IPHV8I1075X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

SECURITY ISSUES IN INTERNET OF THINGS

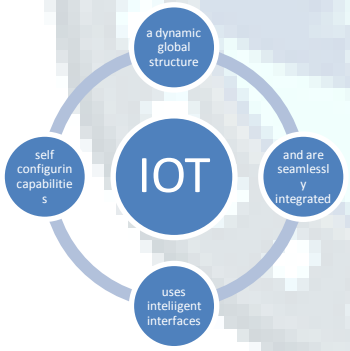
[#1]S. HAR PREETH KAUR, M.Tech Student,
[#2]SUBHASH PARIMALLA, Associate Professor,
Department of CSE,
JYOTHISHMATHI INSTITUTE OF TECHNOLOGICAL SCIENCES,KARIMNAGAR,T.S,INDIA.

ABSTRACT: In these days, people are using internet at anywhere and at any time. Internet of things is nothing but a proposed development of internet in which everyday objects have network connectivity allowing them to send and receive the data. IOT can be utilized by various technologies which gives such creative services in different applications. This implies that IOT deals with various challenges on security and privacy. so, we need to invent flexible security mechanism which can provide a better environment for IOT.[1].

Index Terms—Privacy, Authentication, Access control, Trust, Data Integrity.

I. INTRODUCTION

Internet of things can be defined as "A world where physical objects are seamlessly integrated into the information network and where the physical objects can become active participants in business process. Services are available to interact 'smart objects' over internet, query and change their state and any information associated with them, taking into account security and privacy issues".



IOT Definition

Now a days, internet has become very important in people's life. The IOT[1] refers to the ever growing network of physical objects that feature an IP address for internet connectivity and the communication that occurs between these objects and other internet enabled devices and systems.

Examples of objects that can fall into the scope of IOT which includes connected security systems, cars, thermo stats, electronic appliances, lights in house hold, speaker systems, vending machine to machine and more. As far as the reach of IOT[2], there are more than twelve billion devices that can currently connect to the internet and researcher's at IDC estimate that by 2020 there will be 26 times more connected things than people.

More objects are becoming embedded with sensor's because of which they are gaining the ability to communicate with objects. The resulting information networks promise to create new business models, improve business process and reduce cost and risks.

The purpose of IOT is to make a smart city by which it can gain the ability of public resources and improve the services which can be offered to people. [2]. IOT is aimed at enabling the inter connection and integration of physical world and also, the cyber space.

Here, we discuss related technologies, research challenges, fundamental's of IOT involved in IOT development. The objective of this proposal is to provide detailed information regarding security issues in IOT.

The important challenges while building IOT are

A. Device Heterogeneity

IOT use to connect several smart devices such that connecting heterogeneous devices is a challenge to build an IOT. These devices run by using different platforms and also uses protocols for communication purpose. Here it is especially magnified with emergence of IOT, which is turning 'heterogeneous networks' into super 'heterogeneous networks' of intelligent devices.

B. Scalability

Next challenge we need to focus on Scalability. As, in IOT every day we need to connect number of devices or objects to network. It raises some issues such as naming, addressing conventions, service management, information management.

C. Ubiquitous data exchange through wireless technologies

Here the wireless technology uses smart devices to connect and such issues it involves are network delays, congestion etc.

D. Energy optimized solution

IOT major constraint is energy optimized solution. Many devices which are connected through network utilize more energy for data communication. H ere the challenge will be to decrease the energy used for data communication between various devices.

E. Tracking Behavior and Localization

It is required to know the identification of the object and also tracking capability such as when products are connected to sensors, companies can track the movement of the product. Some companies are also providing location sensors in cars

through which company can know where the car is driven and where it travels.

F. Self-organization

Objects need to have sense of environment without any human interaction such as satellite sensing weather forecast, Interoperability and Data management

A format should be maintained in such a way that data can freely transfer between different applications without any lose of data.

G. Security And Privacy Preserving Mechanism

It is a major challenge in IOT. Because of it ,a design have to be developed so that the security and privacy can be maintained. Here the main issue is "less security" which can give or raise the issues like man-in-middle attacks, exploitations of web applications. It can also involve issues like network delays, congestion, availability etc.

II. RELATED WORK

Many papers have been suggested to address the issues related to IOT. This paper discuss about the security issues in IOT in which it depicts on data confidentiality, privacy and trust.

A lot of research has been done to solve the issues on security. The problem of security based on Privacy, Trust and Authentication has been studied by different researchers [10,14,15].

Various solutions are provided by Cisco which provides solutions not only for backing everything with financial cloud but also enabling the integration of every things software platform with Cisco's IOX and CMX hardware technology. This creates an extremely powerful solutions when it comes to tracking and managing the data flow to/from in IOT context.[15].

"Big data privacy in IOT" proposed by Charith Perara [16].studied that the solutions are capturing large amount of data pertaining to environment and also their users. The objective of IOT is to serve more the system users and to learn more. Some of the solutions stores the data locally on devices or things and others may store in cloud. By collecting data through data processing and aggregation where we can extract new knowledge. Such procedures leads to user privacy issues. It discusses some main challenges of privacy in IOT and opportunities for innovation and research.

C. Nita Rotaru [12] proposed RC4: a Robust Security mechanism which is designed for fast online processing. Here the buffer storage will be limited due to which data items will be dropped from systems and will lost. Due to the lossy streaming environment, various security mechanisms have been studied and hence in data stream systems we need to focus data integrity and confidentiality. A new mechanism is proposed called RC4., that provides data integrity and confidentiality.

W.Lindner [17] proposed Securing the borealis data stream engine. As data stream management system is more popular and there is need to protect systems from threats. This securing technique propose a general security framework and access control model for security of DSMs. By access controls, the Denial of Service attacks can be avoided.

SEDAN proposed in [18] is a hop by hop routing protocol which is implemented, where data is encrypted to provide integrity and data security for public networks. It reduces the processing delay for packets with the help of encryption and decryption protocols of the packet.

Blaze and Feigenbaum proposed [19] a decentralized trust management where trust management is important component of security. The trust management problems consists security credentials and security policies. It determines whether the set of credentials can trust to third parties and also whether it satisfies the policies of security. The trust management gives a new approach called Policy Maker, through which we can develop security features in network services.

Chris Clearfield [21] studies on "Rethinking Security for IOT", where it need to provide solutions for cyber attacks. Cyber Attacks used for stealing confidential information. For Example, in white house, the U.S stock market; news have been revealed and also hackers built a device which can open electronic locks without a key.

The survey presented in this paper includes techniques, applications, functionalities, challenges, concepts, methods, objectives of IOT. This paper also discuss the issues on security where number of devices/objects connected using internet.

I. FUNDAMENTALS OF IOT

A. RFID(Radio Frequency Identification)

The internet of things requires a few components which enable communications between devices and objects. Objects need to be build up with an auto-id technology i.e., RFID tag. So that objects can be uniquely identified. It is also used for designing microchips for wireless data communication.

B. Sensor network

Here the smart objects will be embedded with a sensor to measure data. Sensor captures fluctuations in surrounding temperature, changes in quantity or other types of information. With these sensor we can see the exact location of the objects. It improves efficiency, reduces wastes and low costs, consumes low power devices in remote sensing applications.

C. Data Storage

IOT deals with storing and sharing huge amount of data, where the data must be used carefully for actuation and monitoring purposes.

D. Visualization:

It represents the abstract business or scientific data as images that can aid in understanding the meaning of data where it establish an interaction of user with environment.

II. RESEARCH CHALLENGES

IOT has been playing an important role in organization from many years but due to negligence in development, some industry people started calling it as "Internet of No Things". By

this it is claimed to know that development of IOT is in trouble. There are some problems in IOT, they can be solved by giving more capitalization, more consumer interests and more attention.

On the other hand, the problems of IOT extends to security level, where it becomes the biggest concern. The starting few weeks of 2015 gives most negative results related to security. Many industry watchers gave 2015 as "the year of IOT", for its pessimistic performance.

One of the security firm Kaspersky gave a comment on IOT security challenges, with an unfavourable line i.e.," Internet of Crappy Things". Not only home electronic things are connected but also flood appliances, weather forecasting, etc are connected. So, the major concern is hacking issues on these things.

For Example, hacking of a car wash. Now-a-days car washes have smart control systems connected, if it is hacked, hacker can obtain control on all the options of car wash due to which there is also a possibility of damaging a car.

Another example is hack of police surveillance system which is reported by a security expert at Kaspersky Lab.[20]. A paper called "Researching for the Silver Bullet" is published by Wind River on IOT security. In this paper we give an outline of problems associated with IOT. Some of them are, Security must be an organizer for IOT. There are no concurrences on implementation of security in IOT devices. To reduce the threats there no silver bullets present.

But somehow we can use firewalls and protocol to keep IOT devices secure and we need to adapt unique constraints of IOT devices.

Edith Ramirez, U.S. Federal Trade Communication Chairman, prompts that embedded sensors are going to be hacked, a massive security risks are raised. Edith summarizes some key challenges for future of IOT. Such are Pervasive data collection, possibility for unexpected users of consumer data, Intensive Security risks.

III. SECURITY ISSUES

A. Access Control

The main functionality of access control is to give access rights to the things/devices in IOT environment. In database management systems, processing of data is done, where in IOT the process of flowing of data is done. Two words are described for access control.[7].

1. Data Holders

Data Holders are 'users' who can send and receive the data to objects. The data should be sent only to authenticated objects.

2. Data Collectors

Here users should have authenticated identity for systems to provide location in emergency situation.

The essential enablers for access controls are Identity Management, and authentication and to control access you must be able to identify your devices and users. In IOT context access control must make sure only trusted parties can access sensor data, and can update device software. So, the issues of data ownership can be solved by access control.

IOT consists set of access control challenges due to low bandwidth between IOT devices, low power requirements in IOT devices, ad-hoc networks.

B. Authentication and Confidentiality

There are many mechanisms established to deal with authentication and confidentiality in IOT. Some of the related works of authentication and confidentiality are[10] presents a distributed key management and authentication approach which is recently developed the concepts of identity based cryptography and threshold secret sharing. The identity based cryptography is applied to provide end to end authenticity and confidentiality and also to save bandwidth and computation power of wireless nodes.[11] Public key infrastructure is also built for IOT. Business security IOT protocol which combines platform communication with authentication, signature and encryption.

Ensuring data confidentiality is a basic constraint for many applications. For example, bio-sensors provides data on bacterial composition of product used in food industry. This data is confidential if not it will harm the company fame and reputation. In IOT environment an approach called "Role Based Access Control"(RBAC) is used. Here RBAC gives successful alternatives, and mandatory access controls.

Mainly users and permissions are assigned for roles. Benefit of RBAC, is the modification of access right can be done by changing role assignments. Access controls are embedded with data stream management systems where this data stream management systems are used for real time applications.

For example, RC4 encryption algorithm is used to solve decryption failures occurred because of synchronization problem.[12]. This algorithm is proposed in Nile Stream Engine.[13].Data streaming access control is used to investigate the streaming data for unauthorized access, in IOT. In RBAC, it introduces a query rewriting mechanisms, where the user queries are rewritten where the data tuples are not returned and will not be accessed to access control policies.

This mechanism consists of a module which translates the rewritten query in a way that can be executed by heterogeneous stream engine solutions. Hence the development of solutions for IOT applications needs to be concentrated. Still need to work on protocols for authentication and confidentiality in IOT context.

C. Privacy

Privacy of things/objects one of the key challenges in IOT, in order to drive the success of IOT. The invisible, ubiquitous collection and spreading of data of people's private life gives rise to privacy burdens. Such that ignoring these issues can effect on failure of services, disturbance to reputation.

In RFID technology of IOT context, privacy issues are raised at RFID tags. On researching, we found threats identification and tracking of people through hidden tags of RFID[8]. Various techniques are proposed such as tag encryption, tag identifier, blocking of tags, etc. Hence RFID tag issue became a major challenge in IOT.[9]. For managing privacy in IOT, a data tagging is proposed. Also a user controls privacy preserved access control protocol, based on k-anonymity privacy mode which is proposed in [14]. Some more work has to be done on privacy preserving mechanisms in IOT.

D. Trust and Data Integrity

Systems will integrate data from connected sensors in IOT.[2]. But how sure in an organization that consists the data which is not interfered with others? An example of shopping mall such as wall mart keeping records of customer by using smart meters. Researchers have extracted that smart meters can be hacked. They were able to spoof messages which are sent from the meter to shopping malls and sends false data.

Here antivirus protection can be downloaded only in PC's, Laptops. But in IOT, security does not exist in many devices. Such that security should be built in devices and system should create trust in both integrity of data and hardware.

E. Mobile Security

Mobile nodes in IOT move from one cluster to another cluster, where cryptography protocols are used for authentication, identification and privacy protection.

IV. CONCLUSION

In this paper we discussed about the security issues in IOT in which it depicts on data confidentiality, privacy and trust. Internet of Things is so close to implement that a person could think. Most of the organizations needs IOT have already with them and some technologies have been implementing the versions of it.

The reason why IOT has not implemented correctly is due to the impact on Trust, Data Integrity and Security fields. Hackers could probably access it and the workers could probably abuse it. Mostly organizations don't want to share the data and people don't like the absence of privacy. The technologies of IOT such as Sensors and RFID makes our life easier and comfortable.

REFERENCES

[1] "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.
[2] "Internet of Things", ITU retrieved 26 June 2015. <http://www.itu.int/internet of things/>.
[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol.29, no.7, pp. 1645–1660, 2013.
[4] Glenn Surman: Understanding Security Using the OSI Model. SANS Institute InfoSec Reading Room, 2002.
[5] By INFSO D.4 NETWORKED ENTERPRISES and RFID INFSO G.2 MICRO AND NANOSYSTEMS.
[6] John Domingue, Dieter Fensel, Paolo traverso "Future Internet-FIS:First future internet symposium,2008.
[7] A. Alcaide, E. Palomar, J. Montero-Castillo and A. Ribagorda, "Anonymous authentication for privacy preserving IOT target driven applications", Compute. Secure. 37, 111–123, 2013.
[8] D. Evans and D. Eyers, "Efficient data tagging for managing privacy in the internet of things", in: Proceedings – 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCom 2012, Besancon, France, 2012, pp. 244–248.
[9] X. Huang, R. Fu, B. Chen, T. Zhang and A. Roscoe, "User interactive internet of things privacy preserved access control", in: 7th International Conference for Internet Technology and Secured Transactions, ICITST 2012, London, United Kingdom, 2012, pp.597–602.
[10] Lan. Li Study on security architecture in the Internet of Things." In Measurement, Information and Control (MIC).
[11] E.Mykletun, J.Girao, D.Westhoff, Public Key based cryoto schemes for data concealment in wireless sensor networks, in: Proceedings of IEEE ICC, Istanbul, Turkey,2006,pp,41-47.
[12] M.Ali, M.Eltabakh,Nita Rotaru FT-RC4: A Robust Security Mechanism for Data Stream Systems, Purdue University, Technical Report, TR-05-024.
[13] M.Hammad, M.Franklin, W.Aref, A.Elmagarmid, Scheduling the shared window joins over data streams, in Proceedings of the 29th international conference on Very Large Database(VLDB'03), Morgan Kaufman Publishers Inc., Berlin,Germany,2003,pp,297-308.
[14] Juels A.RFID Security and Privacy: a research survey. Selected areas in communication, IEEE Journal on 2006.
[15] "IOT Startup EVRYTHNG Secures $7m Series A From Atomico, BHLP, Cisco And Dawn".Techcrunch.
[16] Perera, Charith; Ranjan, Rajiv; Wang, Lizhe; Khan, Samee; Zomaya, Albert (2015)."Privacy of Big Data in Internet of Things Era". IEEE Professional Magazine. Retrieved 1 February 2015.
[17] W.Lindner, J.Meier, Securing the borealis data stream engine, in: Proceedings of the International Database Engineering and Application Symposium(IDEAS'06), Delhi, India, 2006, pp,137-147.
[18] M.Bagaa, N.Lasla, A.Ouadjaout, Y.Challal, SEDAN: secure and efficient protocol for data aggregation in wireless sensor networks ,in: Proceedings of IEEE LCN, Dublin, Ireland, 2007,pp,1053-1060.
[19] M.Blaze, J.Felgenbaum, J.Lacy, Decentralized trust management, in: Proceedings of IEEE international Symposium Security and Privacy, Colorado Springs, 1996,pp, 164-173.
[20] Eugena Kaspersky, waging war against malware, retrieved in may 2011. <eugena.kaspersky.com>.
[21] Christopher Clearfield "Rethinking Security for Security for the Internet of Things" Harvard Business Review Blog, 26 June 2013.