Internet of Things: Architecture, Applications and Challenges

Mubashir Hussain
Department of Virtualization, School of Computer Science,
University of Petroleum and Energy Studies,
Dehradun, Uttarakhand, India

Mohammad Saqib
Department of Computer Science,
SRM University, Dehli-NCR, India

ABSTRACT

"Internet of Things (IoT)" – a relatively recent term, build on decades of research has revolutionized almost every field in today's world. IoT makes smart objects the ultimate building blocks in the development of cyber-physical smart pervasive frameworks. It has influenced our living from the way we react to the way we behave by utilizing the full potential of internet in enhancing the lifestyle of human beings. IoT is a network that connects physical devices of various domains like home automation, industrial process, vehicles, healthcare, weather monitoring, etc. to internet. From air conditioners that we can control with our smart phones, to smart cars providing the shortest route or smart watch which is tracking our daily activities.

This paper is devoted to study the security architecture and its features in the domain of IoT. In the next part of the paper, the need and applications of IoT in various fields are discussed. This paper provides a general literature survey of recent progress and advances in the field of IoT. Next a hand-to-hand discussion of various issues and challenges being faced by various organizations are studied. In the final part of the paper, the most significant conclusions and suggestions are offered.

Keywords

Internet of Things (IOT), Cloud, Internet, System Architecture, Sensor Devices

1. INTRODUCTION

Internet of Things, a system of interconnected devices, was first coined by Kevin Ashton in 1999 [1]. IoT is a concept that connects all the surrounding smart devices (things) to internet and let them communicate with each other over the internet. These devices use sensors and actuators to communicate with each other across the internet. IoT is driving the automation to a next level where devices will communicate with each other to make decisions on their own without human intervention fig.1. These devices gather and share data about how they are used and the environment in which they are operated. It is done using sensors which are embedded in every physical device. These sensors continuously emit data about the working state of the devices.

IoT provides a common platform for all the connected devices to dump their data and a common language for all the devices to communicate with each other. IoT employs a number of protocols and technologies to communicate with the devices based on the requirements. The commonly used technologies and protocols that are used are Bluetooth, wireless, NFC, RFID, radio protocols and WiFi-direct. Data is emitted from various sensors and sent to IoT platform securely. IoT platform integrates the collected data from various sources and then further analytics is performed on the data and valuable information is extracted as per requirement. Finally, the result is shared with other devices for better user experience automation and improving efficiencies.

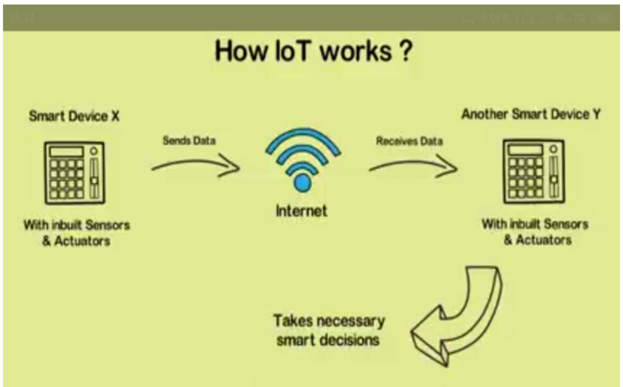
How IoT works ?
Smart Device X
With inbuilt Sensors & Actuators
Sends Data
Internet
Receives Data
Another Smart Device Y
With inbuilt Sensors & Actuators
Takes necessary smart decisions

Fig.1-The IoT Network

2. NEED FOR IOT

IoT applications are flourishing across all industries and market. The basic need for enabling IoT based applications is to reduce human intervention with the devices. Nowadays we almost have internet infrastructure available everywhere and we can employ it whenever we want. IoT tries to establish advanced connectivity among the devices like mp3 player, MRI, Traffic lights, microwave oven etc with the aid of internet. Rather to run from machine to machine giving them commands to do work, with the intervention of internet of things these devices can interact, collaborate and learn from the experiences of one another just like the humans do. The machines are in continuous touch with each other and could be pre-instructed on what to do and when to do it. These machines can even adapt to our needs and modify how they function.

As per researches over 20 million devices will be over internet using IoT services by 2020. In a nutshell IoT wants to connect all potential objects to internet in order to interact with each to provide secure, comfort life for human.

3. APPLICATIONS OF IOT

Applications of IoT can be scaled across verticals such as healthcare, manufacturing, asset tracking, street lighting etc. Internet of Things equips a multitude of domains and millions of devices with connectivity every day [1]. They are:

IoT in Everyday Life: IoT can connect our fit bits to our vehicles from our smart phones to our in-flight services from home appliances like ACs to whole entire cities. Consider a home appliance such as AC receives a message when your car is 5mins away if it is connected to cloud could be turned on before we arrived and create an ambience that we liked. This could only be possible through internet of things.

IoT in Healthcare: IoT open ways to a sea of valuable data through analysis and real time testing. IoT empowers healthcare professionals and improves the quality of care. It ultimately reduces the unsustainably high cost of medical devices. For e.g., a care device has certain parameters that are considered safe. Once one of them is breached, the sensor immediately relays this message via secure gateway to a cloud [7].

IoT in Smart cities: The only way to make a city smarter is to cater specifically to its problem. One such problem consistent among the most urban cities is traffic. For e.g. take an intelligent device like a traffic camera that can monitor the road of traffic jams, accidents and rains etc and communicate that status to a gateway. It quickly learns and predicts patterns in traffic. It will analyze the situation, predicts its impact and relay this information to other cities that connect to the highway via other own monitoring systems.

IoT in Agriculture: Manual handling in agriculture often results in loss of energy, labor cost and other inaccuracies which make all its processes less effective. IoT here can provide with the number of solutions that is precision farming, smart irrigation and smart greenhouse.

IoT in Industrial Automation: The problems faced due to manual practices in the industries are inconsistency in data entry, time consumption in production and reporting, lack of security, labor and staff training cost.

4. LITERATURE REVIEW

Farooq et al[2]discusses the security issues and challenges of the IoT system. They explained the security architecture of IoT which can provide confidentiality of the data security and privacy. They suggested that instead of focusing the attention on seeking the new possible security solutions, we have to further elaborate the accomplishments which are already achieved in IoT. The authors also suggested two-step authorization using biometric except in case of machine-to-machine communication.

Zhao et al[3]presents several security issues of IoT that exist in the three layer system structure. It gives the summary of the threats and the requirement analysis about IoT security architecture. The author lists the various attacks in perception layer, network layer and application layer such as node capture, replay attack, DoS attack, network congestion, authentication problem, data protection and recovery, identity authentication, data access permissions etc. They also focus on the security measures at each layer. Encryption is used as a security measure which is introduced in the perception layer. Network virtualization technology is used in the network layer while protection of the private information is one of the security measures in the application layer.

Chahid et al[4] gave a brief definition of the Internet of things. They proposed the three-layer architecture (protocols, layers, entities). They also mentioned the faults which are detected in each layer. They tried to analyze some solutions which help researchers to start their researches on internet of things security subject.

Zhang et al[5] presents general information of the security background of IoT .They also described the security related challenges that IoT will encountered such as object identification, authentication and authorization, privacy and malware in IoT. They tried to point out some research directions which will be performed in future work for the solutions to the security challenges. The main challenges that IoT security faces are from the heterogeneity and the large scale of objects. They discuss the new research topics and their possible solutions.

Mahmoudetal[6] presents an overview of security principles, technological and security challenges, countermeasures. They also proposed the future directions for securing the IoT. Each layer is defined by its functions and the devices which are used in that layer in IoT. The security goals of IoT are Confidentiality, Integrity and Availability (CIA). They also suggested that state of research in IoT is mainly focused on authentication and access control protocols. Due to the rapid advancement of technology, it is necessary to incorporate new networking protocols like IPv6 and 5G to achieve the dynamic mash up of IoT topology.

5. SECURITY OF IOT

Security and privacy are the two key issues for IoT applications. The data collected from the IoT sensors contains a large amount of private information and thus it needs to be preserved. There will be severe challenges involved in the security. Some of them include:

a) The IoT ranges the internet with the help of the mobile network, customary internet, Bluetooth sensor network and so on.

b) All' thing' in IoT will be linked to 'internet'.

c) These different things will connect and talk with each other. Due to this communication, the new privacy along with the security problems will arise.

Hence, there is a need for research in the areas of authenticity, confidentiality and integrity of the data collected in the IoT.

Confidentiality, Integrity and Availability are typically viewed as the primary goals and objectives of a security infrastructure [6]. They are commonly seen as security essentials that they are referenced by the term CIA triad.

6. IOT SECURITY ARCHITECTURE AND ITS FEATURES

a) IoT Architecture

Each layer is defined by its functions and the devices that are used in that layer fig.2. There are four fundamental layers that are available for any security related analysis [2]. Security issues are associated with each layer of IoT.

i) Perceptual layer is also recognized as recognition layer. It is the most basic level which gathers all types of information with the help of physical equipment that include RFID reader, GPS and all kinds of sensors which identifies the external world. Although there are different components involved, but the key component in this layer is the sensors that are used for capturing and representing the physical world. The information from them includes the properties of the objects or the things, environmental conditions etc.

ii) Network layer is the second layer in the security architecture. This is responsible for the dependable broadcast of data and information from the previous layer, initial handling of the data collected through the sensors, cataloguing and polymerization. In this layer the data broadcast is trusted on numerous basic networks which could be one of the mobile communication networks, wireless network, satellite nets etc.

iii) Support layer is a kind of the mediator between the upper layer and the lower layer. This layer will set up a dependable platform for the application layer. It also helps us in merging the application layer upward and the network layer downward. In this we have the grid and cloud computing because these are mostly used for all kinds of intelligent computing powers.

iv) Application Layer is the topmost layer. This layer delivers the personalized services based on the user needs. Application layer helps users to access the internet of things (IoT) through the interface using personal computer, mobile equipment, television etc.

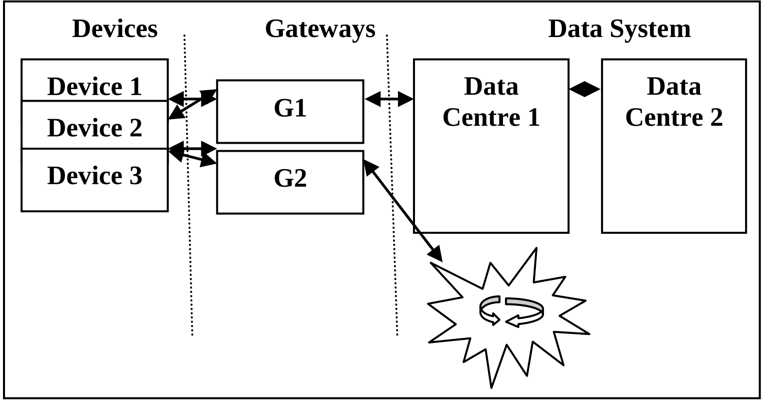

Fig.2 IoT System Architecture

b) IoT Security Features

IoT is having three characteristics: comprehensive perception, reliable transmission, and intelligent processing. Comprehensive perception is defined as the sensor nodes of perception layer having object information anytime and anywhere; reliable transmission means that the information of objects safely and completely transfer through the wireless or wired network to the data centre in real time; intelligent processing implies that middle-ware analyse and deals with the collected information before submitting to application terminal eventually. The security principles that should be imposed to achieve a secure communication framework for the people, software, processes and things are [6].

Confidentiality: Confidentiality means that only the authorized individuals/systems can view sensitive or classified information. This also implies that unauthorized individuals should not have any type of access to the data. For example, it is necessary to make sure that sensors don’t reveal the collected data information to neighboring nodes. One of the confidentiality issues is that it must address how the data will be managed.

Integrity: Integrity is defined as the consistency, accuracy and validity of data or information. It applies to systems and data. For data means that changes made to data are done only by authorized individuals/systems. Corruption of data leads to a failure for maintaining data integrity. Firewalls and protocols manage the data traffic, but it does not guarantee the security at endpoints because of the characteristic nature of low computational power at IoT nodes.

Availability: Availability describes a resource being accessible to a user, application, or computer system when required. It also applies to systems and data. If the network or its data is not available to authorized users, the impact may be significant to organizations and users who rely on that network as a business tool. The failure of a system, to include data, applications, devices and networks, generally equates to loss of revenue. E.g.: - a commercial website must never be down.

Lightweight: The processor performance of sensor nodes is lower, so it should be lightweight encryption algorithm and security authentication. Lightweight solutions are a unique security feature involved in the IoT because of the limitations in the computational and power capabilities of the devices.

Authentication: Each object in the IoT should clearly identify and authenticate other objects. Because of the nature of the IoT, the process can be very challenging. Many entities are involved (devices, people, services, service providers and processing units) and sometimes objects may need to interact with others for the first time (objects they do not know). Thus, a mechanism to mutually authenticate entities in every interaction in the IoT is needed.

Complexity: The number of security issues and complexity determines the type of the application. Each layer has certain security problems that should be considered synthetically.

Key Management Systems: The devices and IoT sensors need to exchange some encryption materials in IoT to ensure confidentiality of the data. Thus, there is a need of a lightweight key management system for all frameworks which can enable trust between different things and can distribute keys by consuming devices’ minimum capabilities.

7. SECURITY ISSUES IN THE INTERNET OF THINGS

Due to complexity, heterogeneity and a large number of interconnected resources, the security of IoT is a big challenge [5]. This led to attack on IoT system by damaging or tampering some node or from within its network by using faults in routing protocol or by using malicious program and by breaking encryption strategy. We need to understand the potential attacks and kinds of security problems of different layer. Considered the system as a whole, in the beginning of the design the security problems should be solved. The application for the security state assessment about IoT is based on grey correlation algorithm which put several common attacks as the security factor and realizes quantitative evaluation of the entire network about environment and status. It mentions the steps that we can apply to this algorithm to do the security state evaluation.

1. Security analysis in the perception layer

The perception layer is at the lowest level of IoT architecture. It is the source of access to information throughout the IoT. The security problems faced in this layer includes nodes physical capture, replay attack, sensing information leakage, side channel attacks, integrity attacks, energy depletion attacks, congestion attack, unfair attacks, denial of service attacks, and node replication attacks. The equipment used in perception layer is RFID, zigbee and all kinds of sensors [3]. Physical security of sensing devices and the security of information collection are the main security issues. The IoT cannot provide a unified security protection system due to the weak protective capability of sensing node and deployed mostly in unmanned harsh environment without a special standard and is vulnerable to the invasion and attack, which affects the security of the wireless sensor network, M2M terminal and RFID. To achieve noncontact automatic identification technology RFID technology utilizes RF communication. Information leakage (the location of the reader and user, the user information and other information), information tracking, replay attacks, cloning attacks, tampering and man-in-the-middle attacks are the various security problems of RFID.

2. Security issues in network layer

IoT faces the risks in the communication network, including illegal access, data eavesdropping, confidentiality, integrity, destruction, denial of service attacks, man-in-the middle attacks, virus attack and the use of factory examines the variety of attacks outside the tools and system vulnerabilities. Hackers can easily collect a large number of the user's privacy information because of development of the information retrieval technology and social engineering. Since the Internet of things senses a large number of devices and data collected in a variety of formats, thus the data information has a massive, multi-source and heterogeneous characteristic. Heterogeneity makes security interoperability which resulted into the coordination of network becoming worse [3]. This causes the network layer bring more complex security issues, such as data transfer needs a large number of nodes leading to network congestion, resulting in denial of service attacks.

3. Security issues of application layer:

The close integration between computer technology, communication technology and industry professional, has resulted in the widespread applications of IoT which can find nuisance in many aspects. The applications face many extra security issues, besides the business in the traditional communication network abuse such as replay attacks, application of information security issues such as eavesdropping and tampering. It has become particularly prominent, including cloud computing, middleware, data mining, data storage and backup, management and authentication mechanisms, information disclosure, intellectual property rights and privacy protection security issues. Since each application will have a large number of users. It will be used differently by various users. Effective authentication technology should be used in order to prevent illegal user intervention. The ability to process mass data leads to a large number of nodes which results into an enormous amount of data transmission and complex environment. The interruption and loss of data will occur once the data processing capacity and adaptability cannot meet the requirements.

8. CHALLENGES IN IOT SECURITY

Heterogeneity and the large scale of objects are the main challenges for IoT Security [5] which is difficult to deal with. Each IoT layer is vulnerable to security threats and attacks. The following section discusses a detailed analysis of the security issues with respect to each layer.

1. Perception Layer Challenges

The IoT perception layer mainly consists of sensors and RFIDs. The storage capacity, power consumption, and computation capability of sensors and RFIDs are very limited making them vulnerable to many kinds of threats and attacks [8].

RF Interference on RFIDs: By sending noise signals over radio frequency signals, the attacker performs Denial of service (DoS) attack. These signals are utilized for RFID's communication.

RFID Cloning: In this type of attack, adversary copying data from pre-existing RFID tag to another RFID tag [4]. Original ID of RFID tag is not copied. The attacker can insert wrong data or control the data passing via the cloned node in a way so that the reader can't distinguish between the original and the compromised tag.

Node Capture attack: In this attack, attacker can add another node to the network and then threatens the integrity of the data in this layer by sending malicious data. The attackers restrained the key nodes such as gateway node.

RFID Spoofing: An attacker spoofs RFID signals. It captures the information which is transmitted from a RFID tag. Spoofing is when an attacker gives wrong information which seems to be correct and then the system accepts that information.

2. Network Layer Challenges

The data is transmitted from the sensor by network layer consisting of Wireless Sensor Network to its destination with reliability. The related security issues are:

Sleep Deprivation Attack: The aim of the attacker is to use more power as a result battery lifetime is minimized which results in shutting down of nodes.

Sink Hole Attack: It is a type of attack where an adversary compromises a node inside the network and performs the attack by using this node. It tries to attract network traffic by sending the fake routing information to its neighboring nodes so that it has the minimum distance path to the base station [2]. It can then alter the routing information and drop the packets also.

Man in the Middle Attacks: The attacker over the internet intercepts the communication between the two nodes hideously by pretending the identity of the victim. They obtain the sensitive information by eavesdropping in which the target of the attack is communication channel.

Denial of Service: An attacker floods the network with large traffic and makes the services unavailable to its intended users [4].

Sybil Attack: In this attack, malicious node takes the identities of multiple nodes and acts as them resulting in false information. For e.g. voting system single node can vote many times in case of wireless sensor network.

3. Application Layer Challenges

Application layer security challenges are more complex and costly. The related security issues of this layer are discussed below:

Denial of Service: The attacker blocks the users from the application layer make the device, resource or network unavailable to authorized users by denying services.

a. **Phishing Attacks:** The adversary captures the private information like username, passwords by email spoofing and by using fake websites [2].

b. **Malicious Code Injection:** By injecting malicious code, the adversary physically introduces it into the node of IoT system. The attacker can get full control of IoT system which results in stealing some kind of data from the user.

c. **Sniffing Attack:** In a sniffer attack, an attacker can force an attack on the system by using a sniffer application (an application aimed at capturing network packets) into the system, which could gain information to eventually cause the network to corrupt or crash of the system.

9. CONCLUSION

In this paper, well-defined architecture for the IoT security was presented. We have discussed the security goals, possible security challenges and issues of the IoTsystem. With the development of IoT industry, its importance of the security is being increased simultaneously and in today's ever-expanding world of technology IoT has emerged as its most prominent and significant component. IoT also faces many security threats with its development. Currently, many researchers are undergoing for the safety of IoT but there are still in initial stages and due to this the safety mechanism is yet to be developed perfectly. This is the reason we need an impenetrable security mechanism which handles maximum security problems to find a secure and efficient solution.

10. ACKNOWLEDGEMENT

The paper is the outcome of study done during previous few years and will be helpful to the students that are new to the field as this will provide them with nut shell information regarding this ever expanding field. It is also going to help with larger perspective to the people in the field of academia, research and IoT applications developers to a greater extent.

11. REFERENCES

[1] K. Ashton, "That 'Internet of Things'thing",*RFiD Journal,* 2009.

[2] M.U. Farooq,MuhammadWaseem, AnjumKhairi, SadiaMazhar,"A Critical Analysis on the Security Concerns of Internet of Things (IoT),"International Journal of Computer Applications (0975 8887) Volume 111 - No. 7, February 2015.

[3] Kai Zhao, LinaGe,"A Survey on the Internet of Things Security," Nineth International Conference on Computational Intelligence and Security, 2013.

[4] Yassine Chahid, Mohamed Benabdellah, Abdelmalek Azizi ACSA Laboratory,"Internet of Things Security"

[5] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, "IoT Security: Ongoing Challenges and Research Opportunities,"2014 IEEE 7th International Conference on Service-Oriented Computing and Applications.

[6] Rwan Mahmoud, TasneemYousuf, FadiAloul, Imran Zualkernan,"Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures,"10th International Conference for Internet Technology and Secured Transactions (ICITST-2015).

[7] S. M. Riazul Islam, Daehan Kwak, Md.Humaun Kabir, Mahmud Hossain, And Kyung-Sup Kwak, The Internet of Things for Health Care: A Comprehensive Survey, 2169-3536 2015 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission.http://www.ieee.org/publications_standards/publications/rights/index.html for more information. VOLUME 3, 2015.

[8] Falguni Jindal, Rishab Jamar, Prathamesh Churi, Future and Challenges of Internet of Things, International Journal of Computer Science and Information Technology (IJCSIT), Vol. 10, No. 2, April 2018.

12. AUTHOR'S PROFILE

Mubashir Hussain pursed Bachelor of Computer Applications and Master of Computer Applications from University of Kashmir, and University of Jammu, Jammu and Kashmir, India. Currently he is pursuing his Ph.D. from University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India and has worked Assistant Professor in PG Department of Computer Applications, MIET, Jammu, Jammu and Kashmir, India. He has qualified National Eligibility Test conducted by University Grants Commission for higer education and JK State Eligibility Test conducted by University of Kashmir, Jammu and Kashmir, India. His main research work focuses on Website Design Analysis, Big data sciences, Cloud Computing, Big Data Analytics, Machine Learning and Computational Intelligence based reaearch fields.

Saqib Mohammad pursed Bachelor of Engineering and Master of Technology from University of Jammu, Jammu and Kashmir, India. Currently he is pursuing his Ph.D. from SRM University, Delhi NCR, India. He has qualified National Eligibility Test conducted by University Grants Commission for higer education. His main research work focuses on Big data sciences, Cloud Computing, Network Security, Machine Learning and Computational Intelligence based reaearch fields.