Comprehensive Survey on Security Problems and Key Technologies of the Internet of Things (IoT)

Jinal P Tailor
Department of Information Technology
Shri S'ad Vidya Mandal Institute of Technology
Bharuch, India

Ashish D Patel
Department of Computer and Information Technology
Shri S'ad Vidya Mandal Institute of Technology
Bharuch, India

***Abstract*— Internet of things (IoT) is a collection of many interconnected objects, services, humans, and devices that can communicate, share data, and information to achieve a common goal in different areas and applications. The vision of IoT is to enable devices to collaborate with each other on the Internet. IoT security focuses on authentication and access control protocols. IoT security is the area with protection connected devices and networks. There are many key challenges in designing a secure IoT: Privacy, Authentication, Access Control, Trust, Confidentiality, Mobile Security, etc. Attacks on IoT security devices are physical attacks, side channel attacks, cryptanalysis attacks, software attacks, network attacks. This paper describes Security Problems of IoT, Security issues and Key Technologies of IoT.**

***Index Terms*- Internet of Things, Security issues, Security in IoT.**

I. INTRODUCTION

The Internet of Things (IoT) is considered as a network of highly connected devices. The concept of the IoT is being connected strongly by developments in computing network and developments in the next generation Internet. IoT is a technology where objects will able to connect to each other (e.g. machine to machine) and communicate through the Internet. The focus of IoT is on the data and information, rather than point-to-point communication [11]. The Internet at the start was mostly defined by the World Wide Web which was a collection of linked HTML. IoT is characterized by the presence of hardware, software and middleware components collaborating with each other [9]. The Internet has changed the world in many ways and with the introduction of devices connecting to the Internet, a new dimension to the Internet has arisen. The interconnection of the devices helps in improving people's lives through automation and growth [9].Now a day, The Internet of Things has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items [13]. This paper describes Key Technologies, Security Issues, Security Problems and Security Measures of IoT. The applications area of the IoT includes smart homes, smart cities, industrial automation, etc.

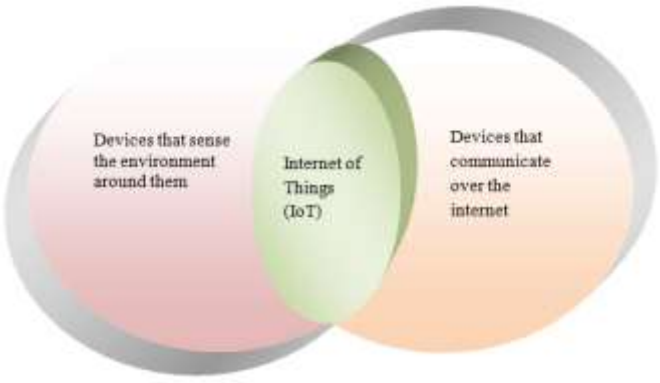

Fig. 1: Internet of Things Architecture

II. KEY TECHNOLOGIES FOR IOT SECURITY

A. Certification and Access Control:

Certification specifies the implementation way that the both sides communicate with each other and can confirm the true identity of each other. Access control technology in the perspective of the IoT has extends from authorization and access control for people to use of machines and objects, which effectively blocking the banned entity access to resources. Access control technology can be correctly implemented on the basis that certification technology can ensure the entities identification. For example, we can do node to node identity certification before communication; or design a new key agreement scheme, so that the attackers cannot or hardly derive key information from the node information they obtain [3].

B. Data Encryption:

Data encryption is an important means of protecting data security. Data encryption technology aims to protect the confidentiality and integrity of information transmission and to prevent theft or damage while transmission. In IoT, the encryption can be taken by two ways that are hop by hop encryption (node to node) or end to end encryption. The first is processed in the network layer to understand cipher text conversion on each node. The end to end encryption execute on the application layer, the sender encrypts only decrypted at the receiving end [3].

C. Middleware:

In IoT, the middleware is located in fixed devices of server-side, the perception layer and transport layer of the IoT. In which server-side is called as IoT transaction basis middleware. The middleware's feature is to hiding the details of different technologies is fundamental to free from the programmer from issues that are not directly relevant to their focus, which is the development of the specific application enabled by the IoT infrastructures [3].

D. Cloud Computing:

Cloud computing is a good technical support for IoT. Two key conditions must be considered when combining cloud computing with IoT:(1) Scale is the basis for combination. It is possible for IoT to combine with cloud computing only when its scale is large enough. (2) Practical techniques are achieving condition. Appropriate business model and practical services can make IoT and cloud computing better provides human and society [3].

III. SECURITY ISSUES IN IOT

A. General Security Issues

i. Access Control

Access control concern with access rights given to the devices in IoT atmosphere. Two words that describe for Access Control are: Data Holders that are Users, who send/receive data to device. They must send data to authenticated things and Data Collectors that are Things, which must authenticate users. All access control models can be performed using either a distributed or centralized architecture. In distributed architecture, an access control server allows access tokens to users, who use to access the IoT devices directly. In centralized architecture, the user accesses only cloud-based servers that approve the request and relay data between the user and the IoT devices. Identity management and authentication are important supporters (enabler) for access control, and to control access it must to be able to identify users and devices [11].

ii. Privacy

Internet of Things privacy is the particular considerations essential to protect the information of individuals from coverage in the IoT environment. The IoT devices gather a huge amount of information and also carry a large potential of privacy risks in relative to the use of the data and its access [11].

iii. Trust

The concept of Trust is used in various contexts and with different explanations. The satisfaction of trust constraints are closely connected to the identity negotiation and access control effects. A main difficulty with many approaches towards trust definition is that they do not lead to the organization of metrics and evaluation technique [11].

iv. Mobile Security

Mobile Security nodes in IoT commonly move from one cluster to another, in which cryptography based protocols are used to allow expeditious identification, authentication, and privacy protection [11].

v. Confidentiality

Confidentiality is generally the same to privacy. A good example of methods used to make sure confidentiality is an account number when banking online. A very key important component of protecting information confidentiality is encryption. Encryption ensures that only the right people can read the information [11].

B. Layer wise Security Issues

There is need to understand all kinds of security problems of different layer, and potential attacks. Considered the system as a whole, the security problems should be solved at the beginning of the design. The following paper will discuss the security problems in each layer [3].

i. Perception Layer Security Problems

The main equipment in perception layer includes RFID, Zigbee, and all kinds of sensors. When data are collected, the way of information transmission is basically the wireless network transmission. The signals are exposed in the public place. The most of sensing devices are deployed in the unmanned monitoring sites. The attackers can easily gain access to the equipment, control or physically damage them. For instance, DPA (Differential Power Analysis) is a very effective attack [3].

ii. Network Layer Security Problems

- Traditional Security Problems. General security problems of communication network will threat to data confidentiality and integrity. Although the existing communication network has a relatively complete security protection measures, there are still some common threats, including illegal access networks, eavesdropping information, confidentiality damage, integrity damage, DoS attack, Man-in-the middle attack, virus invasion, exploit attacks, etc [3].
- Compatibility problems. The existing Internet network security architecture is designed based on the perspective of person, and does not necessarily apply to communication between the machines. Using the existing security mechanisms will split the logic relationship between IoT machines [3].

iii. Application Layer Security Problems

In application layer, for different industry or environment, its security issues are also different. At present there are no universal standards for the construction of IoT application layer. But some enterprises carry out M2M (Machine to Machine) mode of IoT, such as intelligent community, intelligent household, medical, etc [3]. Application layer

security is more complex and intense; it can still be summed up some common security problems:

a) *Data Access Permissions, Identity Authentication:* Different applications have different users; each application will have a large number of users. So in order to prevent the illegal user intervention, should take effective authentication technology [3].

b) *Data Protection and Recovery:* Data involve user privacy. Data protection mechanism and data processing algorithm are not perfect, and it may cause data loss and even catastrophic damage [3].

IV. IOT SECURITY MEASURES

This section introducing security measures for each layer will focus on the security technology involved in perception layer.

A. Perception Layer Security Measures

RFID and WSN are an important part of IoT perception layer, their security measures are described here.

i. RFID Security Measures:

a) *Data Encryption:* In RFID data security system, it is essential to encrypt the RFID signal [4].

b) *Access Control:* To prevent the user's privacy leaks, RFID tags protect the user's information and do not allow user's information to leak [4].

c) *Based on IPSec Security Channel:* IPSec protocol provides two types of security components: authentication and encryption. To confirm the sender's real identity, authentication mechanism is used at the receiver of IP communication data. Data encryption mechanisms prevent enemy from eavesdropping (gossip) and various data during transmission, and encode data for ensuring data confidentiality [4].

d) *Cryptography Technology Scheme:* Cryptography technology not only can realize the user privacy protection, but also can protect the confidentiality, authenticity and integrity of the RFID system [4].

ii. Wireless Sensor Network Security Measures:

a) *Key Management:* The design of security requirements of WSN key management mainly reflects in security of key generation, forward privacy, backward privacy and extensibility, against collusion attacks and source authentication [4].

b) *Intrusion Detection Technology:* IDS (Intrusion Detection System) can observe the performance of network nodes, and find the doubtful behavior of nodes [4].

B. Network Layer Security Measures

In the existing structure of IoT, network layer exists based on the Internet or the existing communication network, old network communication technology is not completely adapted to IoT. Due to huge amount of data, network availability should be measured. In addition it also should support cross-domain authentication and cross network authentication in network layer. Network virtualization technology reduces the complexity of network management, and the possibility of wrong operation [4].

C. Application Layer Security Measures

The Applications of IoT application layer have variety and uncertainty. It shows up that different application environment have different security needs. There are two main aspects of the measures such as Technical and Nontechnical. Technical contains Across Heterogeneous Network Authentication and Key Agreement and The Protection of the Private Information. Nontechnical contains Increasing the Awareness of Safety and Strengthen Information Security Management [4].

V. CONCLUSION

IoT is the first step towards using Internet anywhere and anytime. IoT is identifying by the presence of hardware, software and middleware mechanism collaborating with each other. The target of IoT is on the data and information, rather than point-to-point communication. Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), Addressing Schemes, Data Storage and analytics, Visualization, etc are some of the elements in IoT environment. Security issue should be the first thinking in the development of the IoT. The Internet of Things (IoT) is a rising and promising pattern that can be considered as an extension of the Internet to interconnect all smart objects. To secure the IP-based Internet of Things it focuses on secure network access, key management, and secure communication. The most essential requirement for the IP-based IoT environment is Security and Privacy. Confidentiality, Integrity, Availability, etc are some security functions for the smart home system. A user privacy data leakage, social infrastructure stopping, and economic losses and a risk of human life can be occurred in the IoT environment. The IoT is a category of intelligent method, which uses intelligent things with perception, communication and computing ability to take different information in physical world and interconnects the physical objects which can individually addressing. The applications area of the IoT includes smart homes, smart cities, industrial automation, etc. IoT promises to lead in a new, fully interconnected "smart" world, with relationships among objects and environment and objects and people becoming more closely connected. Thus this paper includes Key Technologies, Security Issues, Security Problems and Security Measures of IoT.

REFERENCES

[1]. Oscar Garcia-Morchon, Sye-Loong Keoh, Sandeep S. Kumar, Pedro Moreno-Sanchez, Francisco Vidal-Meca, and Jan Henrik Ziegeldorf, Securing the IP-based Internet of Things with HIP and DTLS, ACM, 2013

[2]. Quandeng GOU, Lianshan YAN, Yihe LIU and Yao LI, Construction and Strategies in IoT Security System, IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, IEEE, 2013.
[3]. Xu Xiaohui, Study on Security Problems and Key Technologies of The Internet of Things, International Conference on Computational and Information Sciences, IEEE, 2013.
[4]. Kai Zhao, LinaGe and Guangxi, China, A Survey on the Internet of Things Security, Ninth International Conference on Computational Intelligence and Security, IEEE, 2013.
[5]. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh and IEEE Fellow, IoT Security: Ongoing Challenges and Research Opportunities, IEEE 7th International Conference on Service-Oriented Computing and Applications, IEEE, 2014.
[6]. Somia Sahraoui and Azeddine Bilami, Efficient HIP-based approach to ensure light weight end-to-end security in the internet of things, ELSEVIER, 2015.
[7]. Kim Thuat Nguyen, Maryline Laurent and Nouha Oualha, Survey on secure communication protocols for the Internet of Things, ELSEVIER, 2015.
[8]. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul and Imran Zualkernan, Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures, The 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2015.
[9]. Rajendra Billure, Varun M Tayur and Mahesh V, Internet of Things - A Study on the Security Challenges, IEEE, 2015.
[10]. Jin Hee Han, YongSung Jeon and Jeong Nyeo Kim, Security Considerations for Secure and Trust worthy Smart Home System in the IoT Environment, IEEE, 2015.
[11]. Ashvini Balte, Asmita Kashid and Balaji Patil, Security Issues in Internet of Things (IoT): A Survey, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.
[12]. Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song and David Wagner, Smart Locks: Lessons for Securing Commodity Internet of Things Devices, ACM, 2016.
[13]. http://www.internetsociety.org/sites/default/files/ISOC-IoT/Overview/20151014_0.pdf