International Journal of Engineering Computational Research and Technology
Journal home page: www.ijecrt.org
ISSN (Online): 2456-9852 Volume 4, Issue 1, June 2019

IoT (Internet of Things) Security

Neetu Sharma[a], Lalit Kumar Singh[b, *]

[a-b] *Department of Cyber Forensic and Information Security, Maharshi Dayanand University, Rohtak , Haryana, INDIA*

[*] Corresponding author:
E-mail address: lalitkumarsingh@gmail.com (Lalit Kumar Singh).

ABSTRACT

Global IoT(Internet of Things) requirement is increasing exponentially. Number of end users, end devices and IoT components are increasing day by day. It's necessary to understand the different component of IoT solution and its threats and vulnerability and the technique to protect each layer of IoT from the external threats and protect it from unauthorized access to run the system smoothly.

Keywords:
IoT Security
Hardware or Device or Edge security
System security
Information security

1. Introduction

IoT stands for Internet of Things and it consist of two words, first word is Internet- which means connected or network and second the second word is Things- which means all object which act as data source in that network, these objects could be hardware or software or any other objects like human beings, animal and plants, but in most of the cases these things are sensor and devices. In IoT use cases all components of IoT are interrelated to each other to share their information. This interconnection could be between human to human or between machine to machine either on real time or near real time [1].

Based on Industry adoption IoT terms is used in different way based on their regulation adoption and ecosystem.

- Manufacturing Industry-IIOT(Industrial IOT)
- Aviation Industry- AIOT(Aviation IoT)
- Automobile Industry- AIOT(Automobile IoT)
- Medical Industry-IOMT(Internet of Medical Thing)
- Enterprise- EIOT(Enterprise IoT)

Due to adoption of IoT and evaluation of new technology in different industry it has high impact on our way of living because of impacts on communication, health, business, education, transportation, science, government, cities and human in general. Because of this adoption and exposure several issues and complexities are threatening the IoT ecosystem like security, confidentiality and privacy in this technology [2].

This work proposed some major issues which are common and that should be faced by community related to the privacy, confidentiality, security and vulnerability in the

IoT. Based on our evaluation, we highlight some possible method and directions for its prevention.

2. Component of IoT

The main component of IoT (Internet of Things) are following [3]

- Sensing.
- Communication
- Platform & Cloud
- Application / Delivery of information/User Interface

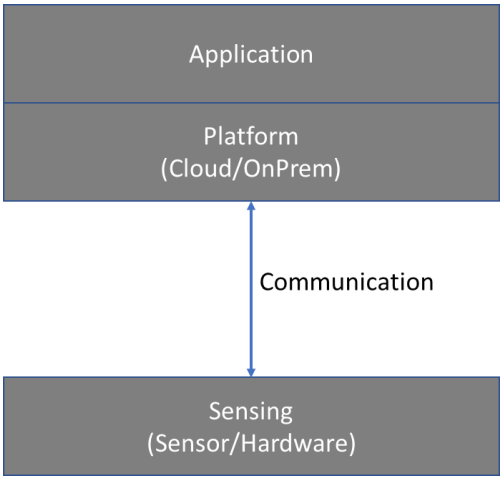

Fig 1. Component of IoT

2.1 Sensing

The first layer in IoT stack is gathering information or data source. This can be information captured by devices or "Edge" which could be an appliance, a wearable device, a wall mounted control or any number of commonly found devices. The sensing can be biometric, biological, environmental, visual or audible.

2.2 Communication

This is way or medium by which devices start communicating the platform to send or receive information. IoT devices require a medium for transmitting the sensed information at the device end to a Cloud-based service for other useful information processing. Different type of communication network is used between the sensing devices to communicate with the cloud or platform. It consists of short range communication, long range communication, wired communication or wireless communication, point to point communication or point to multipoint communication. Communication happened over different network topology like mesh, simple etc. There is different method of casting of the communication messages like broadcast, unicast and multicast.

Some of the communication interfaces are WiFi, Cellular (GSM, GPRS, 3G, 4G, LTE), ethernet, fiberoptic, satellite communication, WiMax, Bluetooth, Zigbee, LoRa, Sigfox, Z-Wave, HART, USB, LiFi, etc.

There are different communication protocols which are common in IoT use cases like REST, MQTT, AMQP, CoAP, Modbus, Ethernet-IP, Profibus, Profinet etc.

2.3 Cloud and Platform

Platform is the environment where transmitted data from the things of IoT is collected and processed for the useful information and analysis for the end user of the whole system or subsystem. Platform could be on premise or cloud. On Premises platform could be dedicated and used by single entity where as cloud platform could be shared but virtually dedicated to individual identity. Platform consist of all necessary database, services and UI which are necessary to run the software for data processing and visualising and generating reports based on the requirement.

2.4 Application

Special users in the whole IoT solution such as consumer, commercial, industrial etc. and each user have its own requirement and expectation from the solution. Application is the peace of software which meets the user requirement in their simple and desired way with useful information. These application are designed and build with well thought out process by considering the whole ecosystem need like user requirement and the hardware platform requirement where it will be executed like PC, tablet and smart devices on different operating system.

3. IoT Security

IoT security consist of the security of all layers of the IoT as describe in above section i.e

- Sensing Layer -Device or Edge security
- Communication security
- Cloud or Platform Security
- Application Security

3.1 Edge Security

Edge play very important role in IoT. IoT acts as data source and can also provide control to other OT system. So, securing the edge is very important because most of time it is exposed in uncontrolled environment due to which the risk of external threats increases, Edge security are complex because each edge or devices expose or communicate on different interface and different protocol running on different execution platform like controller or processor and operating system. Many security function and module are designed and developed to ensure the edge or device security and it can be executed and deployed on the edge as a self-contained module to enforce uniform security policy. These self-contained security module or agent can track and monitor and manage the activity perform on the edge devices [4].

There different ways to attack an endpoint and therefore many issues to deal or address. The issues to deal or address include:

- Secure boot attestation
- Separation of security agent
- Endpoint identity
- Endpoint attack response
- Remote policy management
- Logging and event monitoring
- Application sandboxing
- Application whitelisting
- Network whitelisting
- Dynamically deployed countermeasures
- Peripheral devices management
- Endpoint storage management

3.2 Communication Security

All component of IoT communicate each other with different types of communication protocol, communication interface and data format either in one direction or bidirectional. It's important that the communication must be secure, protected and reliable.

- Architectural considerations at transport layer
- Client-Server Security in request-response and publish-subscribe communications
- Mutual authentication
- Communication authorization
- Identity proxy/consolidation point
- User authentication and authorization
- Encryption communication

3.2 Platform/Cloud Security

Platform is the environment in which a piece of software is executed. With the help of software platform collect data from various sources of IoT to store, visualize, analyze, predictive and for monitoring purpose and to provide processed and useful information to the end user. The platform can be on- premises or cloud based. The threats for both type of platform are different. The platform security is the architecture framework, software or tools, method or process ensure the security of whole software environment. The platform security consists of security of the platform software, hardware, storage database, network and all other component of the platform environment. Platform security also includes information about dedicated hosting, managed hosting, shared hosting, security and performance .The Platform security include

- Operating system security
- Data security
- Software security
- Information security
- Services security
- Network security
- Management
- Performance

3.2 Application Security

Application security involves the security of the software application running on the IoT platform from the external threats or malicious attacks. Application security ensures the protection of application against unauthorized access and attacks. Application Security threats are:

- Eavesdropping
- Malware
- Spyware
- Ransomware

- Trojans
- Viruses
- Worms
- Rootkits
- Keyloggers
- Computer crime
- Vulnerabilities
- Screen scrapers
- Backdoors
- Logic bombs
- Payloads
- Denial of service

Technique to protect Application

- Application whitelisting
- Antivirus software
- Secure coding
- Secure by default
- Secure by design
- Secure operating systems
- Authentication
- Multi-factor authentication
- Authorization
- Data-centric security
- Encryption
- Firewall
- Intrusion detection system
- Mobile secure gateway
- Computer access control

4. Conclusion

The famous common phrase "Prevention is better than Cure". Similarly, it is important to know the security threats and vulnerability and its method to prevent the IoT solution in the digital environment

References:

[1] Maciej Kranz, "Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry", Kindle Edition, Wiley; 1 edition (November 9, 2016).

[2] Vlasios Tsiatsis, Stamatis Karnouskos, Jan Holler, David Boyle, Catherine Mulligan, "Internet of Things: Technologies and Applications for a New Age of Intelligence", 2nd Edition, Academic Press; 2 edition (December 14, 2018).

[3] IEEE Internet of Things Journal, https://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6702522 [2019]

[4] Internet of Things, "Technology, Communications and Computing", Springer Nature, 2019. https://www.springer.com/series/11636?detailsPage=titles