Indian Journal of Science and Technology, *Vol 10(3), DOI: 10.17485/ijst/2017/v10i3/110642, January 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Security and Privacy Challenges: Internet of Things

Seema Nath[1] and Subhranil Som[2]

[1]Department of Management and Information Technology, Ideal Institute of Management and Technology, Guru Gobind Singh Indraprastha University, Dwarka, Delhi-110078, India; seemanath.iimt@gmail.com,
[2]Amity Institute of Information Technology, Amity University, Noida-201303 Uttar Pradesh, India; ssom@amity.edu

Abstract

Background/Objectives: This survey reports on the current research on the Internet of Things by examining the related literature, identifying current trends, challenges that threaten IoT and future directions. **Findings:** Most of the people use the Internet every day but little knows how it really works. Now a Days internet of things (IoT) has been area of research as many heterogeneous devices are connected through internet. This will capacitate the devices with new abilities. In such a case, the confidentiality of data plays an important role. It includes data validation and confidentiality, secrecy and reliability amongst various users and the constraints of security and privacy policies. Traditional security methods cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Moreover, the amount of more interconnected devices will lead to less adaptability; so a more modifiable structure is needed to deal with security threats in a drastically dynamic environment. **Application/Improvements:** The concept of loT brings a new challenge regarding privacy, security, confidentiality, reliability and trust. The major issues are lot of devices are not protected under mechanisms such as firewalls and are not following the specific standards. They are easily attacked by wireless channels. Such devices can be stolen and can be analysed by attackers to reveal their key material. Combining data from different sources is the other major issue since there is no guarantee of security between data providers and data consumers from very beginning. Secure exchange platform is required between IoT devices and consumers of their information.

Keywords: Adaptability, Heterogeneous Devices, Internet of Things, Privacy, Security

1. Introduction

IoT is an interface of things wirelessly connected with the help of intelligent and reliable. Objects with this facility will be able to have an interface without any human interference. Some applications in IoT are developing in healthcare, transportation, automotive industries, & electronic meters. The concept of IoT is quite complex and has multiple folds, it includes distinct technologies and services[1].

Gubbi describes a brief look upon the various aspects of IoT, for example the technologies included are various applications, cloud services, architecture, total power utilization and reliability problems, peculiarity of service and data mining implications:

The development of IoT involves several issues such as connected devices, communication network, standards, protocols and interfaces.

The security, confidentiality and integrity needs to be ensured, along with validation and validation mechanisms in order to prevent illegitimate users to access the system[5].

The most important and concerned issue is confidentiality, users private data has to be ensured, since devices will also be managing sensitive information.

The rest of the report includes the following: In Section 2, Enabling technologies are studied. In section 3, analyzing available approaches regarding confidentiality and authentication, Sections 4 deal with privacy issues. In Section 5, Application of IoT is reviewed. At the end future research directions are discussed.

**Author for correspondence*

2. Enabling Technologies in IoT

IoT was referred as uniquely distinguishable exchangeable connected objects with radio-frequency identification (RFID). It is defined as "a dynamic global network infrastructure with self-configuring capabilities based on exchangeable communication protocols; physical and virtual things in IoT have identities and attributes that are capable of using intelligent interactions and being integrated as an information network". IoT is generally a parent class of combined devices that are exceptionally distinguished through field communication technology.

The words "Internet" And "Things" means a correlated network which is worldwide has sensoring capacities, communication systems, networking, and data processing, that may be a new variant of information and communications technology (ICT). Inspite of many arguments on the definition of IoT, technologies are developing at a fast pace by many institutions, intelligent sensoring along with wireless communication technologies are now a part of Internet of Things and new demands have arisen. International Telecommunication Union (ITU) talked about technologies, potential markets, and emerging challenges and the impacts of Internet of Things. Evolution of IoT is picturized in various stages. The IoT is initiatialised by using RFID technology that is used in pharmaceutical production, logistics and various other areas of applications. The emerging wireless sensor technique has widely advanced the sensory capacities of devices and hence the concept of Internet of Things extends from here toencompassing smartness and self-governing controls. Wireless sensor networks (WSNs), smart sensing, NFC, barcodes, cloud computing and low energy wireless communications are examples of some technologies that have been introduced in IoT till now. Evolution of such technologies leads to new technologies of IoT. IoT delineates the new era of Internet, wherein objects will be accessible and identifiable via Internet. The fundamental concept of IoT implies that the connected objects can be distinguished distinctly in virtual representation. Each and every object can communicate and interchange data, process and modify data according to some predesigned techniques.

2.1 Current Research

During the recent years, RFID-based authentication is used widely in pharmaceutics, logistics and retail. Since 2010, along with the new advancements in smart sensing techniques, less power wireless communication, and networking through sensor technology, things can now be networked to internet. For providing services to users through application, technical standards are defined and structured based on the particularization of data processing, and data communication in the network itself. Things connected to internet must be able to exchange data with each other simultaneously. When billions of things are integrated smoothly and effectively, IoT can then have various applications. Emergence of such technologies originates new technologies in IoT. IoT delineates the new era of Internet, wherein objects will be accessible and identifiable via Internet. The fundamental concept of IoT implies that the connected objects can be distinguished distinctly in virtual representation. Each and every object can communicate and interchange data, process and modify data according to some predesigned techniques. Each and every object is able to communicate and interchange data, process and modify data according to some predesigned techniques.

3. Authentication and Confidentiality

The approach for authentication uses a mechanism which is a custom encapsulation mechanism, intelligent Service Security Application Protocol.

A secure communication system is established along with cross platform communication, encryption, authentication and signature so as to improve IoT's application development capacity. The first completely implemented two way validation security technique namely Datagram Transport Layer Security (DTLS) protocol that resides in the transport and application layer.

Concerned with confidentiality/secrecy and integrity, it is noted the already existing main management systems can be useful in the IoT context. Key Management System (KMS) protocols are classified in four main categories - key pool framework, negotiation framework, mathematical framework and public key framework. Key pool framework suffers from improper connectivity as well as the deployment knowledge to upgrade the structuring of data structures is used by mathematical framework, but this is not possible, combinatorics-based protocols writher from authentication, scalability & connectivity; the wireless channel and its inherent features to negotiate a common key are used by negotiation, but they are also not suitable as the server and client nodes have different networks and has to route the information via Internet[2].

The basic requirements for such schemes are multiple countermeasures to manage the authentication of various devices. For instance, there is a framework that is on PKI. A transmission model which has signature encryption technique addresses IoT security requirements which actually mean trustworthy, confidentiality and attack-resistant with the help of some Object Naming Service queries.

In this process of transmission, the data of object is wrapped in various layers of encryption with routing the node's public key by Remote Information Server of Things(R-TIS). Data which was encrypted is decrypted at each routing node, until a plain text is received by Local Information Server of Things (L-TIS). At the same time, the integrity of data that is received and the credibility of the routing path in the process of transmission can be checked with the help of nodes[3].This kind of model for transmission leads to low resistance for attacks. To ensure confidentiality a unique and a précised solution is lacking.

Many initiatives have been done in this field but several questions came up:

- Considering heterogeneity of the devices which are connected, are the WSN proposals applicable?
- Is it best to start with a new solution to reuse classic security mechanism?
- Which key Managing mechanism is suitable the most?
- How end to end integrity verification mechanism is ensured so that the system is more resistant to malicious attacks?

Few new studies have started answering to such questions. There is validation/authentication protocol where lightweight encryption method is used based on XOR manipulation for anti-counterfeiting. Initially with WSN context, user authentication and key agreement scheme for heterogeneous wireless sensor network is proposed.

Establishment of the key session on the basis of elliptic curve Cryptography was aimed by the authentication and access control method that is another lightweight encryption mechanism. An attribute authority manages the attribute-based access control policies that are defined by this scheme enhances mutual authentication among the users & sensory nodes, as well as solving the resource-constrained issue at application level.

4. Privacy in IoT - Privacy Enhancing Technologies (PET)

It is difficult to fulfil the customer privacy requirements. Technologies are developed to achieve information confidentiality[4]. Privacy Enhancing Technology (PET) is explained as follows:

1. Virtual Private Networks (VPN) isan extranet originated by groups of business partners. Since partners have access only, the data is confidential and has integrity. VPN doesn't allow worldwide data exchange dynamically, it is highly inappropriate with respect to third parties.
2. Confidentiality and integrity of the IoT can be improved by Transport Layer Security (TLS). The information search could be negatively affected because of many additional layers as each ONS delegation step requires a new TLS connection.
3. Public key cryptography is used by DNS Security Extensions (DNSSEC) to sign resource records to guarantee authenticity and integrity of delivered data. Only global ONS information authenticity is assured by DNSSEC if the entire internet community adopts it. The internet traffic is encrypted and mixed using Onion Routing from various sources i.e. data is packed in many layers of encryption. Such a process will obstruct the match of a specific Internet Protocol. But onion routing increases time complexity resulting in issues with the performance. To hide which customer is interested in which particular information we use Private Information Retrieval (PIR) systems. A system such as ONS that is globally accessible system arises due to problems of key management and scalability and makes this method impractical. In order for increasing security and privacy we use Peer-to- Peer (P2P) systems that gives high scalability and good performance. These are based on Distributed Hash Tables (DHT). The customer authentication is done by using public-key cryptography[6].

5. Applications of IOT

Information gathering, transmitting and storing is ensures by IoT for the objects that are equipped with sensors/tags. IoT has its applications in areas such as retailing, healthcare, smart shelf operations,

travel, management, manufacturing, environmental monitoring, food, restaurants, library services, logistics and many more.

All this shows that IoT plays a key role in our society. In order to increase its areas of applications, the growing IT sector plays an important role. In the coming years IoT can largely contribute to address all the issues i.e both public and social.

Currently, the areas where IoT has already been deployed are:

- To allow the users access additional information regarding products, many hardware and software components (social networks, RFID tags, mobile apps and mobile phones) are used.
- With help of unique distinguishing techniques, like RFID tags, barcodes and intelligent sensors, many products are being made. Such technologies help the products to be monitored and tracked in their life cycles[7].
- Efficiency of old industries is increased by new data exchange and processing techniques.

5.1 Industrial Applications

Smart service networks in business transactions can increase the effectiveness of real-time data processing and managing applications, like critical data storage, online-payment and aggregated QoS.

In intra & inter-organizations certain business models could be benefited, with more profitable, competitive products, and greener business models, real-time information pro-cessing and optimized resources. Manufacturers can have a benefitted, where business partners can integrate the enterprise's resources.

5.2 Social IoT (SIoT)

A world where everything around humans would be intelligently sensed, networked and tracked was described by a concept proposed namely as "Social Internet of Things (SIoT)". The marketability of Internet of Things can be effectively improved by SIoT. The confidential technologies used in social networking websites can be used to improve confidentiality[8].

The concept of SIoT motivated all thesocial networks: Twitter, Facebook and micro-blog. The scientists and researchers in fields such as Electronic learning, Electronic business, sociology, networking and psychology are influenced by SIoT.

5.3 Healthcare Applications

Another important application of Internet of Things is healthcare. It has enhanced service quality and reduced costs. Medical parameters like blood pressure, body temperature and blood glucose level can be monitored via certain sensors. The driving forces for the implementation of IoT in healthcare are the advancements in sensors, data processing technologies and wireless communication technologies. The wearable body sensor networks (WBSNs) are also developed to continuously monitor activities of the patients.

The current living solutions can be improved by IoT. The medical devices that can be connected to internet are some wearable sensors and medical sensors. To collect information and transmit them to remote medical centers they can be used. Devices with wearable biosensors are used in tracking daily activities, monitoring patients and to take care of elderly people. Intelligent medical sensors can enhance the life quality rapidly and will be able to prevent the emergence of multiple health problems. Low cost medical sensors are combined with objects wirelessly; it will become practicable to develop implementable sensors to track patient's health. The BLE-based technologies are applied to connect things such as smart phones, personal computers, home appliances and body sensors for the applications in fitness healthcare, security, and entertainment.

The sudden development healthcare applications create a large industry in this area of application. Many portable health applications have been developed to serve healthcare tasks such recording of blood glucose or the measurement of blood pressure.

6. Scope of Paper

It is observed that the research done on Internet of Things is mainly focused only on different types of technology and its area of application. It is obvious as Internet of Things is something which has not been identified yet. As this enhances and matures, the research on IOT will expand to various fields such as: law, management, operations economics and sociology and many more. Through Literature Review we yielded some important findings that help us to understand concept of IOT as well as give new opportunity to scholars working on it.

7. Conclusion

The concept of loT brings a new challenge regarding privacy, security, confidentiality, reliability and trust. The

major issues are lot of devices are not protected under mechanisms such as firewalls and are not following the specific standards. They are easily attacked by wireless channels. Such devices can be stolen and can be analysed by attackers to reveal their key material.

Combining data from different sources is the other major issue since there is no guarantee of security between data providers and data consumers from very beginning. Secure exchange platform is required between IoT devices and consumers of their information.

8. References

1. LiS, Da Xu, L, Zhao S. The internet of things: a survey. Information Systems Frontiers.2015; 17(2):243–59.
2. Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks. ACM Transactions on Information and System Security (TISSEC). 2005;8(1): 41–77.
3. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: Vision, applications and research challenges. Ad Hoc Networks. 2012;10(7):1497–516.
4. Emmerson B. M2M: the Internet of 50 billion devices. WinWin Magazine. 2010;(1):19–22.
5. Weis S. A. Security and privacy in radio-frequency identification devices. Doctoral dissertation, Massachusetts Institute of Technology. 2003.
6. Weber R. H. Internet of Things–New security and privacy challenges. Computer Law & Security Review. 2010;26(1):23–30.
7. Saini R., Khari, M. Defining Malicious Behavior of a Node and its Defensive Techniques in Ad Hoc Networks. Journal of Smart Sensors and Adhoc Networks (IJSSAN). 2011;1:18–21.
8. Sinha A, Kumar P. A Novel Framework for Social Internet of Things. Indian Journal of Science and Technology. 9(36).