Analysis on securing the data over the Internet of Things (IoT)

MADHUSUDHAN REDDY.K, K. NARENDRA KUMAR, V. HARSHA VARDHAN

Abstract—The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic idea is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. IoT is rapidly developing, but there are some uncertainties about its security and privacy which would affect its growth. In this paper, we have analyzed the security issues and challenges and we have provided well defined security architecture as a confidentiality of the user's privacy and security

Index Terms— Internet of things, IoT Security, Securing the IoT data.

1 INTRODUCTION

THE Internet of Things (IoT) was firstproposed by kevin Ashton in 1999. Internet of Things (IoT)is defined in many ways, and it encompasses many aspects of life from connected homes and citiesto connected cars and roads, roads to devices that track an individual's behavior and use the data collected for push services. Some mention one trillion Internet-connected devices by 2025 and define mobile phones as the eyes and ears of the applications connecting all of those connected things. By these internet of things billions of objects can communicate over worldwide over a public, private internet protocol network in 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Smartcities, Smart cars, Public safety, Smart Industries and Environmental Protection has been given the high intention for future protection by IoT Ecosystem. For the development the government of Europe, Asia and America has considered the Internet of Things has area innovation and growth. Many visionaries have seized on the phrase Internet of Things to refer to the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable, and/or controllable via the Internet, irrespective of the communication means (whether via RFID, wireless LAN, wide- area networks, or other means).Radio Frequency Identification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. This results in the generation of enormous amounts of data which must be stored, processed and presented in a seamless, efficient, and easily interpretable form. This model will consist of services that are commodities and delivered in a manner like traditional commodities.

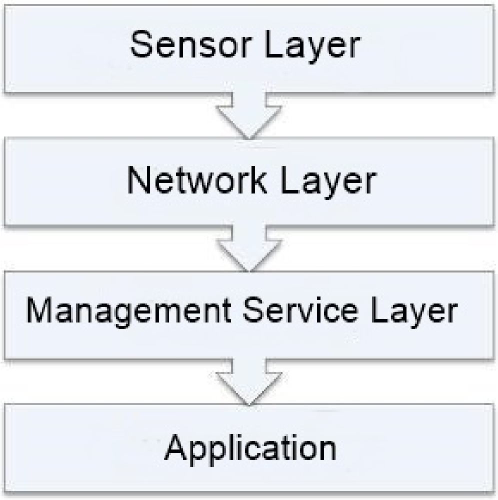
Internet of Things (IoT) is a new revolution of the Internet. Internet of Things (IoT) can be said the expansion of internet services. It provides a platform for communication between objects where objects can organize and manage themselves. It makes objects themselves recognizable. The internet of things allows everyone to be connected any time and anywhere. Objects can be communicated between each other by using radio frequency identification (RFID), wireless sensor network (WSN) etc. Radio Frequency identification assigns a unique identification to the objects. RFID technology is used as more secure identification and for tracking/locating objects, things, vehicles.

IoT has the great potential and promises a great future but it has a security problems too. There are many things to be clarified for its worldwide adoption and without answering them and finding the solutions for the problems there will be no future.due to easy accesability of the devices,they can be easily exppoloited by the hackers .The devices are prone to various kinds of attacks.we should ensure the proper security by providing the security measures.Since the devices have a direct impact on the lives of users the security considerations must be a high

- *MadhsudhanReddy.K is currently pursuing Master of Computer Applications in KMMInstitute of PG Studies in S.V. University,Tirupati, AndhraPradesh, PH:9963488389. E-mail: madhusudhanreddy1221@live.com.*
- *Narendra kumar. K is currently pursuing Master of Computer Applications inKMM Institute of PG Studies in S.V. University, Tirupati,AndhraPradesh, PH: 9492964912.E-mail: luckynarendra52@gmail.com*
- *V.harshavardhan is with Department of Master of Computer Applications, working as Assistant professor in KMM Institute of PG Studies, Tirupati, AndhraPradesh, PH:9959974097. E-mail: vemuriharsha@gmail.com.*

priority and there must be some proper security infrasrtructure that can limit the threats .

2 ARCHITECTURE OF THE INTERNET OF THINGS



2.1 Sensor layer

This layer consists of different types of data sensors such as RFID, Barcodes or any other sensor network.the basic idea of this layer is to identify the unique objects and deal with its collected data that has been obtained from thr real world with the help of its respective sensors.

2.2 Network layer

The idea behind this layer is to transmit the collected infirmarion from the sensor layer to any information processing system through existing communication network like internet, mobile network or any other reliable network.

2.3 Management service layer

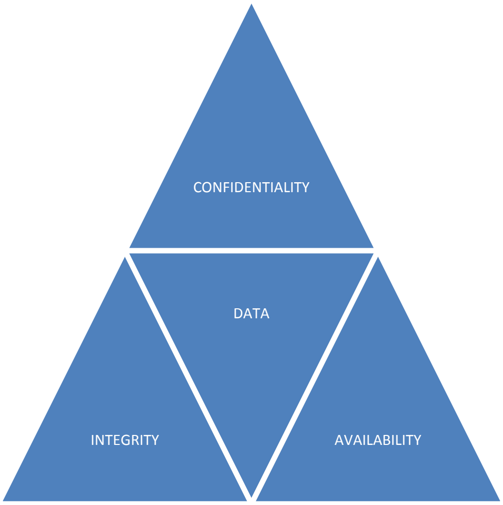
This layer consists of information processing system that take the automated actions based on the results of processed data and links the system with the database which provides storage facilities to the data.

2.4 Application layer

This layer realizes various practical applications of IoT based on the needs of the users and different kinds of industries such as smart home, smart cities, smart companies, smart hospitals, smart transportation etc.

3 DATA PROTECTION

IoT has the potential to optimize efficiencies, create new revenue streams and enable organizations to leverage big data for smarter business decisions. However, as enterprises embrace IoT, security must be a top priority to ensure the sensitive information captured by these connected devices does not fall into the wrong hands.



3.1 Data confidentiality

Data confidentiality is like providing freedom to user from the external interference .it is the ability to provide confidence to the user about the privacy of the sensitive information by using different mechanisms so that its disclosure to unauthorized party is prevented and can be accesed by the authorized user only. there are many security mechanisms to provide confidentiality of the data. some of the techniques which are used to gain the data confidentiality is by using data encryption where the data is encrypted and two step verification which provides authentication by two dependent components and allows access only if both the devices pass the authentication test. biometric verification can be used to obtain the data confidentiality.

3.2 Data integrity

During the communication, data could be altered by the cybercriminals or could be affected by various other factors that are beyond human control including the crash of server or an electromagnetic disturbance. Data Integrity refers to the protection of useful information from the cybercriminals or the external interference during transmission and reception with some common tracking methods, so that the data cannot be tampered without the system catching the threat. The methods to ensure the accuracy and originality of data include methods like Checksum and Cyclic Redundancy Check (CRC) which are simple error detector mechanisms for a portion of data. Moreover, continuous syncing of the data for backup purposes and the feature like Version control, which keeps a record of the file changes in a system to restore the file in case of fortuitous deletion of data can also ensure the integrity of data such that the data on IoT based devices is in its original form when accessed by the permitted users.

3.3 Data availability

One of the major goals of IoT security is to make data available to its users, whenever needed. Data Availability ensures the immediate access of authorized party to their information resources not only in the normal conditions but also in disastrous conditions.

4 DATA PROTECTION CHALLENGES AND ISSUES

There have been many achievements in the research field of IoT, however there are still some open challenges that needs to be ad-dressed for the ubiquity of this technology. In this section, some of the threats in each architectural layer that needs special attention are discussed.

4.1 Sensor layer Problems

Sensor layer consists of different sensor technologies like RFID which are exposed to many kinds of threats which are discussed below:

4.1.1UnauthorizedAccess to theTags.

Due to the lack of proper authentication mechanism in many RFID systems, tags can be accessed by someone without authorization. The attacker cannot just read the data but the data can be modified or even deleted as well.

4.1.2 Tag Cloning.

Since tags are deployed on different objects which are visible and their data can be read and modified with some hacking techniques therefore they can be easily captured by any cybercriminal who can create a replica of the tag and hence compromising it in a way that the reader cannot distinguish between the original and the compromised tag

4.1.3 Eavesdropping.

Because of the wireless characteristics of the RFID it becomes very easy for the attacker to sniff out the confidential information like passwords or any other data flowing from tag-to-reader or reader-to-tag which makes it vulnerable because the attacker can make it to use in despicable ways

4.1.4 Spoofing.

Spoofing is when an attacker broadcasts fake information to the RFID systems and makes it to assume its Originality falsely which makes it appear from the original source.This way attacker gets full access to the system making it vulnerable.

4.1.5 RF Jamming.

RFID tags can also be compromised by kind of a DoS attack in which communication through RF signals is disrupted with an excess of noise signals.

4.2 Network layer problems

Network layer consists of the Wireless Sensor Network (WSN) which transmits the data from the sensor to its destination with re-liability. The related security issues are discussed below:

4.2.1 Sybil Attack.

Sybil is a kind of attack in which the attacker manipulates the node to present multiple identities for a single node due to which a considerable part of the system can be compromised resulting in false information about the redundancy.

4.2.4 Sinkhole Attack.

It is a kind of attack in which the adversary makes the compromised node look attractive to the nearby nodes due to which all the data flow from any particular node is diverted towards the compromised node resulting in packets drop i.e. all the traffic is silenced while the system is fooled to believe that the data has been received on the other side. Moreover, this attack results in more energy consumption which can cause DoS attack.

4.2.5 Sleep Deprivation Attack.

The sensor nodes in the Wireless Sensor Network are powered with batteries with not so good life-time so the nodes are bound to follow the sleep routines to extend their lifetime. Sleep Deprivation is the kind of attack which keeps the nodes awake, resulting in more battery consumption and as a result battery lifetime is minimized which causes the nodes to shut down.

4.2.6 Denial of Service (DoS) Attack.

The kind of attack in which the network is flooded with a useless lot of traffic by an attacker, resulting in a resource exhaustion of the targeted system due to which the network becomes unavailable to the users.

4.2.7 Malicious code injection.

This is a serious kind of attack in which an attacker compromises a node to inject malicious code into the system which could even result in a complete shutdown of the network or in the worst case; the attacker can get a full control of the network.

4.2.8 Man-in-the-Middle Attack.

This is a form of Eavesdrop-ping in which target of the attack is the communication channel due to which the unauthorized party can monitor or control all the private communications between the two parties hideously. The unauthorized party can even fake the identity of the victim and communicate normally to gain more information.

4.3 Middle-ware Layer Challenges

This layer is composed of data storage technologies like cloud computing. The security challenges of this layer are discussed below:

4.3.1 Unauthorized Access.

Middle-ware Layer provides different interfaces for the applications and data storage facilities. The attacker can easily cause damage to the system by forbidding the access to the related services of IoT or by deleting the existing data. So, an unauthorized access could be fatal for the system.

4.3.2 DoS Attack.

It is similar to the DoS attack discussed in the previous two layers i.e. it shuts down the system which results in unavailability of the services.

4.3.3 Malicious Insider.

This kind of attack occurs when some-one from the inside tampers the data for personal benefits or the benefits of any 3rd party. The data can be easily extracted and then altered on purpose from the inside.

4.4 Application Layer Challenges

The related security issues of this layer are described below:

4.4.1Malicious Code Injection.

An attacker can leverage the at-tack on the system from end-user with some hacking techniques that allows the attacker to inject any kind of malicious code into the system to steal some kind of data from the user.

4.4.2 Denial-of-Service (DoS) Attack.

DoS attacks nowadays have become sophisticated, it offers a smoke screen to carry out attacks to breach the defensive system and hence data privacy of the user, while deceiving the victim into believing that the actual attack is happening somewhere else. This put the non-encrypted personal details of the user at the hands of the hacker.

4.4.3 Spear-Phishing Attack.

It is an email spoofing attack in which victim, a high-ranking person, is lured into opening the email through which the adversary gains access to the credentials of that victim and then by a pretense retrieves more sensitive information.

4.4.4 Sniffing Attack.

An attacker can force an attack on the sys-tem by introducing a sniffer application into the system, which could gain network information resulting in corruption of the system.

5. SECURITY AT DIFFERENT LAYERS

There are many researches being carried out to provide a reliable well-defined security architecture which can provide confidentiality of the data security and privacy. W. Zhang et al. proposed architecture for the security against the possible threats, as shown below

5.1Perception Layer

Perception Layer is the bottom layer of the IoT architecture which provides various security features to the hardware. It serves four basic purposes which are Authentication, Data Privacy, and Privacy of sensitive information and Risk Assessment which are discussed below:

5.1.1 Authentication.

Authentication is done using Crypto-graphic Hash Algorithms which provides digital signatures to the terminals that could withstand all the possible known attacks like Side-channel attack, Brute force attack and Collision attack etc.

5.1.2 Data Privacy.

Privacy of the data is guaranteed by sym-metric and asymmetric encryption algorithms such as RSA, DSA, BLOWFISH and DES etc which prevents an unauthorized access to the sensor data while being collected or forwarded to the next layer. Due to their low power consumption benefit, they can be easily implemented into the sensors.

5.1.3Privacy of sensitive information

As for hiding the sensitive information, anonymity of the location and identity is obtained using K-Anonymity approach which ensures the protection of the information like identity and location etc of the user.

5.1.4 Risk Assessment.

It is a fundamental of IoT security which discovers the new threats to the system. It could help preventing the security breaches and determining the best security strategies. An example of it is the Dynamical Risk Assessment method for IoT.
Even with such security measures, if an intrusion is detected in the system, an automated Kill-command from the RFID reader is sent to the RFID tag which prevents an unauthorized access to the RFID tag data.

5.2 Network Layer

The network layer which could be both wired or wireless is exposed to various kinds of attacks. Due to the openness of the wireless channels, communications can be monitored easily by some hack-ers. The network layer security is further divided into three types which are discussed below:

5.2.1 Authentication.

With the help of a proper authentication process and point to point encryption, illegal access to the sensor nodes to spread fake information could be prevented. The most common kind of attack is the DoS attack which impacts the net-work by driving a lot of useless traffic towards it through a number of botnets fueled by the system of interconnected devices.

5.2.2 Routing Security

After the Authentication process, routing algorithms are implemented to ensure the privacy of data exchange between the sensor nodes and the processing systems. There have been many researches carried out for the routing ways including Source Routing, in which data to be transmitted is stored in the form of packets which is then sent to the processing system after being analyzed by the intermediate nodes, And the Hop-by-Hop routing in which only address of the data destination is known. The security of routing is ensured by providing multiple paths for the data routing which improves the ability of the system to detect an error and keep performing upon any kind of failure in the system.

5.2.3 Data Privacy.

The safety control mechanisms monitor the system for any kind of intrusion and finally Data integrity methods are implemented to make sure that the data received on the other end is the same as the original one.

5.3 Middle-ware and Application Layer

This layer amalgamates the Middle-ware and Application layer to form an integrated security mechanism. The security categorization is discussed below:

5.3.1 Authentication.

Firstly, it goes through the authentication process which prevents the access to any miscreant user by integrated identity identifications. This is exactly similar to that of the identification process in either of the layers except that this layer encourages authentications by some certain cooperating services which means users can even choose the associated information to be shared with the services. The major technologies used in this layer are Cloud computing and Virtualization, both of which are ripe to various attacks. The cloud technology can be easily compromised; one of the worst threat is the insider threat. Similarly, Virtualization is exposed to DOS and a lot of research is needed in both domains and to provide secure environment.

5.3.2 Intrusion Detection.

Its intrusion detection techniques pro-vide solutions for various security threats by generating an alarm on occurrence of any suspicious activity in the system due to the continuous monitoring and keeping a log of the intruder's activities which could help to trace the intruder. There are different existing intrusion detection techniques including the data mining approach and anomaly detection.

5.3.3 Risk Assessment.

The risk assessment gives justification for the effective security strategies and provides improvements in the existing security structure.

5.3.4 Data Security.

Data security is ensured by various encryption technologies which prevent the data stealing threats. Moreover, to prevent other malicious activities from the miscreant users, Anti-Dos firewalls and up to date spywares and malwares are introduced.

6. CONCLUSION

The only hurdle that stands in the way of the IoT development is the security and privacy issues. Security at all the levels of IoT is expository to the functioning of IoT. Luckily, there already have been many research achievements in the IT security concerns and for effective implementation of a security infrastructure for IoT, these achievements must need to be further expanded instead of focusing the attention towards seeking the new possible security solutions, to make IoT able to provide services to the futuristic data-hungry billions of devices with the ability to thwart the adversaries. So the adequate privacy and security measures through substantial researches must be made and the answers for the number of open questions in this research field must be provided, before it gets deployed in the society. This paper discussed the security goals and possible security challenges and issues of the IoT system. Then a well-defined architecture for the IoT security was presented. In the future, more authentications, risk assessment and intrusion detection techniques in each architectural layer must be explored in parallel to the implementation of the security infrastructure using existing IT security features. Moreover, legal frameworks, proper regulations and policies must be devised to ensure stable development of the secure technologies.

7. REFERENCES

[1] Kevin Ashton," That 'Internet of Things' Thing", RFID Journal, 22 June 2009

[2] Miao Wu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du," Research on the architecture of Internet of things," in Advanced Computer Theory and Engineering (ICACTE), 2010, pp. 484-487

[3] DebasisBandyopadhyay, Jaydip Sen," Internet of Things - Applications and Challenges in Technology and Standardization" in Wireless Personal Communications, Volume 58, Issue 1, pp. 49-69

[4] Benjamin Khoo," RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in Internet of Things (iThings/CPSCom), 2011, pp. 709-712

[5] H. Zhang, L. Zhu," Internet of Things: Key technology, architecture and challenging problems", in Computer Science and Automation Engineering (CSAE), 2011, Volume: 4, pp. 507-512

[6] RFID Security Issues – "Generation2 Security". It can be accessed at: http://www.thingmagic.com/index.php/rfid-security-issues