Security Privacy in Internet of Things(IOT)

Samruddhi S. Burhade
MCA&B.A.M.U.,
Maharashtra, India

Sonal N. Deshmukh
PhD MCA&B.A.M.U.,
Maharashtra, India

Abstract—The Internet Of Things(IOT) is interconnection between identifiable embedded computing devices. Internet of Things is highly on the rise from smart cities, environment, health, energy, vehicle, transport, public safety to our daily essentials. Internet of Things has completely revitalized these areas. IOT expect the advanced connectivity with devices services. This paper highlighted the security and privacy aspect of IOT and various security threats which are given in each concept related to IOT. Various techniques are used for security and privacy of IOT devices and easy to adapt by users.

Keywords—Include at least 5 keywords or phrases IOT (Internet of Things),Denial of service, security, privacy, NFC(New Field Communication),RFID

I. INTRODUCTION

IOT-Internet Of Things is connecting lots of devices every day and in future most of devices are based on IOT concept. It is beneficial for people to change the way people carry out every day task. Having smart home like smart lighting, AC reducing light energy and power electric bill to. It is also helpful to company, smart city. When object can sense and communicate if changes how and where decision are made latest trends and challenges and future scope of this technology have been touched upon for better understanding. A new era of IOT service which will connect everything is on the way. IOT triggered by technological advance is embedded systems, hardware, software, connectivity, Networking concepts.[1]Internet of things is continuously developing, significant potential of high scale development can also be seen in other related technologies like Computer computing, Big Data, Robotics, Semantic Web, Augmented Reality etc. The meaning of IOT is device and object which are connected to internet providing desire data. e.g. smart phones, smart watches, Augmented Reality devices, vital reality devices and etc. Lots of security and privacy issues will arise and more attention is required in IOT especially with regard to issues like authenticity, confidentiality and integrity, Availability of data and services.[2]Each and every device is connected to each and every Internet and Internet is always regarded as unsecured medium. IOT is a system of various interrelated computing devices, digital systems, machines, sensors, objects, animal or people that have a unique identifier associated with them and the ability to transfer data over a network without the need of human-to-computer or human-to-human interaction. IOT is a technology that has evolved with convergence of various technologies like wireless communication, MEMS(micro-electromechanical systems), Wireless Sensor Network, Mobile Communication etc..

Fig1. IOT Theft

This convergence has proved to be vital as it has led to bringing operational technology (OT) and information technology (IT) on a common platform, which in turn allows unstructured machine-generated data to be further analyzed.
for initiating further improvements in decision making process in automation. **Operational technology** (OT) is combination of hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. It comprises the devices, sensors and software necessary to control and monitor plant and equipment etc. Information Technology (IT), on the other hand, combines all necessary technologies for information processing. **Information Technology** is the application of computers to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.

**II. SECURITY**

There are many advanced technology involve into IOT such as wireless sensor network, low energy wireless communication, near field communication, barcode, Intelligent sensing, Radio frequency identification, cloud computing etc. The security and Privacy requirements in IOT are authentication, Access control, Data confidentiality, security and trust, etc. different layers of IOT[6]. Security problems, such as denial of service attacks, sybil attacks, data attacks, code attacks, local security of sensing nodes. Threat modeling using the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (DOS), Elevation of privilege (STRIDE) software approach was conducted to identify the attack scenarios and formulate mitigation plans for gateway, service, Data store, web app, web interface.

![Security Threats](Fig2.png)

In security by using IOT devices for reorganization of main objective is the deeper collection of all kinds of information of all kinds of devices in terms of properties, environmental condition. The duty of providing reliable platform via various services in terms of Web services and interfaces.

**III. PRIVACY**

Right user willing to share information it self with others. The environment is sensed by connected devices. Protecting the personal information in case of the device. They broadcast the gathered information and particular event to server which carries out the application logic. Privacy should be protected in the device in storage during communication and processing which helps to disclose the sensitive information.[4]The sensitive information may be leaked out in case of unauthorized manipulation or handling of hardware and software in these devices. Encryption during the communication can be replaced for better Privacy.[3] Device should be communicate iff when there is need to degrade privacy induced at the time of communication.
The privacy of households could be compromised by solely analyzing smart home network traffic patterns without dissecting the contents of encrypted application data, yet a synthetic packet injection scheme can be used to safely overcome such invasion of privacy[5]. Limited data or needed data should be stored. As name suggested IOT i.e. everything is connected to internet when user use location to control device location privacy is critic infrastructure. The most notable potential breach is the tracking of user among the services ecosystem via his fingerprint.

IV. (NFC) NEW FIELD COMMUNICATION

Near field communication maintains interoperability between different wireless communication methods like Bluetooth and other NFC standards. Contactless communication allows a user to wave the device over a NFC compatible device to send information without needing to touch the devices together or go through multiple steps setting up a connection. The most well-known use of NFC technology is for contactless payment. Customers can swipe their device over a card reader to make a purchase without fumbling through credit and debit cards or counting out cash[3]. The small size of NFC tags and their lack of a battery, relying instead on radio frequency signals sent from a device or other NFC compatible device to operate, let them go virtually anywhere. Passive devices, such as the NFC tag in smart posters, store information and communicate with the reader but do not actively read other devices. Peer-to-peer communication through two active devices is also a possibility with NFC[8].

V. RFID

The acronym refers to small electronic devices that consist of a small chip and an antenna. Data is typically stored in user memory on a tag. This is separate from the field for the unique serial number, which can be pre-programmed or assigned by a user. The chip typically is capable of carrying 2,000 bytes of data or less. The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information. The RFID card is faster to use. The contactless cards use highly secure data transmission standards. Contactless cards make use of the most secure encryption standards practical
128-bit and triple DES encryption to make it nearly impossible for thieves to steal your data[7][9].

Fig5. RFID

VI. CONCLUSION

IOT device has to fit the consumer needs. This is importance in case privacy and security protection. It requires additional consumer intervention in comparison to a non-protecting device entering a password when accessing. The privacy gain for the effort remains low so that to protect and maintain potential privacy. It reduces vulnerabilities and leakage of personal data. Authentication and weak authentication method on IOT devices increase the threat of device penetration or security because breaking into weak authentication. For IOT device with high or strong encryption of data, HTTPS or SSL methods are used.

REFERENCES