The main required detail is the capacity to convey utilizing one of the perfect conventions.

### **3.8.3. Security features**

SmartThings stage underpins a substantial sort of IoT gadgets that would each incorporate with the SmartThings center or interface promptly to the cloud backend. These gadgets are counterfeit by numerous providers like Samsung, Google, Amazon, Philips Hue, and a lot of others. The main required detail is that the ability to impart the work of one of the good conventions.

**Authentication:** Incorporating new Smart Device in SmartThings surroundings includes utilizing OAuth/OAuth2 convention for validating this Smart-Device and approving SmartThings stage to get admission to its capacities. Cloud-and LAN-associated devices watch a piece exceptional strategy for confirmation because of the use of various correspondence conventions to pass the door and interface specifically to the cloud. Every one of them requires making sense of a custom bearer chief Smart-App together with a gadget handler for setting up

associations, overseeing verification, allowing approval, and keeping up the discussion. The essential highlights of the transporter manager are taking care of validation with outsider cloud benefit, gadget disclosure, starting the association the utilization of OAuth convention, and controlling cunning bad habit developments. The gadget handler is subject for parsing messages being dispatched or acquired by methods for the comparing shrewd bad habit. Nonetheless, making sense of the Smart-Device amid the confirmation framework is principally founded on numerous elements as a result of the extensive variety of the upheld Smart-Devices from various organizations. Instances of such components comprise of a specific identifier e.g. sequential range, media get to control (MAC) address, specific IP address, etc.

**Authorization and access control:** Approaching Smart-Devices the utilization of Smart-Apps pursues the rules controlled by the SmartThings usefulness rendition. A capacity is a basic thought inside the basic design which has a place with a legitimate layer that gives a reflection of the capacities of Smart-Devices. The Smart-App must request a consent to apply a usefulness offered by method for a Smart-Device. The ability, as perceived by methods for it Name, comprises of an immovable of directions and their related qualities. Directions are strategies or capacities to play out a couple of moves at the shrewd instrument, while traits are entering parameters speaking to the condition of the gadget. Table 1 shows a few instances of a couple of gifts in the SmartThings stage. Due to applying this model, introducing a battery-checking Smart-App may be approved to apply the usefulness of battery and turned away from accessing different sources or capacities bolstered by method for the Smart-Device.

All Smart-Apps are practiced by methods for the SmartThings environment. This implies those applications run either inside the shut source cloud or on the SmartThings center point. The SmartThings foundation environs-proposed applies Kohsuke sandboxing approach [107] and separates both Smart-Apps and Smart-Devices (instrument Handler times) from each extraordinary [108]. In the vibe of bestowing a massively controlled encompassing by utilizing Groovy, Kohsuke sandbox is a proficient usage that secludes untrusted running bits of code and lets in best strategy calls which are predefined in a whitelist, put away inside the limited running gadget. Developers can't make their own one of a kind exercises or load outside libraries in such condition and after they post a Smart-App or a brilliant gadget, a non-open remotes information

spare is allocated.

**Secure communication:** The SmartThings Hub could be a security-empowered Z-Wave item. While a security-empowered Z-Wave gadget is conveyed to the Hub's people group, the discussion can be encoded the utilization of 128-piece AES. Because of the center point moreover bolsters the ZigBee convention, it gives the indistinguishable wellbeing guarantees to ZigBee-empowered stock. When all is said in done, correspondences between all building squares of the SmartThings surroundings is finished over partner SSL (Secure Sockets Layer)/TLS (Transport Layer Security convention).

# Chapter 4

## Attack or threat

### 4.1. DoS attack

In processing, a disavowal of-benefit snare (DoS attack) is an ambush of advanced assault wherein the transgressor hopes to make a gadget or framework push distant to its suggested customers by using quickly or uncertainly irritating commitments of a group related to the web. Renouncing of a transporter is all things considered finished by a technique for flooding the connected with machine or help with futile requests in an undertaking to over-load structures and keep a couple or each and every generous interest from being fulfilled. In a disseminated refusal of-benefit ambush (DDoS attack), the data moving toward traffic flooding the sufferer starts from various specific resources. This viably makes it unrealistic to stop the strike really by techniques for obstructing a singular source.

A DoS or DDoS assault has likenesses to a gathering of individuals swarming the section entryway of a store, making it intense for real clients to go into, disturbing trade. Criminal culprits of DoS attack much of the time objective sites or contributions facilitated on unnecessary profile net servers which incorporate banks or charge card expense doors. Retribution, extortion, and activism can propel those attacks. [109]

**Attacking method:** An application layer DDoS assault is performed particularly for definitely focused on capacities, which incorporates upsetting exchanges and get admission to databases. It requires fewer sources than system layer assaults however as often as possible goes with them. An attack is camouflaged to give off an impression of being legitimate guests, with the exception of it objectives explicit programming bundles. The attack at the utility layer can upset administrations including the recovery of information or inquiry trademark and in addition net program trademark, email contributions, and picture applications. To be regarded a conveyed refusal of bearer strike, additional than round 3– five hubs on explicit systems should be utilized; the use of less hubs qualifies as a DoS attack yet now not a DDoS attack.[109]

## 4.2. Jamming Attack

Jamming attack are unnecessary Denial-of-benefit assaults towards remote medium. on this work, contemplating the situation of the remote foe, which objectives the parcels of over the top hugeness by utilizing discharging radio recurrence pointers and don't conform to fundamental system engineering.

**Attacking method:** Jamming attack is a type of Denial of service attack, which keeps distinctive hubs from the use of the channel to impart through involving the channel that they are conveying on. We diagram the jammer in remote sensor arrange as an element who's intentionally trying to intercede with the physical transmission and gathering of wi-fi interchanges. A typical circumstance of sticking assault is demonstrated in decide 1. The customary hubs C and D have been stuck through the noxious hub X, so the interchanges between the stuck nodes(C, D) and the standard hubs (A, B, E, H, I) are disturbed. Fig.4.1 given blow. [110]

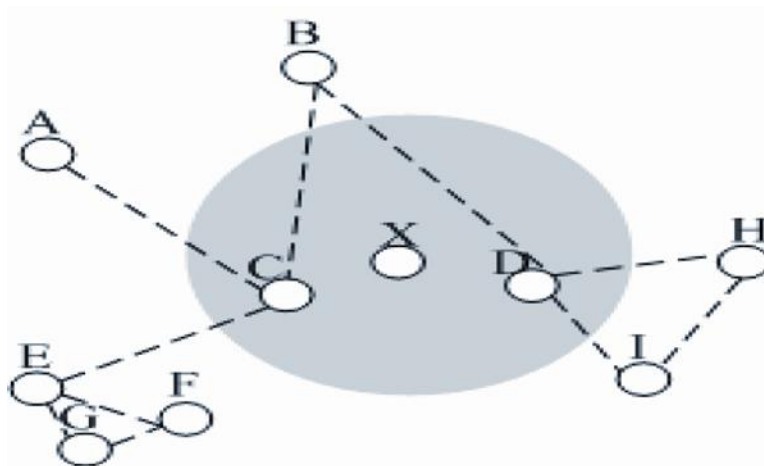


Fig.4.1 jamming attack matrix

## 4.3. Blue borne attack

Blue Borne is an attack which vector through programmers can use Bluetooth associations with



entering and take all together to influence over focused gadgets. Blue Borne impacts ordinary PC frameworks, cell phones, and the other domain of IoT gadgets. The attack does now not require the focused on an instrument to be combined to the assailant's gadget, or possibly to be determined to creatable mode. Armis Labs has analyzed eight 0-day vulnerabilities up until now, which propose the ways of life and capacity of the assault vector. Armis accepts numerous more noteworthy vulnerabilities hang tight for revelation inside the different frameworks the utilization of Bluetooth. Those vulnerabilities are totally operational and can be effectively misused, as exhibited in our examinations. The Blue Borne attack vector might be utilized to direct an enormous assortment of offenses, for example, far-flung code execution notwithstanding man-in-the-middle attack. [111]

**Attacking method:** The BlueBorne attack vector has various dimensions. Initially, the assailant finds vigorous Bluetooth associations around her or him. Gadgets can be perceived notwithstanding the way that they're never again set to "discoverable" mode. Next, the attacker acquires the instrument's MAC address that is a one of a kind identifier of that exact device. Through testing the device, the aggressor can figure out which running framework his injured individual is utilizing, and adjust his endeavor henceforth. The attacker will at that point exploit helplessness inside the execution of the Bluetooth convention inside the significant stage and preferred standpoint they get section to he wishes to follow up on his pernicious goal. At this dimension, the aggressor can choose to make a man in-The-middle assault and control the device's correspondence, or take full control over the gadget and use it for a major scope of cybercriminal purposes. [111]

#### **4.4. Remote access using telnet**

Telnet is a convention applied at the net or neighborhood placed network to offer a bidirectional sensible revealed content material-oriented discussion office using a sophisticated terminal association. Patron information is blended in-band with Telnet manage actualities in an 8-bit byte oriented statistics association over the Transmission Control Protocol (TCP). Telnet modified into cutting aspect in 1969 beginning with RFC 15, reached out in RFC 855, and institutionalized as internet Engineering assignment pressure (IETF) internet famous STD eight, one of the primary net norms. The name means "print network". [112]

Typically, Telnet furnished get admission to an immediate line interface (typically, of a working contraption) on a remote host, as an example, maximum system framework and running structures with a design software, (as an instance, structures basically dependent on Windows NT).but, in view of notable insurance worries at the same time as the usage of Telnet over an open machine collectively with the net, its usage for this goal has wound down truly for SSH. The term telnet is in like manner used to allude to the product software that executes the consumer a piece of the conference. Telnet purchaser packages are handy for surely all computer systems. Telnet is additionally applied as a movement phrase. To telnet,manner to deal with the buildup an affiliation making use of the Telnet convention, both with order line patron or with an automated interface. as an instance, a no longer sudden mandate is presumably: "To change your secret word, telnet into the server, check in and run the password command." often, a customer can be telnetting to a Unix-like server system or a network tool (which incorporates a switch) and obtaining a login incite to a course line printed content material interface or a person or woman primarily based complete-display display screen administrator.

**Attacking method:** Telnet is a remote access get passage to gadget used to sign into remote servers; however, it has been logically supplanted by ssh, furthermore alluded to the as quiet shell. Chiefs are typically advised to cripple telnet if the convention isn't constantly used to spare you attacks focused on it, anyway some disregard. This convention is utilized to set up an association with Transmission Control Protocol (TCP) port assortment 23, wherein a Telnet server application (telnetd) is tuning in. [113]

#### **4.5. Sybil attack**

The Sybil strike in PC security is an ambush wherein a reputation system is subverted by delivering characters in appropriated networks. It is named after the subject of the book Sybil, a relevant examination of a woman resolved to have a dissociative identity disorder.[114] The name was prescribed in or before 2002 by Brian Zill at Microsoft Research.[115] The term pseudo caricaturing had as of late been created by L. Detweiler on the Cypherpunks mailing list and used in the composition on circulated structures for a comparative class of strikes going before 2002, nonetheless, this term did not get as much effect as "Sybil attack".[116]

**Attacking method:** The assault starts by way of making an expansive quantity of characters. The much less highly-priced in the exertion to make extra, the less stressful its miles to expand numbers, undermining the notoriety arrangement of that shared device. The primary component is, how an awful lot the notoriety framework acknowledges contributions from hubs that do not have a series of agree with connecting them to known, confided in hubs and if that framework treats all hubs indistinguishably, the less complicated it's far to undermine the whole notoriety framework and basically declare that notoriety framework. An enemy may display various characters to a shared system so as to show up and work as numerous unmistakable hubs. The foe may hence have the capacity to get an unbalanced dimension of authority over the system, for example, by influencing casting ballot results. [117]

#### **4.6. Exploit kit**

A make the most pack or exploit kit is a type of toolbox cybercriminals use to ambush vulnerabilities in frameworks that will disperse malware or perform diverse malevolent games. Make the most units are bundled with endeavors which could objective typically mounted software. An ordinary adventure bundle by and large bears an administration reassure, a gaggle of vulnerabilities focused to unmistakable bundles, and a few transfers on capacities that make it less troublesome for a cybercriminal to discharge an attack. [118]

**Attacking method:** Exploit bundle is an application that attackers use to discharge misuses towards helpless bundles. An exploit is a thing - including a bit of code or series of directions that exploits helplessness in a product to weight it to act startlingly. Make the most pack is really an application for collecting and adapting to more than one endeavors. They go about as a kind of storehouse and make it simple for clients absent much-specialized comprehension to utilize misuses.

It's essential to take note of the utilization of endeavor units isn't restricted to noxious sites. Attackers should simply implant a quiet HTML tag into an authentic site page or into an ad on that page and everybody who visits that site will be assaulted. [119]

## 4.7. Man in the middle attack

In cryptography and PC wellbeing, a man-in-the-middle attack (MITM) is an ambush wherein the attacker subtly transfers and more than likely changes the correspondence among gatherings who consider they might be on the double speaking with each unique. One case of a MITM is exuberant listening stealthily, in which the attackers make unbiased associations with the people in question and transfers messages among them to make them trust they are talking on the double to one another over an individual association, while in truth; the entire discussion is overseen by methods for the aggressor. The attacker ought to be fit to catch every single pertinent message going among the 2 exploited people and infuse new ones. This is clear in loads of conditions; for instance, an aggressor inside gathering scope of a decoded remote inspire right of passage to point [120] could embed himself as a man-in-the-middle. [121]

As an attack that interests at evading shared confirmation, or scarcity in that department, a man-in-the-middle attack can be fruitful most straightforward when the assailant can imitate every endpoint to their pleasure as anticipated from the real finishes. Greatest cryptographic conventions comprise of a couple of types of endpoint confirmation Wi-Fi to avert MITM attacks. For instance, TLS can verify one or the two occasions utilizing an, on the whole, relied upon trust. [120]

**Attacking method:** In fact, showing up a triumph man-in-the-middle attack is on the other hand muddled. Nonetheless, modern devices for showing up them are very easy to be had, each for programmers and for entrance experimenting with. For instance, the Metasploit entrance looking at gadget helps numerous styles of MITM ambushes out-of-the-compartment and contraptions like Armitage offer a clean-to-use graphical UI for performing such strikes remotely.

Acting a MITM snare routinely calls for having the capacity to energize packs among the help and server to encounter a structure the assailant controls. Arp poisoning is dependably used for including site visitors in a locale structure to the aggressor's machine. Accumulated arranging ambushes may be used to do the strike remotely. It's in like manner not exceptional for programming engineers and malware to get switches, DSL modems, and Wi-Fi base stations to put in malware on them that plays out the man-in-the-center assaults. [122]

## 4.8. Replay attack

A replay attack (which is known as playback attack) is a type of network attack in which an authentic measurements transmission is malevolently or deceitfully rehashed or deferred. This is finished either by methods for the originator or through a foe who captures the data and re-transmits it, likely as a piece of a disguise ambush with the guide of IP bundle substitution. This is one of the decline level renditions of a "man-in-the-middle attack".

Some other way of depicting such an attack is: "an ambush on a security convention the utilization of replay of messages from an alternate setting into the implied (or bona fide and anticipated) setting, consequently tricking the genuine player(s) into pondering they've proficiently completed the convention run." [123].

**Attacking method:** Replay attack, in which assailants capture and re-transmit organize bundles that don't have a place with them, are uncommonly risky and can at times cause genuine loss. What makes those kinds of attacks significantly more noteworthy dangerous is that they can be arranged on encoded verbal trade channels without accessing the decoding keys. Aggressors handiest should snoop on your line and highlight a famous comprehension of what undertaking a chose set of bundles are showing up, and with the guide of resending those parcels or demands, they will have the capacity to upset your correspondences or reason increasingly ominous results. [124]

## 4.9. Ransomware

Ransomware is a kind of malevolent programming from cryptovirology that undermines to post the unfortunate casualty's certainties or persistently square get the section to it until the point that a payoff is paid. indeed, even as a couple of straightforward ransomware may likewise secure the gadget a way which isn't constantly troublesome for an educated individual to an inverse, additional predominant malware makes utilization of a method called cryptoviral coercion, in which it encodes the sufferer's records, making them out of reach, and needs a payment cost to unscramble them. [125] In an appropriately connected cryptoviral blackmail attack, enhancing the reports without the decoding mystery's an obstinate inconvenience – and hard to indicate computerized monetary forms which incorporate Ukash and digital currency are utilized for the payments, making following and arraigning the culprits hard. Ransomware strikes have typically

completed the use of a Trojan this is veiled as a genuine archive that the client is deceived into downloading or beginning while it touches base as an email connection. Be that as it may, one inordinate profile example, the "WannaCry worm", voyaged routinely between PC frameworks without client exchange.

**Attacking method:** Maximum ransomware is conveyed through email that appears to be substantial, connecting with you to click a connection or download a connection that can give the vindictive programming. Ransomware is likewise conveyed by means of weight by utilizing download assaults on traded off or vindictive sites. Some ransomware attacks have even been sent the utilization of internet-based life informing.

Standard ransomware is scarcely ever in my view concentrated, but instead a "shotgun" strategy where aggressors accumulate arrangements of messages or traded off sites and impact out ransomware. Given the quantity of assailants available, it will be plausible that on the off chance that you get hit more than multiple times, it will probably be by utilizing an alternate aggressor.

Regardless of whether or no longer the payment is paid, consider that assailants will continually endeavor to remove valuable certainties from a traded off gadget. expect every tricky datum at the contraption transformed into traded off, that could envelop usernames and passwords for inward or web resources, charge information, electronic mail locations of contacts, and that's just the beginning. [126]

#### **4.10. Side channel attack**

In computer security, a side-channel attack is any attack fundamentally dependent on records got from the usage of a PC framework, rather than shortcomings inside the actualized calculation itself (e.g. cryptanalysis and programming program bugs). Timing data, vitality utilization, electromagnetic releases or even solid can offer an additional supply of data, which can be exploited. A few side-channel strikes require a specialized comprehension of the inner task of the machine, despite the fact that others comprising of differential power assessment are viable as dark holder assaults. The ascent of net 2.zero bundles and programming as-a-supplier has likewise obviously raised the likelihood of angle channel assaults at the web, notwithstanding when transmissions between an internet browser and server are scrambled (e.g., through HTTPS or Wi-Fi encryption), with regards to scientists from Microsoft research and Indiana college.

[127] many powerful aspect channel assaults depend absolutely on factual techniques spearheaded by utilizing Paul Kocher.

Endeavors to intrude on a cryptosystem by means of misdirecting or constraining individuals with substantial motivate passage to are not ordinarily thought about side-channel assaults: see a social building and elastic hose cryptanalysis.

**Attacking method:**Cloud computing is seized into consideration one of the most dominant paradigms in the information of technology IT industry in recent times. It supports multi-tenancy to fulfill future growing needs for getting access to and the use of assets provisioned over the internet. Multi-tenancy permits to percentage computing physical sources among cloud computing tenants and give cost-powerful on-call for scaling. But multi-tenancy in cloud computing has unique vulnerabilities including customers' co-house and digital machine physical co-residency. Bodily co-residency of virtual machines can facilitate attackers with a capacity to intervene with some other virtual gadget running at the same physical machine due to an inadequate logical isolation. In the worst state of affairs, attackers can infiltrate sensitive records of victims at the identical bodily system via the use of hardware side-channels. Side-channel assaults are an implementation stage assault on cryptographic structures. They take advantage of the correlation between the higher level functionality of the software program and the underlying hardware phenomena. there are various sorts of side-channels assaults which are classified in step with hardware medium they goal and make the most as an example cache facet-channel attack. [128]

# Chapter 5

## Result and comparative analysis

### 5.1. Aws framework

#### **Dos attack:**

AWS offers flexible infrastructure and offerings that assist customers to enforce strong DDoS mitigations and create enormously to be had application architectures that comply with AWS first-rate Practices for DDoS Resiliency. These include offerings inclusive of Amazon route fifty-three, Amazon CloudFront, Elastic Load Balancing, and AWS WAF to manipulate and take in traffic, and deflect undesirable requests. These services combine with AWS shield, a managed DDoS safety service that offers continually-on detection and automatic inline mitigations to protect internet applications strolling on AWS. This document describes not unusual DDoS attack types and offers AWS customers with satisfactory practices and strategies for defensive programs from a DDoS attack.[129]

#### **Blueborne attack:**

The vulnerability placed over approximate 5 billion devices at capability threat, with many yet opens to these flaws. These days, Armis Labs has opened that a predicted 20 million Amazon Echo are at risk of attacks through the BlueBorne exploit. Researchers delivered that attackers can take whole control of the device within the case of the Amazon Echo.

No longer all BlueBorne vulnerabilities (there have been over eight) have an effect on the device. Amazon Echo is at risk of CVE-2017-1000251 (RCE flaw in Linux Kernel) and CVE-2017-1000250 (data leak inside the SDP Server). Researchers introduced that attackers can take entire control of the tool within the case of the Amazon Echo.

#### **Jamming:**

Wireless networks provide a wide range of services which is never so easy by any other medium, its mode of working tends it to have many security breaches. In the modern era of communication, trillions of profitable vital information is available on the internet and they are



accessible through this open medium. Such vital information can be achieved through intentional interference or jamming. There have a shield technique to prevent jamming and different avoidance techniques.

[130]

### **Remote access using telnet:**

with a view to supplying an oversight administration encounter, Amazon RDS does not give shell get right of the section to in DB examples, and it limits get passage to specific framework systems and tables that require propelled benefits. Amazon RDS encourages access to the database on a DB case the use of any favored sq. server control studio. Amazon RDS does not allow guide have got admission to in a DB occurrence through telnet, secure shell (SSH), or windows remote registering device association.[131]

### **Exploit kit:**

For an attacker, breaching a system is about exploiting its weaker spots. Cloud environments shift these weaknesses dramatically. Some traditional attack vectors become very difficult to exploit and thus less important, while many new vectors open up. This presents new challenges for security teams, as they have to model their security very differently from traditional data centers.

EC2 instances, RDS, Amazon Redshift, etc.: customers can control on which VPC or subnet to launch these resources, thus controlling access to the resources. Aws VPC defines an excellent perimeter that provides security groups for firewalling.[132]

### **Man –in-the-middle attack:**

Man in the middle (MITM) attacks. All the AWS APIs are to be had through SSL protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificate on first boot and log them to the instance's console. You may then use the secure APIs to call the console and access the host certificate earlier than logging into the instance for the primary time.[133]

**Ransomware:**

Unsecured Amazon s3 buckets are prime cloud target for ransomware attacks. Misconfigured s3 buckets are a too-common problem among Amazon web services (aws) users and security researchers are taking notice. Noted security researcher Kevin Beaumont has warned that publicly writable s3 buckets could be used by criminals in ransom attacks.[134]

**Side channel attack:**

Updated kernels for Amazon Linux AMI 2017.09 (alas-2018-1058), Amazon Linux AMI 2018.03 (alas-2018-1058), and Amazon Linux 2 (alas-2018-1058) are to be had within the respective repositories. As a standard security excellent exercise, we recommend that clients patch their operating systems or software program as applicable patches grow to be available to deal with emerging side-channel problems.[135]

## 5.2. ARM mbed

**DoS attack:**

Little, low-vitality gadgets like sensors and surveillance cameras are the greatest unmistakable a piece of IoT, and that they're legitimate in ARM's wheelhouse on the grounds that the overwhelming weight in low-vitality chips. Anyway, the association featured a cloud-based SaaS displaying rather than chips or edge gadgets themselves. IoT depends upon on once more end aptitudes as parcels as feature gadgets, and the association wants to assume a job in it all. The SaaSstage, known as mbed Cloud, handles gadget association and setup, encryption-key provisioning, and firmware refreshes. [136].

**Jamming attack:**

An embedded sensor hub microcontroller intended to help sensor organize applications with serious security requests is exhibited. It includes a low power 16-bit processor center upheld by various equipment quickening agents intended to perform complex activities required by cutting-edge crypto calculations. [137].

**Remote access using telnet:**

In arm mbed, there is an access of remotely login. Data is encrypted when access. There is a password to log in. The HTTPS server makes use of the ARM mbed TLS software program component to allow secure communication. [138].

**Man in the middle attack:**

ARM's "mbed TLS" programming system might be deceived into a validation sidestep and needs a fix.

Made by methods for PolarSSL, which was gotten in February by methods for ARM, mbed is a crypto library intended to make it simple for inserted framework designers to include SSL/TLS capabilities to their items. ARM's embedded TLS can fixes man-in-the-middle attack. [139]

**Replay attack:**

The BLE Gateway and BLE Sensor is an endeavor at alleviating the defenselessness to replay attack when utilizing reference point type ads. It's composed for nRF51822 equipment with no locally available NVRAM. [140].

**Side channel attack:**

Side channel attack can be entered into the cloud.but can be detected. There using the mbedTLS functions of AES256-GCM. [141].

**5.3. Azure IoT suite****DoS attack:**

Application layer assurance with purplish azure web application firewall. Protection against the unanticipated expenses of a ddos attack. [142].

**Blueborne attack:**

To abuse the vulnerability, the aggressor should be inside the physical closeness of the focused on the client, and the client's PC needs Bluetooth empowered. The attacker would then be able to start a Bluetooth association with the objective PC without the client's information. [143]

**Jamming attack:**

In azure IoT suite, there have a security protocol that can fix the jamming attack. [144]

**Remote access using telnet:**

If an IoT Gateway is deployed within the industrial plant and if a few application crashes in Gateway or a few need of login to the gateway. If so, Azure IoT edge must permit users to remotely log in to the IoT gateway the use of ssh/telnet. This can be very easy to reveal the status and debugging/protection. [145]

**Sybil attack:**

The enterprise makes use of machine studying structures to assist prevent cyber assaults or to mitigate ability damage have to they succeed. Every day, Microsoft's account protection structures automatically locate and prevent greater than 10 million attacks from tens of hundreds of locations, even if the attacker has legitimate credentials. [146]

**Man in the middle attack:**

Numerous Microsoft Azure IoT SDKs are inclined to a security weakness that may enable aggressors to direct ridiculing attack. A man-in-the-middle attack can misuse this issue to lead caricaturing attack and perform unapproved activities. [147]

**Replay attack:**

Microsoft engineers have pooled their endeavors to propose an assurance against what are known as "replay attack". These will be happen when an aggressor takes something like an injured individual's OAuth token and utilizations it to mimic them to get to generally anchored assets.[148]

**Ransomware:**

Microsoft antimalware products had been up to date with signatures for this threat which includes windows defender antivirus. These submit summarizes measures that azure clients can take to prevent and stumble on this threat through azure security. [149].

**Side channel attack:**

Microsoft has sent alleviations over all the cloud administrations. The foundation that runs azure and confines client remaining burdens from one another is ensured. This implies a potential attacking utilizing a similar foundation can't attack any application utilizing these vulnerabilities. [150].

**5.4. Brillo/weave****DDos attack:**

Google released Brillo/Weave platform for the rapid implementation of IoT applications. From the last few years our favorite searching site google was attacked by Distributed denial of service or DDos .A DDos attack is an attempt to make an online service unavailable overwhelming it with traffic from multiple sources.They can have a huge impact if businesses aren't adequately prepared. As a google cloud customer we are protected by default to this type of attack. As the scale of our infrastructure enables us to simply absorbed many of them. For context a huge attack last year had a strength of around one terabit per second (1Tb/sec) .The whole internet has a bisection bandwidth of 200Tb/sec.Now when we compare this to a single Google data center which has a bisection bandwidth of 1,300Tb/sec.

We can see Google already built in level of internal capacity multiple times doubt of any traffic load we anticipate. When there is an attack, Google have time to isolate it and address it but Google don't stop there. In Google cloud platform customers benefit directly from Google central dose mitigation service that provide an additional multi tear multi-layer protection and further reduces the risk to services running behind of Google front end. When the system detects an attack is taking place it can configure load balancers to drop or throttle traffic associated with the attack.[151].

**Blueborne attack:**

Google related android device can minimize the BlueBorne attack. [152]

Below is a list of android devices that have the ability to stand against the blueborne attack:

- .Nexus 5X
- .Nexus 6P
- .Nexus 6
- .Nexus 9

**Jamming Attack:**

Mobile jamming attack is a power wasting denial-of-service attack. The mobile jamming protecting method works multi topologies scheme to reduce the mobile jamming attack so the affected area also be reduce. [153]

**Remote access using telnet:**

There is remote access in google but the hacker can't do anything cause the data being encrypted.

**Sybil attack:**

Existing decentralized defences have largely been designed for peer-to-peer networks but not for mobile networks. That is why a new decentralized defence for portable devices and call it MobID. The idea is that a device manages two small networks in which it stores information about the devices it meets: its network of friends contains honest devices, and its network of foes contains suspicious devices. By reasoning on these two networks. [154]

**Exploit Kit:**

Exploit kit have some program interface which permit non-technical clients to through unclean attacks for stealing corporate and personal data. Google cloud can minimize this problem by default. [155]

**Man in the middle attack:**

Google related application like googlechrome can recognize man in the middle attack automatically. Google chrome warn the clients when 3rdparty software try to hack the web connection or something other data. [156]

**Replay attack:**

To keep away from this kind of attack is all about having the right method of encryption. Google already released encryption at rest in google cloud platform and G suite encryption to prevent this attack on google cloud. [157]

**Ransomware:**

Google related android device can also prevent the ransomware attack by having antivirus like Bitdefender,Kaspersky,Mcafe,AVG etc.[158]

**Side channel attack:**

Side channel attack can be removed by some steps,

Eliminating the arrival of private data or confirming this data is random to private information.

Electrical cable molding and separating to dissuade control checking assaults and also emanating a station with commotion. [159]

**5.5. Ericsson/Calvin****DDos attack:**

An effective way to improve the resilience of the centralized control plane and prevent the spread of DDoS control-plane attacks to the rest of the network is to rate-limit NEs in terms of bandwidth and resource consumption – such as cpu load, memory usage, and api calls. [160]

**Remote access:**

Remote access is a product developed by Ericsson to offer video/sound conferencing, screen recording, screen capture, and cloud-based storage together with the additional usefulness of

"atomic" checklist, genuine time bookmarking, accessible hyperlinked work area of substance, commented on screen catches, connections to supplemental material.

Ericsson's workers, suppliers and customers can utilize the product program as a way to associate and lead classes for VPWs and distinctive meetings.

### **Man in the middle attack:**

Something like 76 famous applications on Apple's iOS stage are vulnerable attack that could enable programmers to block and take information without being taken note.

### **Replay attack:**

Homekit device can prevent replay attack by default.

### **Ransomware:**

Apple says Icloud won't be hacked by a ransomware attack. Cause the device had remotely locked in exchange for ransom. [161]

## **5.6. Apple homekit**

### **DDos attack:**

Apple was generally late to the table with its HomeKit smart home stage. It was inventin 2014, and the first HomeKit-suitable smart device didn't begin rolling off until a year later. A major piece of that delay was likely the security requests AAPL put on producers, including the additional expense of a authentication chip every device requires. [162]

### **Blueborne attack:**

The older model of apple device can't take away the BlueBorneattack.below a list of the oldest device that can't discover this assault. [163]

- iPhone 4S and older
- iPad (third generation) and older



- iPad mini (1st generation) and older
- iPod touch (fifth generation) and older
- Apple TV (third generation) and older

However in the more modern version device can detect BlueBorne attack

### **Remote access using telnet:**

In apple homekit Device has remote access. A center hub is set up to the homekitdevice. By utilizing the home application the client can oversee or control the homekit accessories by iOS device or mac.

### **Man in the middle attack:**

The first-rate way to stay away of this will be to root the device and manually incapacitate it. Take a look at or update the embedded declarations with burpsuite's. This will be require a notably extra complex size of attack and if the device is jailbroken/rooted there are different attack vectors to ponder.

### **Ransomware attack:**

Apple has launched security update iOS 10.3.2 and macOS 10.12.5 on may additionally 15th that rolled out over 20 security fixes for iPhones and iPads and 30 protection someplace for Mac. The cyber-attack is extreme sufficient to make Apple patch up the vulnerability in iBooks for iOS and macOS. As soon as being attacked, iOS isn't as that secure as the customers have considered ever. New update is available now. So we can update to the latest iOS or macOS to fix the bugs.

## **5.7. Smartthing/Samsung**

### **DDoS attack:**

Watched a development of new reflex and improvement DDoS ambushes manhandling Internet of Things devices like smartthings on Samsung which that mishandles correspondences traditions. The data is as per the revelations of the report starting late issued by Arbor Networks related to DDoS ambush saw in Q3 2014. The SSDP tradition misused by peril performing

craftsmen are routinely used by such gadgets to speak with every other and to encourage practices with various types of hardware. The IoT gadgets revealed on the Internet are engaged by horrendous performing craftsmen that exchange off them to sort out critical real assaults against big business targets. [164][165]

#### **Blueborne attack:**

The BlueBorne weakness licenses remote software engineers to broaden full control upon Bluetooth-enabled gadgets withal while it isn't coordinated with the developer's gadget or perhaps set to definable mode. It's prepared to affect cell phones, medications, pcs, or possibly IoT contraptions. A settle for the BlueBorne weakness end up settled with the Sept 2017 assurance rebuilding, be that as it may, Samsung has ceased the territory on its gadgets with the August 2017 security fix. These updates are incorporated into microcode shapes that contain the letter 'T' inside the penult position. [166]

#### **Jamming attack:**

Experts found a blemish in the crucial ZigBee sorting out tradition that would allow attackers to stick correspondences on the framework in the midst of a break-in, thusly keeping security alarms from initiating. Samsung issued a fix for customers two or three months sometime later. [167]

#### **Remote access using telnet:**

Samsung's execution for the Android Radio Interface Layer (RIL), that handles interchanges for modem. At the same time as identifying Samsung's RIL to make its very own substitution, Kocialkowski determined the product utilizes the Samsung IPC convention to actualize RFS directions and perform far flung I/O sports. Which usage the Samsung IPC conference, for maximum part Intel XMM6160 and Intel XMM6260 modems.[168]

#### **Exploit kit attack:**

Investigators from Austria's Graz Technical college,who found that they may abuse the Meltdown weakness to attack Samsung gadgets.[169]

**Main in the middle attack:**

As per varela's exploration the MITM assault can screen the correspondence among the Samsung pc and Samsung servers enabling the aggressor to block a demand for an xml paper that take on the model id for which the drivers are being asked. Samsung executed a figured correspondence between the instrument and its servers and furthermore a confirmation system. [170]

**Relay attack:**

Samsung FAQ secured. "Samsung Pay and our associates respected this power hazard worth offered them to a super degree low likelihood of a productive token exchange assault. [171]

**Ransomware:**

Bug in Samsung they can't minimize Ransomware Attacks. [172]

**Side channel attack:**

Samsung built up any other rendition of a side channel attack to split the worldwide AES-CCMkey that Philips makes use of to encode and verify new firmware. [173]

**5.8. Kuru/Java****DDos attack:**

Memory and cpu advantages woodstox-focus asl are vulnerable against refusal of organization dos attacks. That shortcoming can be initiated when xml with a broad number of segments qualities or settled creates are passed to readerconfig.java causing cpu and memory usage.[174]

**Blueborne attack:**

The blueborne strike vector has a couple of series. Inside the primary spot hacker uncovers dynamic bluetooth relationship round which separate. Gadgets have avility to analyzed paying little mind to whether they may be not appropriate to discoverable mode. Resulting hackers gets the instrument's macintosh clue which is a first class identifier of that express device. Which means of experimenting with the device the hacker can recognize out which working procedure his harmed individual is using and manage his experience in like manner. The hacker will by

then abuse feebleness inside the execution of the bluetooth convention to monstrous degree.[175].

### **Jamming attack:**

optimal jamming attacks and system barrier approaches in remote sensor systems venture is a 2010 cse venture which is actualized in java stage. This task clarifies about sticking and barrier instrument is executed in java/osgi-base. [176]

### **Remote access using telnet:**

Apache activemqartemis is helpless against deserialization assaults. The jms self-command plots a get item technique on the javax.jms.object message magnificence. The apache artemis execution of this technique permits the deserialization of things from untrusted assets. There are some spots within which apache artemis utilizes this get item approach. Those elements may also on this manner be defenseless against a distant code execution assaults. for this vulnerability to be exploited the sender of the listed off message must be confirmed and approved an honest thanks to sending the message to the artemis representative and influenced coaching device directions gift at the artemis magnificence manner.[177]

### **Exploit kit attack:**

We sort abuses in our malware reference book by the stage they target. For instance exploit java/cve-2013-1489.a is an adventure that objectives a helplessness in java. Basic vulnerabilities and exposures cve is utilized by numerous security programming merchants. The undertaking gives every defenselessness an extraordinary number for instance cve-2016-0778. The bit 2016 alludes to the year the helplessness was found. The 0778 is a one of a kind id for this explicit weakness.[178]

### **Ransomware:**

java is not defined via the manner wherein it acknowledges the files are defiled in its assault in order to be set apart with the report expansion '.java ' introduced as a ways as practicable of the prompted files' names. The java not-dharma ransomware changed into first seen from april of 2018 and the java not-dharma ransomware indicate to do a ransomwaretrojan assault like

numerous ransomware. It is being utilized to target non-public ventures and internet servers right now. [179]

**Side channel attack:**

Vulnerabilities in java/osgi bundle interactions assaults against java segments at the case of osgi group's scientific categorizations .a portion of the issues it addresses by changing the sort arrangement of java. [180].

**Table.1 comparative security's analysis**

<b>Attack/Cloud</b>	<b>DoS/DDoS Attack</b>	<b>Blue Borne</b>	<b>Jamming Attack</b>	<b>Remote access using Attack</b>	<b>Sybil Attack</b>	<b>Exploit Kit Attack</b>	<b>Man in The middle attack</b>	<b>Replay Attack</b>	<b>Ransomware Attack</b>	<b>Side channel Attack</b>
<b>AWS(Amazon Web Service)</b>	Yes	No	Yes	There Is no access	No Result	Yes	Yes	No Result	No	Yes
<b>ARWmbed</b>	Yes	No Result	Yes	No Data Encrypted	No Result	No Result	Yes	Yes	No Result	Attacked But can be deleted
<b>Azure IoT Suite</b>	Yes	No	Yes	Remotely login	Yes	Yes	No	Yes	Yes	Yes
<b>Brillo/Weave</b>	Yes	Yes	Yes	No Result	Yes	Yes	Yes	Yes	Yes	Yes
<b>Calvin</b>	Yes	No Result	No Result	Remotely login	No Result	No Result	No	Yes	Yes	No Result
<b>Home Kit</b>	Yes	Yes	No Result	Yes	No Result	No Result	No	No Result	Yes	No Result
<b>Kura</b>	Yes	Yes	Yes	Yes	No Result	No	Yes	Yes	No	No
<b>Smarthing</b>	Yes	Yes	Yes	No	No Result	Yes	No Result	No Result	No	No

## **Chapter 6**

### **Conclusion**

The IoT market is growing rapidly and as a consequence, the attention has shifted from proposing single IoT elements and protocols towards application platforms in order to identify frameworks supporting the standard IoT suites of regulations and protocols. This study has covered a subset of commercially available frameworks and platforms for developing industrial and consumer-based IoT applications. The selected frameworks have the same design philosophy in terms of identifying cloud-based applications by centralizing distributed data sources. However, they followed various approaches in order to apply this philosophy. A comparative analysis of the frameworks was conducted based on the architecture, hardware compatibility, software requirements, and security. We highlighted on the security measures of each framework as verifying the various security features and immunity against attacks is one of the most important contemporary issues facing the Internet of Things.

## References

- [1] Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N., & Thomas, T. (2010). LTE-advanced: next-generation wireless broadband technology. *IEEE wireless communications*, 17(3). [Accessed time:9.09 AM 12-Oct-18]
- [2] Al-Fuqaha A , Guizani M , Mohammadi M , Aledhari M , Ayyash M . Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Commun Surveys Tutorials* 2015; 17(4):2347–76. . [Accessed time: 9.12 AM 12-Oct-18]
- [3] Derhamy H, Eliasson J, Delsing J, Priller P. A survey of commercial frame- works for the internet of things. In: 2015 IEEE 20th conference on emerging technologies & factory automation (ETFA). IEEE; 2015. p. 1–8. [Accessed time: 9.17 AM 12-Oct-18]
- [4] Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE Wireless Communications*, 20(6), 91-98. [Accessed time: 10.19 PM 12-Oct-18]
- [5] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, 4(5), 1250-1258. [Accessed time: 10.25 PM 12-Oct-18]
- [6] Kumar JS, Patel DR . A survey on internet of things: security and privacy is- sues. *Int J Comput Appl* 2014;90(11). [Accessed time: 11.02 PM 12-Oct-18]
- [7] Vikas, B. O. (2015). Internet of things (iot): A survey on privacy issues and security. *International Journal of Scientific Research in Science, Engineering and Technology*, 1(3), 168-173. [Accessed time: 11.22 PM 12-Oct-18]
- [8] Vikas, B. O. (2015). Internet of things (iot): A survey on privacy issues and security. *International Journal of Scientific Research in Science, Engineering and Technology*, 1(3), 168-173. [Accessed time: 11.22 PM 12-Oct-18]
- [9] Borgohain T., Kumar U., Sanyal S. Survey of security and privacy issues of in- ternet of things. arXiv:150102211 2015. [Accessed time: 10.05 AM 14-Oct-18]
- [10] Bouij-Pasquier I , El Kalam AA , Ouahman AA , De Montfort M . A security frame- work for internet of things. In: International conference on cryptology and network security. Springer; 2015. p. 19–31. [Accessed time: 10.12 AM 14-Oct-18]
- [11] Brown, Eric (13 September 2016). "Who Needs the Internet of Things?" Linux.com. Retrieved 23 October 2016. [Accessed time: 10.18 AM 14-Oct-18]
- [12] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P. ... & Alexander, R. (2012). *RPL: IPv6 routing protocol for low-power and lossy networks* (No. RFC 6550). [Accessed time: 10.23 AM 14-Oct-18]
- [13] Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solution. [Accessed time: 10.45 AM 14-Oct-18]
- [14] Odelu, V., Das, A. K., Khan, M. K., Choo, K. K. R., & Jo, M. (2017). Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts. *IEEE Access*, 5, 3273-3283. [Accessed time: 11.22 AM 14-Oct-18]



- [15] Ab Malek, M. S. B., Ahmadon, M. A. B., Yamaguchi, S., & Gupta, B. B. (2016, October). On privacy verification in the IoT service based on PN 2. In *Consumer Electronics, 2016 IEEE 5th Global Conference on* (pp. 1-4). IEEE. [Accessed time: 11.30 AM 14-Oct-18]
- [16] Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S. R., Rahmani, A. M., & Liljeberg, P. (2016). On the feasibility of attribute-based encryption on internet of things devices. *IEEE Micro*, 36(6), 25-35. [Accessed time: 11.40 AM 14-Oct-18]
- [17] B.-C. Chifor, I. Bica, V.-V. Patriciu, F. Pop, A security authorization scheme for smart home Internet of Things devices, *Future Gener. Comput. Syst.* (2017). <http://dx.doi.org/10.1016/j.future.2017.05.048>. [Accessed time: 11.45 AM 14-Oct-18]
- [18] Mai, V., & Khalil, I. (2017). Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. *Future Generation Computer Systems*, 72, 327-338. [Accessed time: 09.02 AM 15-Oct-18]
- [19] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84, 25-37. [Accessed time: 09.10 AM 15-Oct-18]
- [20] Wan, J., Canedo, A., & Al Faruque, M. A. 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). [Accessed time: 09.15 AM 15-Oct-18]
- [21] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on* (pp. 257-260). IEEE. [Accessed time: 09.20 AM 15-Oct-18]
- [22] Specification Z. Zigbee alliance. URL: <http://www.zigbee.org> 2006; 558. [Accessed time: 09.50 AM 14-Oct-18]
- [23] Z-Wave. Z-wave public specification. <http://z-wave.sigmadesigns.com/design-z-wave-public-specification>. [Accessed time: 11.15 AM 14-Oct-18]
- [24] Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9), 11734-11753. [Accessed time: 11.25 AM 14-Oct-18]
- [25] Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N., & Thomas, T. (2010). LTE-advanced: next-generation wireless broadband technology. *IEEE wireless communications*, 17(3). [Accessed time: 11.45 AM 14-Oct-18]
- [26] Dierks, T., & Rescorla, E. (2008). *The transport layer security (TLS) protocol version 1.2* (No. RFC 5246). [Accessed time: 12.15 PM 14-Oct-18]
- [27] Shelby, Z., Hartke, K., & Bormann, C. (2014). *The constrained application protocol (CoAP)* (No. RFC 7252). [Accessed time: 12.30 PM 14-Oct-18]
- [28] Locke D. Mq telemetry transport (mqtt) v3.1 protocol specification. <http://www.ibm.com/developerworks/webservices/library/ws-mqtt/index.html> On- line; [Accessed time: 1.15 PM 14-Oct-18]
- [29] Saint-Andre, P. (2011). *Extensible messaging and presence protocol (XMPP): Core* (No. RFC 6120). [Accessed time: 2.05 PM 14-Oct-18]

- [30] Vinoski, S. (2006). Advanced message queuing protocol. *IEEE Internet Computing*, 10(6). [Accessed time: 08.15 AM 17-Oct-18]
- [31] Group O.M. Data distribution service v1.2. <http://www.omg.org/spec/DDS/1.2/>. [Accessed time: 08.20 AM 17-Oct-18]
- [32] <https://www.linkedin.com/pulse/thesis-ideas-internet-things-advantages-applications-manpreet-kaur/?fbclid=IwAR3DTh778bpW0xCZVHZRgcyi3gF8gPZ-A2Yqv568KxSNhvigtmBNWNxKpQc>. [Accessed time: 08.35 AM 17-Oct-28]
- [33] <https://www.semtech.com/applications/internet-of-things>. [Accessed time: 08.45 AM 17-Oct-18]
- [34] <https://dzone.com/articles/top-10-uses-of-the-internet-of-things>. [Accessed time: 09.45 AM 17-Oct-18]
- [35] <https://www.linkedin.com/pulse/thesis-ideas-internet-things-advantages-applications-manpreet-kaur/?fbclid=IwAR3DTh778bpW0xCZVHZRgcyi3gF8gPZ-A2Yqv568KxSNhvigtmBNWNxKpQc>. [Accessed time: 10.00 AM 17-Oct-18]
- [36] Amazon. Aws iot framework. <https://aws.amazon.com/iot>. [Accessed time: 10.45 AM 17-Oct-18]
- [37] Amazon. Amazon dynamodb. <https://aws.amazon.com/dynamodb>. [Accessed time: 11.45 AM 17-Oct-18]
- [38] Amazon. Amazon s3. <https://aws.amazon.com/s3>. [Accessed time: 12.45 PM 17-Oct-18]
- [39] Amazon. Amazon machine learning. <https://aws.amazon.com/machine-learning>. [Accessed time: 1.45 PM 17-Oct-18]
- [40] Hunkeler, U., Truong, H. L., & Stanford-Clark, A. (2008, January). MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks. In *Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on* (pp. 791-798). IEEE. [Accessed time: 8.45 PM 20-Oct-18]
- [41] Dierks T., Rescorla E. The transport layer security (tls) protocol version 1.2. <https://www.ietf.org/rfc/rfc5246.txt>. [Accessed time: 9.45 PM 20-Oct-18]
- [42] Amazon. Amazon iot protocols. <http://docs.aws.amazon.com/iot/latest/developerguide/protocols.html>. [Accessed time: 11.45 PM 20-Oct-18]
- [43] Amazon. Amazon lambda. <https://aws.amazon.com/lambda>. [Accessed time: 8.45 AM 22-Oct-18]
- [44] Amazon. Amazon management console. <https://aws.amazon.com/console>. [Accessed time: 8.59 AM 22-Oct-18]
- [45] Amazon. Amazon kinesis. <https://aws.amazon.com/kinesis>. [Accessed time: 9.45 AM 22-Oct-18]
- [46] Amazon. Amazon command line interface. <https://aws.amazon.com/cli>. [Accessed time: 10.45 AM 22-Oct-18]
- [47] Amazon. Amazon cognito identities. <http://docs.aws.amazon.com/iot/latest/developerguide/cognito-identities.html>. [Accessed time: 11.15 AM 22-Oct-18]
- [48] Amazon. Iam users, groups, and roles. <http://docs.aws.amazon.com/iot/latest/>

- developerguide/iam- users- groups- roles.html. [Accessed time: 11.35 AM 22-Oct-18]
- [49] Cooper D. Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. <https://tools.ietf.org/html/rfc5280>. [Accessed time: 12.45 PM 22-Oct-18]
- [50] Amazon. X.509 certificates. <http://docs.aws.amazon.com/iot/latest/developerguide/x509-certs.html>. [Accessed time: 1.15 PM 22-Oct-18]
- [51] Amazon. Aws identity and access management (iam). <https://aws.amazon.com/iam/>. [Accessed time: 2.03 PM 22-Oct-18]
- [52] Amazon. Amazon cognito. <https://aws.amazon.com/cognito/>. [Accessed time: 2.45 PM 22-Oct-18]
- [53] Amazon. Signature version 4 signing process. <http://docs.aws.amazon.com/general/latest/gr/signature-version-4.html>. [Accessed time: 8.45 AM 25-Oct-18]
- [54] Amazon. Aws authorization. <http://docs.aws.amazon.com/iot/latest/developerguide/authorization.html>. [Accessed time: 9.45 AM 25-Oct-18]
- [55] ARM. Arm mbed iot device platform. <http://www.arm.com/products/iot-solutions/mbed-iot-device-platform>. [Accessed time: 9.05 AM 25-Oct-18]
- [56] ARM. mbed device connector. <https://www.mbed.com/en/platform/cloud/mbed-device-connector-service/>. [Accessed time: 10.15 AM 25-Oct-18]
- [57] ARM. mbed os. <https://www.mbed.com/en/platform/mbed-os/>. [Accessed time: 10.45 AM 25-Oct-18]
- [58] mbed A. mbed client. <https://www.mbed.com/en/platform/mbed-client/>. [Accessed time: 11.45 AM 25-Oct-18]
- [59] mbed A. mbed device connector. <https://docs.mbed.com/docs/getting-started-with-mbed-device-connector/en/latest/Connector-intro/>. [Accessed time: 12.45 PM 25-Oct-18]
- [60] mbed A. mbed cloud. <https://cloud.mbed.com/>. [Accessed time: 1.45 PM 25-Oct-18]
- [61] mbed A. mbed security. <https://www.mbed.com/en/technologies/security/>. [Accessed time: 2.45 PM 25-Oct-18]
- [62] mbed A. mbed uvisor. <https://www.mbed.com/en/technologies/security/uvisor/>. [Accessed time: 3.45 PM 25-Oct-18]
- [63] mbed A. mbed tls. <https://tls.mbed.org/core-features>. [Accessed time: 4.23 PM 25-Oct-18]
- [64] Microsoft. Tap into the internet of your things with azure iot suite. <https://www.microsoft.com/en-us/cloud-platform/internet-of-things-azure-iot-suite>. [Accessed time: 5.45 PM 25-Oct-18]
- [65] Azure M. Microsoft azure iot reference architecture. <https://azure.microsoft.com/en-us/updates/microsoft-azure-iot-reference-architecture-available/>. [Accessed time: 6.45 PM 25-Oct-18]
- [66] Azure M. Azure iot hub. <https://azure.microsoft.com/en-us/services/iot-hub/>. [Accessed time: 7.45 PM 25-Oct-18]
- [67] Azure M. Communication protocols. <https://azure.microsoft.com/en-us/documentation/articles/iot-hub-devguide-messaging/#communication-protocols>. [Accessed time: 9.45 PM 25-Oct-18]

- [68] Azure M. Azure iot protocol gateway. <https://azure.microsoft.com/en-us/documentation/articles/iot-hub-protocol-gateway/>. [Accessed time: 10.45 PM 25-Oct-18]
- [69] Azure M. Azure products. <https://azure.microsoft.com/services/>. [Accessed time: 11.45 PM 25-Oct-18]
- [70] Microsoft. Power bi. <https://powerbi.microsoft.com>. [Accessed time: 8.23 AM 28-Oct-18]
- [71] Microsoft. Security development lifecycle. <https://www.microsoft.com/en-us/sdl/default.aspx>. [Accessed time: 9.23 AM 28-Oct-18]
- [72] Microsoft. Operational security assurance. <https://www.microsoft.com/en-us/SDL/OperationalSecurityAssurance> . [Accessed time: 10.23 AM 28-Oct-18]
- [73] Azure M. Internet of things security from the ground up. <https://azure.microsoft.com/en-us/documentation/articles/iot-hub-security-ground-up/> . [Accessed time: 10.30 AM 28-Oct-18]
- [74] Azure M. What is azure active directory. <https://azure.microsoft.com/en-us/documentation/articles/active-directory-what-is/>. [Accessed time: 11.23 AM 28-Oct-18]
- [75] Azure M. Documentdb. <https://azure.microsoft.com/en-us/services/documentdb/>. [Accessed time: 12.23 PM 28-Oct-18]
- [76] Google. Brillo. <https://developers.google.com/brillo/>. [Accessed time: 12.23 PM 28-Oct-18]
- [77] Google. Weave. <https://developers.google.com/weave/>. [Accessed time: 1.23 PM 28-Oct-18]
- [78] Gargenta A. Deep dive into android ipc/binder framework. AnDevCon: The Android developer conference; 2012. [Accessed time: 2.23 PM 28-Oct-18]
- [79] Google. Ota updates. <https://source.android.com/devices/tech/ota/>. [Accessed time: 3.23 PM 28-Oct-18]
- [80] MSV J. Google brillo vs. apple homekit: The battleground shifts to iot. <http://www.forbes.com/sites/janakirammsv/2015/10/29/google-brillo-vs-apple-homekit-the-battleground-shifts-to-iot/#484c33674cac>. [Accessed time: 4.33 PM 28-Oct-18]
- [81] Intel. Getting started with brillo on the intel edison board. <https://software.intel.com/en-us/articles/getting-started-with-brillo-on-the-intel-edison-board>. [Accessed time: 5.03 PM 28-Oct-18]
- [82] Android. Hardware-backed keystore. <https://source.android.com/security/keystore> . [Accessed time: 6.23 PM 28-Oct-18]
- [83] Ericsson. Open source release of iot app environment calvin. <https://www.ericsson.com/research-blog/cloud/open-source-calvin/> . [Accessed time: 8.23 PM 28-Oct-18]
- [84] Morrison JP. Flow-based programming, 2Nd edition: a new approach to application development. Paramount, CA: CreateSpace; 2010. ISBN 1451542321, 9781451542325. [Accessed time: 9.23 PM 28-Oct-18]
- [85] Hewitt C. Actor model of computation: scalable robust information systems. arXiv:10081459 2010;. [Accessed time: 10.23 PM 28-Oct-18]

- [86] Ericsson. A closer look at calvin. [https://www.ericsson.com/research-blog/ cloud/closer-look- calvin/](https://www.ericsson.com/research-blog/cloud/closer-look-calvin/). [Accessed time: 11.23 PM 28-Oct-18]
- [87] Ericsson. Security in calvin. <https://github.com/EricssonResearch/calvin-base/wiki/Security/>. [Accessed time: 8.23 AM 29-Oct-18]
- [88] Apple. The smart home just got smarter. <http://www.apple.com/ios/home/>. [Accessed time: 8.28 AM 29-Oct-18]
- [89] Apple. About bonjour. <https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/NetServices/Introduction.html>. [Accessed time: 9.23 AM 29-Oct-18]
- [90] Apple. icloud. <http://www.apple.com/lae/icloud/>. [Accessed time: 10.23 AM 29-Oct-18]
- [91] Apple. Mfi program. <https://developer.apple.com/programs/mfi/>. [Accessed time: 11.23 AM 29-Oct-18]
- [92] Apple. ios security. [http://www.apple.com/business/docs/iOS \\_Security \\_ Guide. Pdf](http://www.apple.com/business/docs/iOS_Security_Guide.Pdf). [Accessed time: 12.02 PM 02-Nov-18]
- [93] Bernstein, D. J., Duif, N., Lange, T., Schwabe, P., & Yang, B. Y. (2011, September). High-speed high-security signatures. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 124-142). Springer, Berlin, Heidelberg. [Accessed time: 12.05 PM 02-Nov-18]
- [94] Bernstein D. A state-of-the-art diffie-hellman function. <https://cr.yp.to/ecdh>. Html. [Accessed time: 12.20 PM 02-Nov-18]
- [95] Snow, K. Z., Monrose, F., Davi, L., Dmitrienko, A., Liebchen, C., & Sadeghi, A. R. (2013, May). Just-in-time code reuse: On the effectiveness of fine-grained address space layout randomization. In *Security and Privacy (SP), 2013 IEEE Symposium on* (pp. 574-588). IEEE. [Accessed time: 12.25 PM 02-Nov-18]
- [96] Organization E. Kura framework. <http://www.eclipse.org/kura/>. [Accessed time: 1.02 PM 02-Nov-18]
- [97] Organization E. Kura framework. <http://wiki.eclipse.org/Kura>. [Accessed time: 1.10 PM 02-Nov-18]
- [98] Organization E. Kura - osgi-based application framework for m2m service gateways. <http://www.eclipse.org/proposals/technology.kura/>. [Accessed time: 1.23 PM 02-Nov-18]
- [99] Organization E. Mqtt and coap, iot protocols. [http://www.eclipse.org/ community/eclipse \\_newsletter/2014/february/article2.ph p](http://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php). [Accessed time: 1.48 PM 02-Nov-18]
- [100] Organization E. Kura - raspberry pi quick start. [http://eclipse.github.io/kura/ doc/raspberry-pi- quick- start.html](http://eclipse.github.io/kura/doc/raspberry-pi-quick-start.html) . [Accessed time: 1.55 PM 02-Nov-18]
- [101] Organization E. Kura - beaglebone quick start. [http://eclipse.github.io/kura/ doc/beaglebone-quick- start.html](http://eclipse.github.io/kura/doc/beaglebone-quick-start.html) . [Accessed time: 5.20 PM 02-Nov-18]
- [102] Organization E. Kura - hardware targets. [http://eclipse.github.io/kura/ref/ hardware-targets.html](http://eclipse.github.io/kura/ref/hardware-targets.html) . [Accessed time: 5.22 PM 02-Nov-18]
- [103] Organization E. Eclipse paho. <http://www.eclipse.org/paho/>. [Accessed time: 5.32 PM 02-Nov-18]

- [104] SmartThings. Smartthings documentation. <http://docs.smartthings.com/en/latest/>. [Accessed time: 5.37 PM 02-Nov-18]
- [105] SmartThings. Cloud and lan-connected devices. <http://docs.smartthings.com/en/latest/cloud-and-lan-connected-device-types-developers-guide/>. [Accessed time: 5.44 PM 02-Nov-18]
- [106] SmartThings. Smartthings architecture. <http://docs.smartthings.com/en/latest/architecture/index.html>. [Accessed time: 5.58 PM 02-Nov-18]
- [107] Kawaguchi K. Groovy sandbox. <http://groovy-sandbox.kohsuke.org/>. [Accessed time: 10.32 PM 02-Nov-18]
- [108] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 636-654). IEEE.
- [109] [https://en.wikipedia.org/wiki/Denial-of-service\\_attack](https://en.wikipedia.org/wiki/Denial-of-service_attack). [Accessed time: 10.37 PM 02-Nov-18]
- [110] <https://www.igi-global.com/chapter/jamming-attacks-countermeasures-wireless-sensor/41122>. [Accessed time: 10.38 PM 02-Nov-18]
- [111] <https://armis.com/blueborne/>. [Accessed time: 10.41 PM 02-Nov-18]
- [112] Christoph Meinel; Harald Sack. *Internetworking: Technological Foundations and Applications*. X.media.publishing, 2013. p. 57. ISBN 3642353916. [Accessed time: 11.05 AM 05-Nov-18]
- [113] <https://www.infoworld.com/article/2625148/intrusion-detection/hackers-using-telnet-to-attack-corporate-servers.html>. [Accessed time: 11.11 AM 05-Nov-18]
- [114] Lynn Neary (20 October 2011). Real 'Sybil' Admits Multiple Personalities Were Fake. NPR. Retrieved 8 February 2017. [Accessed time: 11.19 AM 05-Nov-18]
- [115] Douceur, John R (2002). "The Sybil Attack". *Peer-to-Peer Systems. Lecture Notes in Computer Science*. 2429. pp. 251–60. doi:10.1007/3-540-45748-8\_24. ISBN 978-3-540-44179-3. [Accessed time: 11.42 AM 05-Nov-18]
- [116] Oram, Andrew. *Peer-to-peer: harnessing the benefits of a disruptive technology*. [Accessed time: 12.22 PM 05-Nov-18]
- [117] <https://www.quora.com/How-does-the-Sybil-attack-work-How-does-it-initiate-the-attack>. [Accessed time: 12.31 PM 05-Nov-18]
- [118] <https://whatis.techtarget.com/definition/crimeware-kit-attack-kit>. [Accessed time: 12.42 PM 05-Nov-18]
- [119] <https://blog.barkly.com/how-exploit-kits-work>. [Accessed time: 12.54 PM 05-Nov-18]
- [120] Tanmay Patange (November 10, 2013). "How to defend yourself against MITM or Man-in-the-middle attack". [Accessed time: 5.10 PM 05-Nov-18]
- [121] Tanmay Patange (November 10, 2013). "How to defend yourself against MITM or Man-in-the-middle attack". [Accessed time: 5.10 PM 05-Nov-18]
- [122] <https://www.ssh.com/attack/man-in-the-middle>. [Accessed time: 6.21 PM 05-Nov-18]
- [123] Malladi, S., Alves-Foss, J., & Heckendorn, R. B. (2002). *On preventing replay attacks on*

- security protocols*. IDAHO UNIV MOSCOW DEPT OF COMPUTER SCIENCE. [Accessed time: 6.23 PM 05-Nov-18]
- [124] <https://www.sitepoint.com/how-to-prevent-replay-attacks-on-your-website/>. [Accessed time: 2.20 PM 11-Nov-18]
- [125] Young, A., & Yung, M. (1996, May). Cryptovirology: Extortion-based security threats and countermeasures. In *sp* (p. 0129). IEEE. [Accessed time: 2.22 PM 11-Nov-18]
- [126] <https://www.cybereason.com/blog/how-does-ransomware-work>. [Accessed time: 2.28 PM 11-Nov-18]
- [127] Chen, S., Wang, R., Wang, X., & Zhang, K. (2010, May). Side-channel leaks in web applications: A reality today, a challenge tomorrow. In *2010 IEEE Symposium on Security and Privacy*(pp. 191-206). IEEE. [Accessed time: 5.02 PM 11-Nov-18]
- [128] [https://www.researchgate.net/publication/267764296\\_Cache\\_Side-Channel\\_Attacks\\_in\\_Cloud\\_Computing](https://www.researchgate.net/publication/267764296_Cache_Side-Channel_Attacks_in_Cloud_Computing). [Accessed time: 6.18 PM 17-Nov-18]
- [129] <https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>. [Accessed time: 6.19 PM 17-Nov-18]
- [130] <://www.amazon.co.uk/Enhanced-Disassembling-Schemes-Jamming-Prevention/dp/3659443727>. [Accessed time: 6.37 PM 17-Nov-18]
- [131] <https://vceguide.com/does-amazon-rds-allow-direct-host-access-via-telnet-secure-shell-ssh-or-windows-remote-desktop-connection/>. [Accessed time: 8.18 PM 17-Nov-18]
- [132] <https://securityboulevard.com/2018/03/new-attack-vectors-brought-by-the-cloud-and-aws/>. [Accessed time: 9.28 PM 17-Nov-18]
- [133] [https://d1.awsstatic.com/whitepapers/Security/Networking\\_Security\\_Whitepaper.pdf](https://d1.awsstatic.com/whitepapers/Security/Networking_Security_Whitepaper.pdf). [Accessed time: 10.18 PM 27-Nov-18]
- [134] <https://www.techrepublic.com/article/unsecured-amazon-s3-buckets-are-prime-cloud-target-for-ransomware-attacks/>. [Accessed time: 10.23 PM 27-Nov-18]
- [135] <https://aws.amazon.com/security/security-bulletins/AWS-2018-019/>. [Accessed time: 11.29 PM 27-Nov-18]
- [136] <https://www.itworld.com/article/3136307/internet-of-things/to-solve-iot-security-look-at-the-big-picture-arm-says.html> . [Accessed time: 12.12 AM 28-Nov-18]
- [137] [https://www.researchgate.net/publication/301705986\\_An\\_Embedded\\_Sensor\\_Node\\_Microcontroller\\_with\\_Crypto-Processors](https://www.researchgate.net/publication/301705986_An_Embedded_Sensor_Node_Microcontroller_with_Crypto-Processors). [Accessed time: 10.18 PM 02-Dec-18]
- [138] <https://os.mbed.com/forum/mbed/topic/934/?page=1#comment-4523>. [Accessed time: 10.21 PM 02-Dec-18]
- [139] [https://www.theregister.co.uk/2017/08/31/arms\\_embedded\\_tls\\_library\\_patched\\_to\\_fix\\_m\\_bug/](https://www.theregister.co.uk/2017/08/31/arms_embedded_tls_library_patched_to_fix_m_bug/) . [Accessed time: 11.38 PM 02-Dec-18]
- [140] <https://os.mbed.com/users/electronichamsters/notebook/ble-advertisement-replay-attack--spoof-detection/>. [Accessed time: 10.26 PM 03-Dec-18]
- [141] <https://tls.mbed.org/discussions/crypto-and-ssl/aes-implementation-resistant-to-side-channel-analysis-attacks>. [Accessed time: 12.28 PM 04-Dec-18]
- [142] <https://azure.microsoft.com/en-us/services/ddos-protection/>. [Accessed time: 10.26 PM 05-

Dec-18]

- [143] <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8628>. [Accessed time: 10.29 PM 05-Dec-18]
- [144] <https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-ground-up>. [Accessed time: 10.33 PM 05-Dec-18]
- [145] <https://feedback.azure.com/forums/907045-azure-iot-edge/suggestions/34484857-remote-login-to-iot-gateway>. [Accessed time: 10.41 PM 05-Dec-18]
- [146] <https://www.networkworld.com/article/3067358/security/how-microsoft-keeps-the-bad-guys-out-of-azure.html>. [Accessed time: 10.49 PM 05-Dec-18]
- [147] <https://www.symantec.com/en/au/security-center/vulnerabilities/writeup/104070>. [Accessed time: 10.57 PM 05-Dec-18]
- [148] [https://www.theregister.co.uk/2018/10/10/token\\_binding\\_protocol\\_rfc](https://www.theregister.co.uk/2018/10/10/token_binding_protocol_rfc). [Accessed time: 11.02 PM 05-Dec-18]
- [149] <https://azure.microsoft.com/sv-se/blog/petya-ransomware-prevention-detection-in-azure-security-center>. [Accessed time: 6.20 PM 08-Dec-18]
- [150] <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/mitigate-se>. [Accessed time: 6.28 PM 08-Dec-18]
- [151] <https://cloud.google.com/security/>. [Accessed time: 6.38 PM 08-Dec-18]
- [152] <https://www.theandroidsoul.com/blueborne-attack-and-android-everything-you-need-to-know/>. [Accessed time: 6.54 PM 08-Dec-18]
- [153] <https://patents.google.com/patent/US20090325478>. [Accessed time: 7.20 PM 08-Dec-18]
- [154] <https://www.mdpi.com/2073-8994/9/3/35>. [Accessed time: 7.26 PM 08-Dec-18]
- [155] <https://whatis.techtarget.com/definition/crimeware-kit-attack-kit>. [Accessed time: 10.20 PM 08-Dec-18]
- [156] <https://www.v3.co.uk/v3-uk/news/3017079/google-chrome-to-provide-man-in-the-middle-attack-warnings>. [Accessed time: 10.22 PM 08-Dec-18]
- [157] [https://en.wikipedia.org/wiki/Replay\\_attack](https://en.wikipedia.org/wiki/Replay_attack). [Accessed time: 10.25 PM 08-Dec-18]
- [158] <https://www.quora.com/Android-operating-system-How-do-I-block-Ransomware-attacks-on-my-Android-tablet>. [Accessed time: 10.34 PM 08-Dec-18]
- [159] <https://www.jungledisk.com/blog/2017/12/28/be-aware-of-side-channel-attacks/>. [Accessed time: 10.43 PM 08-Dec-18]
- [160] <https://www.ericsson.com/en/ericsson-technology-review/archive/2015/identifying-and-addressing-the-vulnerabilities-and-security-issues-of-sdn>. [Accessed time: 10.52 PM 08-Dec-18]
- [161] <https://www.makeuseof.com/tag/cloud-drive-ransomware/>. [Accessed time: 10.58 PM 08-Dec-18]
- [162] <https://investorplace.com/2016/10/how-apple-inc-aapl-homekit-protects-against-ddos-attacks/>. [Accessed time: 7.21 PM 14-Dec-18]
- [163] <https://www.intego.com/mac-security-blog/what-is-blueborne-an-apple-device-faq/>. [Accessed time: 7.27 PM 14-Dec-18]



- [164]<https://www.cybercureme.com/bugs-in-samsung-iot-hub-leave-smart-home-open-to-attack>.  
[Accessed time: 7.33 PM 14-Dec-18]
- [165]<http://iotworm.eyalro.net/>. [Accessed time: 7.43 PM 14-Dec-18]
- [166]<https://www.sammobile.com/2017/09/25/samsung-rolls-security-patches-fix-blueborne-vulnerability/>. [Accessed time: 7.48 PM 14-Dec-18]
- [167]<https://www.techhive.com/article/3064372/home-tech/samsung-smartthings-vulnerability-lets-hackers-make-their-own-house-keys.html>. [Accessed time: 9.33 PM 14-Dec-18]
- [168]<https://www.zdnet.com/article/backdoor-in-samsung-galaxy-devices-allows-remote-access-to-data/>. [Accessed time: 9.54 PM 14-Dec-18]
- [169]<https://www.silicon.co.uk/mobility/smartphones/samsung-s7-meltdown-exploit-235753>.  
[Accessed time: 8.20 PM 23-Dec-18]
- [170][www.securew2.com/blog/samsung-keyboards-vulnerable-to-man-in-the-middle-exploit](http://www.securew2.com/blog/samsung-keyboards-vulnerable-to-man-in-the-middle-exploit).  
[Accessed time: 8.23 PM 23-Dec-18]
- [171]<https://www.tomsguide.com/us/samsung-pay-tokens-vulnerable,news-23159.html>.  
[Accessed time: 8.35 PM 23-Dec-18]
- [172][https://www.researchgate.net/publication/326609660\\_A\\_taxonomy\\_of\\_cyber-physical\\_threats\\_and\\_impact\\_in\\_the\\_smart\\_home](https://www.researchgate.net/publication/326609660_A_taxonomy_of_cyber-physical_threats_and_impact_in_the_smart_home). [Accessed time: 9.26 PM 23-Dec-18]
- [173]<http://iotworm.eyalro.net/>. [Accessed time: 10.25 PM 23-Dec-18]
- [174]<https://www.sourceclear.com/vulnerability-database/security/denial-service-dos-memory-cpu/java/sid-833>. [Accessed time: 10.34 PM 23-Dec-18]
- [175]<https://security.stackexchange.com/questions/169527/what-is-blueborne-and-how-to-protect-myself>. [Accessed time: 8.28 PM 25-Dec-18]
- [176]<http://1000projects.org/optimal-jamming-attacks-and-network-defense-policies-in-wireless-sensor-networks-project.html>. [Accessed time: 8.29 PM 25-Dec-18]
- [177]<https://www.sourceclear.com/vulnerability-database/security/remote-code-execution-through/java/sid-2786>. [Accessed time: 9.22 PM 25-Dec-18]
- [178]<https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware>. [Accessed time: 10.28 PM 25-Dec-18]
- [179]<https://www.enigmasoftware.com/javanotdharmaransomware-removal/>. [Accessed time: 10.45 PM 25-Dec-18]
- [180]<https://crypto.stackexchange.com/questions/48867/timing-safety-in-jvm-languages/48877#48877>. [Accessed time: 10.53 PM 25-Dec-18]
- [181]<https://apiumhub.com/tech-blog-barcelona/iot-security-issues/>. [Accessed time: 11.29 PM 25-Dec-18]