IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY IN INTERNET OF THINGS(IOT)

[1]Vedavyas Paritala, [2]Venkatachalapathi K V, [3]Pruthvi Raj N N, [4]Manjula M

[1]Student, [2]Studen, [3]Studen, [4]Assistant Proffesor

[1]Computer Science and Engineering,

[1]Atria Institute of Technology, Bangalore, India

Abstract: **Billions of IOT (Internet of things) devices interfacing with the Network and these numbers is raising day by day. As a so far advancing development, IOT devices are used in different fields, for instance, cultivating, therapeutic administrations, manufacturing, imperativeness, retailing and coordination's. Internet of things are changing the world and the way in which we live and think. Regardless, different Internet of things devices have its own designing and facing different types of issues in the dissimilar layers of Internet of things, for instance, illegal entree to the data, copying of the devices, DDOS attacks, etc. IOT gadgets are increasingly defenseless against assaults since it is straightforward and some safety efforts can't be actualized. We examine the protection and safety experiments in the internet of things and review on the comparing answers for upgrade the safety of Internet of things engineering convention. Concentrate more on the safety and defense on IOT and support to advance the improvement of IOT (Internet of things).**

Index Terms **- safety, confidentiality, IOT (internet of things), protocol.**

I. INTRODUCTION

There is a rising development, Internet of Things (IOT) have the described framework each and every device that connected to the Internet. Survey says that in 2020 there are 30 billion devices which are connected to the internet in the world. These numbers will increase to the 75 billion in the year of 2025. The IOT will have the business of 300 billion pay by 2020. IOT devices are in the different fields, for instance, cultivating, social protection, manufacturing, essentialness, transaction and transport. Likewise, the IOT devices are altering the world, the technique wherein we live and associations cooperate.

IOT device are becoming part of our lives and how important the modern world as we discussed in the above paragraph. IOT devices make the human life easier but at the same way putting them into the greater risks. IOT devices has its own flaws for example. In 2016, a DNS (Domain name structure) association, encountered an outrageous DDoS (Distributed Denial of Service) attacks which upset constant help of various noteworthy destinations, for instance, Twitter, Amazon, Facebook. Moreover, wellspring of the outbreak is for the most part from the botnet with countless exchanged off Internet of things (IOT) devices. Additional 5000 devices in a school grounds stretching out from lights to treats machineries are used to dispatch ambushes on DNS questions. Deprived of suitable defense, IOT devices are progressively likely and viably to be criticized and used for malicious resolves and we must yield extra idea on IOT (Internet of things) security and insurance affirmation

A. Architecture of IOT:

In the IOT Architecture there is no particular engineering and structure. And Thousands of structures have been proposed in the past. IOT have the multi layered structure. The standard structure of IOT will have the four layers. Let's discuss the about the standard layers of the IOT.

Perception layer: This layer will be establishment of IOT engineering, and this layer will incorporate the framework of the sensors and the principle protocols of the sensors, labels, standardized identification, etc. The information communicated on the system level is gathered from sensors of the recognition level.

Network layer: This level is acts as bridge among the perception layer and the observation layer. This layer will transmit information gathered from the sensors of the preceding layer perception layer to the observation layer, for example, humidity and the temperature information from the temperature sensor.

Middleware layer: This middleware layer is administration arranged which guarantees similar assistance type among the associated gadgets. This layer will also have called as the support layer which will acts as the authentication layer which will includes the anti-virus, secure cloud-computing, etc.

Application layer: this layer will have Smart home, shrewd city, keen transportation and brilliant emergency clinic are regular utilizations of IOT.

The IOT Architecture doesn't have the particular structure based on the working of the devices the structure of the device is build.

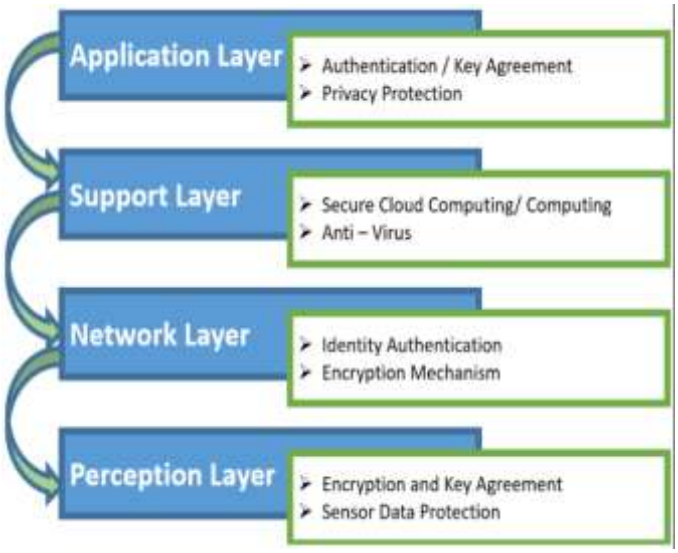

Fig.1.1 Layers of IOT

Layer	Attack	Against
Perception Layer	Node Capture	All
	Replay Attacks	C, I, AC
	Eavesdropping	C, NR, P
	Interference	A, I
	Sleep Deprivation	A
	Physical Damage	All
Network Layer	Sinkhole	C, I, AC, NR, P
	RFID cloning and Spoofing	All
	Sybil attack	NR, C, P, I, AC
	Worm hole	I, C, AC, P, NR
	Hello flood	AC, I, C, NR, P
	Selective forwarding	C, AC, I, NR, P
Application Layer	Malicious code injection	All
	Phishing attack	P
	Buffer overflow attack	A
Multi-Layer	Denial of Service(DoS)	All
	Side channel analysis	C, AU, NR, P
	Man-in-the-middle attack(MITM)	C, I, AC, NR, P

Fig.1.2 Attacks in the IOT Base on layers

B. Key Technologies of IOT:

The key developments of IOT consolidate Electronic Product Code (EPC), short range remote advances, and remote sensor arranger. Some rising headways like appropriated processing, IPv6, man-made mental aptitude in like manner have remarkable effect on the improvement of IOT.

1. **Electronic product code (E-code):**
   Normalized tag and QR code are the most comprehensively recycled e-code in the IOT device structures. E-code is a picture joined to the thing which can be recognizable and scrutinized by the scanner. E-code can be scrutinized by various sorts of contraptions, for instance, unequivocal devices or mobile phone with Internet get to.

2. **wireless Technologies:**
   Most widely used small range remote progresses in the IOT are RFID (Radio Frequency Identification), NFC (Near Field Communication), Bluetooth, Wi-Fi, IPv6 over LoWPAN (6LoWPAN), Ultra-Wideband and Zigbee.

3. **WSN (Wireless sensor network):**
   It is made out of WSN gear, correspondence stack, and programming. There are various centers in the IOT and WSN is the most significant bit of IOT designing.

4. **Cloud Computing in IOT:**
   The billions of IOT devices related with the Internet by 2020 and data created from these IOT sensors will be enormous. Also, where might we have the option to store this data and how to process this ceaseless data like stream sound and video data? Taking everything into account, only the disseminated registering can give growing and versatile limit restrain and explore this data advantageous and effectively. So circulated registering will expect a significant activity later on IOT building.

II. LITERATURE SURVEY

1. Hyun-Jin Kim, Hyun-Soo Chang, Jeong-Jun Suh, A Study on Device Security in IOT Convergence, 2016 IEEE [1]., this paper will explain about the types of devices connect to the internet and the threats in that devices and security necessities.

2. Debdeep Mukhopadhyay,PUFs as Promising Tools for Security in Internet of Things, 2015 IEEE [4]., this paper will explains use of Physically Unclonable Functions (PUFs), as a hardware security primitive for authentication.
3. ShazaZeitouni,YossefOren,Christian Wachsmann, Patrick Koeberl, and AhmadReza Sadeghi, Remanence Decay Side-Channel: The PUF Case, JUNE 2016 IEEE [4]., this paper will explains a side-channel attack based on remanence decay in volatile memory and how it can be exploited effectively to launch a non-invasive cloning attack against SRAM physically unclonable functions (PUFs).

4. AkashdeepBharadwaj,Dr.GVBSubramanyam,Dr.Vinay Aasthi,Dr.Hanumat Sastry, Solutions for DDos attacks on cloud 2016 IEEE [5]. A multi-tiered Network Architecture forDDos mitigation has been proposed wherein hybrid cloud model is used.

5. Albandari Alsumayt, John Haggerty, Ahmad Lot, Detect DoS attack using MrDR method in merging two MANETs 2016 IEEE, in this paper I have studied how to detectdos attack in the process of merging two MANETs

III. SYSTEM ARCHITECTUR

The IOT strategies today, have been passed on with the highlight on speedy opportunity to show off keeping an eye out for huge client necessities to have an edge against different contenders. There is in every way that really matters no undertaking on orchestrating these plans considering security focuses. For all intents and purposes all IOT game-plans today sending information to the cloud benefits that don't ensure about the data in like way permitting assailants to make programming duplicate(clone) and move horrendous information in a similar relationship to the snare of things (IOT) backend in the cloud. Likewise, the IOT device send the data with no security to the cloud through web these will leads for the attacks.

ISSUE 1: Identify the non-cloned device by confirming them and hinder the selection of the clone device with the system and besides avoid the moving the slip-up data.

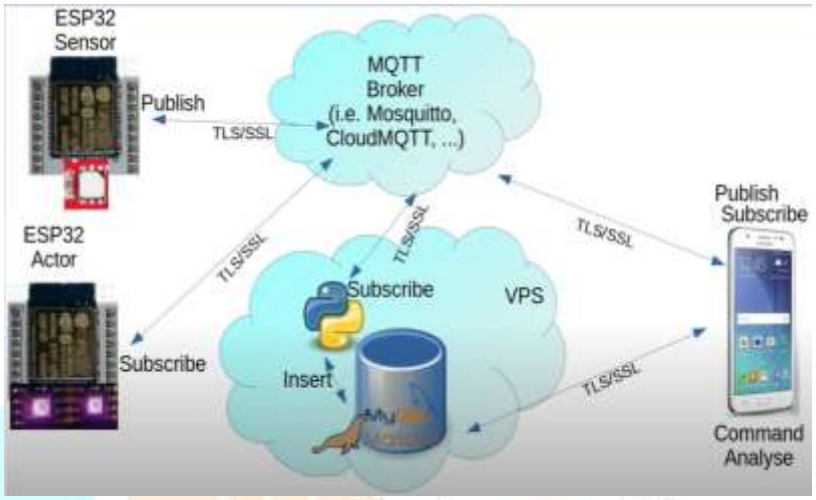

Fig.1.3 System architecture

As observed in fig 1.3, the structure incorporates sensors that are connected with devices where the sensor data is assembled then moved to the cloud by methods using WIFI, GSM, etc. propels. Contraptions are first checked to stop clone devices by swapping keys among device and server encouraged in the cloud to safeguard validation. If check is powerful, the contraption encodes information and moves to cloud to prevent sensitive data introduction. The contraption used is Arduino and sensor are ultrasonic sensor. Information moved by methods using GSM and sent through web using message transport protocols like MQTT. Data is furthermore arranged and taken care of in database like MySQL. Respective clients read the data using webserver.

IV. FLOWCHART USED

Before transferring the data of the device to the cloud, first the authentication Process will run to avoid the clone attacks. Authentication Process is delineated underneath and besides plot in Fig 1.4

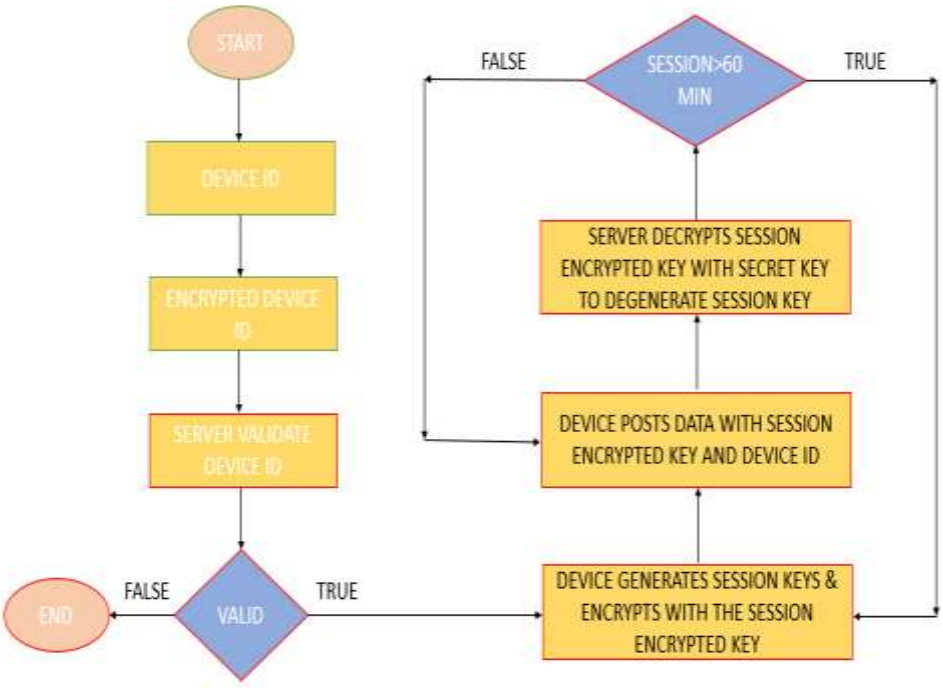

Fig.1.4 Flowchart

i. The First step is to encrypt the device id by the use of encryption key and pass the encrypted device id over MQTT. The device id ought not be sniffed on the system.

ii. The server will decrypt the device id using the encryption key and it will also ensure that the device id present in the server database or not.

iii. The Device id exists banner (truly, no) is come back to gadget by cloud server.

iv. If gadget id exists, gadget creates a remarkable meeting key which is an element of gadget id which is encoded with mystery key delivering a scrambled meeting key utilizing a custom encryption calculation.

v. The gadget posts the sensor information with encoded gadget id and scrambled meeting key to server over MQTT.

vi. Cloud decodes the encoded meeting key with mystery key and recovers the meeting key. The meeting key is checked on the off chance that it is an element of gadget ID. In the event that truly, it is put away in db. where mystery key for that gadget is put away and a meeting of 60 mins is built up.

vii. Every post of sensor information from gadget, the meeting key must match.

viii. Post 60 mins, the meeting is compellingly broken and new meeting is set up.

ix. For encryption, the information transferred is encoded utilizing scrambled meeting key.

V. IMPLEMENTATION

The device code is written in the C language that is engaged with verification. The device will send the sensor data and the encryption device id to the server with the help of the Wi-Fi modules and distributes the equivalent on MQTT message transport. The server will check the device id and complete the authentication process then the device can send the sensor data to the server and the sensor data will be stored in the server once authentication will succeed. The Device data is stored in the database in the encrypted format. The web reassure is html and java content and makes rest programming interface calls executed in python flagon. The End user can see the sensor data in the website.

VI. RESULT

The device will authenticate with the server with the help of the certificate provided to the device. The certificate of the device will be encrypted and the private key will be shared with the server which is showed in the Fig 1.5.

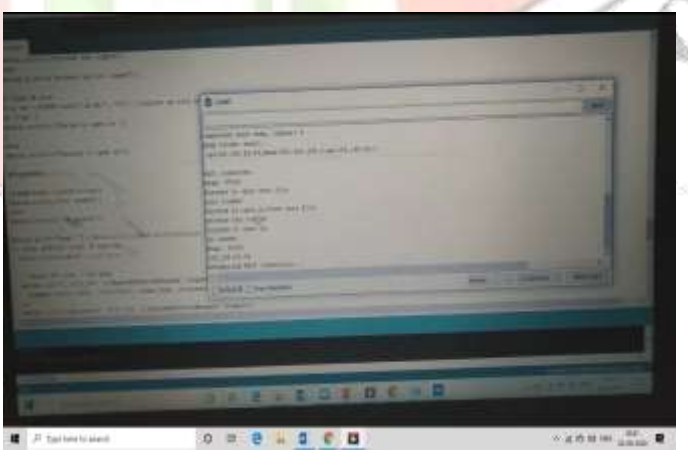

Fig.1.5 Authentication process

Once the Authentication is completed the sensor data will be stored in the server and the same data will be send to the end users in the website Fig 1.6.

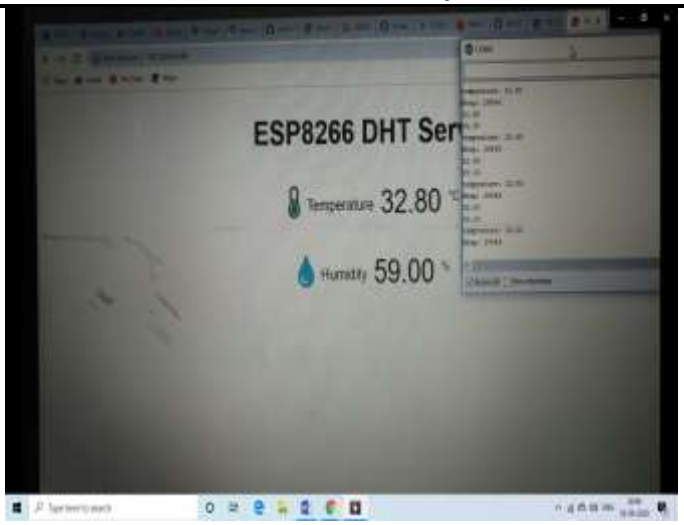

Fig 1.6. Output of the device for the end user

VII. CONCLUSION

The 2 security challenges that establish max security penetrates in IOT scene have now arrangements recognized to forestall assaults. The novel arrangement executed is painstakingly picked because of equipment imperatives of handling and memory on IOT gadgets just as limit cost of information move charged by ISP. Execution is done to set up gadget association with cloud segment for validating gadgets to forestall gadget clone assaults. Post effective validation information is scrambled to forestall delicate information presentation. The arrangement is productive as it is secure with almost no overheads regarding time required for validation which isn't exponential and information size which just includes extra 8 bytes of scrambled meeting key for each datum presented from gadget on cloud. The little cost overhead merits the huge security profits.

VIII. ACKNOWLEDGEMENT

I acknowledge those who have supported me to do things in a better way and it would include my guide Prof. Manjula m for providing the right path throughout this research and giving in her encouragement and support. We are thankful to the authorities of Atria Institution of Technology, Bangalore for all the support and guidance.

REFERENCES

1. “A Study on Device Security in IOT Convergence”, by Jeong-JunSuh, Hyun-SooChang, Hyun-JinKim, 2016 IEEE.
2. “Remanence Decay SideChannel: The PUF Case”, by Christian Wachsmann, ShazaZeitouni, YossefOren, 2016 IEEE.
3. “Solutions for DDos attacks on cloud”, by Dr.Vinay Aasthi, Akashdeep Bharadwaj,Dr.Hanumat Sastry,Dr. GVB Subramanyam, 2016 IEEE.
4. “Denial-of-Service detection in 6LoWPAN based Internet of Things” by MaurizioA.Spirito, Prabhakaran Kasinathan, MarkVinkovits, Claudio Pastrone, 2013 IEEE.
5. “Detect DoS attack using Mr DR method in merging two MANETs”, by John Haggerty, Ahmad Lot, AlbandariAlsumayt, IEEE 2016.
6. “PUFs as Promising Tools for Security in Internet of Things”, by DebdeepMukhopadhyay, 2015 IEEE.