Volume: 7 Issue: VII Month of publication: July 2019

DOI: http://doi.org/10.22214/ijraset.2019.7220

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Data Security in Internet of Things: A Review

Sangeeta Pradhan[1], Shajid Ansari[2], Somesh Deewangan[3]
[1, 2, 3] *Department of Computer Science & Engg, R.S.R. Rungta College of Engineering and Technology, Bhilai (C.G.), India*

Abstract: In recent years, Internet of Things (IoT) has become an interesting research topic in various fields such as technical, academic, medical and industry. With the growing interest in IoT, security must be taken into consideration as it is one of the main issues of IoT platform, technologies and application. The most important part of secure IoT system is verification and authentication between IoT enabled devices and IoT web servers. This paper presents reviews the research on IoT architecture, various securities issues and challenges that must be taken into consideration and also presents a multi-factor authentication for a new solution to ensure confidentiality, integrity, authentication, authorization and ability to identify heterogeneous devices.

Keywords: Internet of things, data security, threats, authentication, IoT architecture.

I. INTRODUCTION

In our day to day life Internet of Things is emerging as a technological breakthrough revolution where billions of heterogeneous devices and homogenous devices that are provided with unique identifiers (UIDs) are embedded with electronics, Internet connectivity and sensors which are connected to internet and can communicate and interact with each other without any human interference.

They can be remotely monitored and controlled [1]. IoT has the prospective to evolve new market opportunities and business model. Meanwhile security, privacy issues should be addressed.

Internet connected devices give lots of opportunities to cyber criminals to do modification in the IoT system on a big scale. This results in creating a lot of risks, issues and challenges in data security. Data privacy, authentication, human factor, data encryption and complex system are the five key security risks and IoT issues [2].

Security attack on IoT devices occurs on the following layers of IoT and they are object layer, transport layer, processing layer and cloud layer [3]. In this paper a study is performed on IoT features and key technologies, security issues and challenges.

II. IOT FEATURES AND KEY TECHNOLOGIES

A. IoT Architecture

IoT architecture is vast and broad concept so far as no uniform IoT architecture has been proposed in the past years. IoT consists of sensors, actuators, networks to make it work and communicate between the computer systems and technologies. The various layered IoT architecture available are three layer, four layer and five layer architecture. Since in this paper we are focusing on the data security issues we will discuss about the five layered IoT architecture model [3].

1) *Object Layer:* The bottom layer is the Object layer. This layer is also known as perception layer or hardware layer. This is the base of IoT architecture that contains sensor, actuators, RFID tags, barcode, etc. The data is collected from sensors and transmitted to the network layer.
2) *Object Abstraction Layer:* This layer is responsible for transmission of data from an object to the service management layer via channel without any intervention. This layer is also known as network or gateway layer which contains physical components and communication software which helps in transmission of information captured from sensor.
3) *Service Management Layer:* This is the middle layer of IoT architecture and hence known as middleware layer. It is a service oriented layer that assures similar type of services between the connected devices on the basis of addresses and paired device name. The main feature of this layer is business and process rule engine. In this layer the received data is processed and control security, make decision and then delivers the requested data.
4) *Application Layer:* This layer provides the services requested by the customer. The IoT application covers smart home, automation, smart hospital, smart city etc.
5) *Business Layer:* The business layer is responsible for making a graph, flowchart and business model. In order to enhance the user's privacy in IoT, business layer compares the output of every layer. It supports designing, analysis, implementation of IoT system related element. [10]

B. IoT Characteristics Based on Security Requirements

The fundamental characteristics of IoT based on security requirements are as follows [4, 5]:

1) *Interconnectivity:* Interconnectivity brings day to day things together to empower IoT as anything can be connected with each other. It enables network accessibility and compatibility in the things.
2) *Resource Constraints:* IoT has caliber to provide things related services within the constraints of things such as privacy protection and semantic consistency between physical things and their associated virtual things. There are major concerns regarding the resource-constrained environments in IoT, including data encryption, privacy-preservation, vulnerabilities, threats, attacks, controls, etc. To address these privacy and security challenges, appropriate technologies have to be developed for resource-constrained environments in IoT.
3) *Heterogeneity:* IoT devices are heterogeneous as they are from distinct hardware platform and network and are able to interact with other devices, platform through various networks. In IoT the key design requirements of heterogeneous things and their environment are interoperability, extensibility, modularity and scalability.
4) *Dynamic Environment:* Gathering data from its environment is the main activity of IoT. This can be obtained by dynamic changes that take place around the devices.

C. IoT Elements

The key elements of IoT are

1) Identification: It plays an important role in identifying each object within a network. The two methods for identification include Naming and Addressing. Naming indicates the object name and addressing indicates object's unique address. Examples of identification method used for IoT are Electronic Product Codes (EPC) and Ubiquitous code [7].
2) *Sensing:* It is a process of collecting information from devices and storing it in database, data warehouse or data center. The examples for sensing devices are sensor, RFID tags etc [7].
3) *IoT Network:* In recent years, IoT becomes a most significant trend where millions of devices are connected and controlled by internet. IoT network is used to communicate between IoT devices [8].
4) *Platform:* An IoT platform is a multilayer technology placed between IoT object layer and IoT gateway layers. This element is also known as computation as it enables object and endpoint management, connectivity, network management, processing and analysis, application development, security, etc [6]. The examples of IoT platform are Thingsworx, AWS, and Microsoft Azure etc.
5) *Services:* In IoT, services are divided into four classes; they are identity-related services, information aggregation services, collaborative aware services and ubiquitous services. Identity-related services identify the object first requested for the services. Information aggregation services first gather all the raw information and then summarize that information for processing and reporting. The data generated from previous class is used for decision making by the collaborative aware services. On customer's demand ubiquitous services delivers the information obtained from collaborative aware services at anytime and anywhere.
6) *Cloud:* In real time for collecting, processing, managing and storing large volume of data from heterogeneous and homogeneous devices, users and applications IoT cloud provides tools that need to be managed in an efficient way. IoT cloud provides accurate data analysis and processes data at high speed. One of the most important components of IoT cloud is distributed management system [8].
7) *Semantic:* The process of extracting knowledge to offer the required services is known as semantic. It is the most important element of IoT which acts like brain of IoT to accomplish all the responsibilities. Some of commonly known semantic technologies are resource description framework, web ontology language, efficient XML interchange [7, 8].

D. IoT Security Standards

The IoT security standards are as follows [9]:

1) *Authentication:* It is the process of verifying the identity of a user or device. Impersonation attack and Sybil attack are the two types of attack related to authentication. Impersonation attack fantasized to be another element. Sybil attack is the type of attack where at a time distinguish identity is used by attacker to attack.
2) *Authorization:* it is the act of granting access to network resource which allows the user to access various resources based on user identity.

3) *Confidentiality:* It means protecting information from being accessed by unauthorized parties. It ensures that the data is only readable by the proposed destination.
4) *Integrity:* It ensures that the information contained in the original message is kept intact. Message alteration attack and message fabrication attack are kinds of attack related to data integrity. Access control method is implemented to protect data integrity.
5) *Availability:* availability means only the authorized user can access the information. The main aim of availability is to protect network services existence against denial of service attack.
6) *Privacy:* It ensures that only the desired sensor devices and gateways are part of the network and hence it prevents devices from malicious attack.
7) *Non-Repudiation:* Non-repudiation gives the assurance that someone cannot deny the validity of something. It provides guaranteed message transmission between two devices through digital signature and encryption method. The attacks are Phishing or man-in-the-middle (MITM) attacks that can compromise data integrity.

III. LITERATURE REVIEW

Trusit et al. [11] proposed a method of secret vault(a set of keys) which shares secret between IoT server and IoT devices. In this paper after successful completion of each session, content of secure vaults changes. For implementation they have used Aurdino device & HMAC algorithm. They used three way mutual authentication mechanisms for authenticating and communicating between IoT devices and IoT server. They proved the feasibility of algorithm on IoT devices with memory and computational power constraints.

Se-Ra Oh et al. [12] developed an OAuth 2.0 framework based on oneM2M security component to provide authentication and authorization between IoT device platforms and IoT service platform. In OAuth2.0 framework to use the resource the client need to receive an authorization grant from resource owner and to access the token it need authorization grant from Authorization server.OneM2M security component performs token-based authentication, it is lightweight and scalable and implemented by using Node.js-based 'oauth2-server' module i.e. OAuth 2.0 server library. In oneM2M security component, resource request from unauthorized user will be blocked and meanwhile for the authorized user the request will be passed. In this the goal of data security is not achieved.

Shantanu et al. [13] presents the classification of IoT security and threats into five distinct categories such as communications, device/services, users, mobility and integration of resources. Sample mechanism for authorization and security is designed in IoT architecture by proposing Attribute Based Access Control (ABAC), Role Based Access Control (RBAC) and capabilities as they employ an access control design. Capabilities structure is used which includes time-stamp, identification of things, operation and condition fields. Capability may grant access to more than one thing and operation on a thing. It is a scalable and flexible method but yet a complex method. Trust and identity management need to be developed.

Swapnil Naik and Vikas Maral in their paper [14] discussed about various security attacks and mainly focused on device cloning and sensitive data exposure to secure the IoT solutions. The solution is efficient and secure with a little cost overheads.

Sheetal Kalra and Sandeep Sood presents a paper [15] proposed a secure communication between the embedded devices and cloud server. A secure ECC based mutual authentication protocol and Hypertext transfer protocol is used. An automated verification of protocol is performed using AVISPA tool which confirms protocol's security in presence of intruder. It is robust against various security attacks with low computational cost but it can be more reliable.

Anusha Medavaka in her paper [16] proposed a concept of protected vault which is a common key in between IoT devices and IoT server. A 3 way mutual authentication takes place between IoT server and devices within IoT session. After the successful completion of session the collection of password is changed hence protects from side channel attacks. Algorithm like AES, HMAC are compared and implemented on Aurdino device to compute the performance analysis and security analysis for power constraints. Hence it is a safe verification mechanism for authentication and communication between IoT devices and IoT server.

Luciano et al. [17] presents an authentication model and several use cases for IoT clouds which allows user and manufacturers to access IoT devices in a secure. Several use cases is based on Identity Provider/Service Provider (IdP/SP) model.

Santoso et al. [18] proposed a methodology to assure a very high security for IoT based smart home system. For authentication process, the system use Elliptic Curve Cryptography (ECC) and AllJoyn framework. The system runs with the help of wifi network. By android application based mobile device user can control the access of system for initial system configuration authentication of IoT devices. A wifi gateway node is used. Authentication process contains two steps, one is authentication between mobile device to IoT device and other is gateway to IoT device and after this process encrypted communication takes place.

TABLE I. Comparisons of various techniques and method used in existing system

S.No.	Title	Year	Method Used	Approach	Strength	Limitation
1	Authentication of IoT Device and IoT Server Using Secure Vaults	2018	HMAC, a key based hashing algorithm. Aurdino device.	Proposed a method of secret vault (a set of keys) which shares secret between IoT server and IoT devices and after successful completion of each session, content of secure vaults changes. A 3-Way authentication message exchange mechanism between IoT server and IoT device is used.	The feasibility of algorithm on IoT devices with memory and computational power constraints. Secure against side channel attacks used to breach the security of the IoT devices.	Other security standards like authorization, confidentiality, and integrity can be included.
2	Development of IoT Security Component for Interoperability	2017	OAuth 2.0 framework based oneM2M security component	Developed an OAuth 2.0 framework based on oneM2M security component to provide authentication and authorization between IoT device platforms and IoT service platform.	In oneM2M security component, resource request from unauthorized user will be blocked and meanwhile for the authorized user the request will be passed.	Need to focus on achieving security goals (e.g., non-repudiation).
3	On the Design of Security Mechanisms for the Internet of Things	2017	Attribute Based Access Control(ABAC), Role Based Access Control(ABAC)	Distinguishes IoT threats and attacks into 5 distinct categories i.e. communications, device/services, users, mobility and integration of resources. A sample mechanism for smart thing authorization is designed and provides basic security mechanism access control.	Policy management is reduced with the combination of ABAC and RBAC. Access control security mechanism is scalable and flexible.	Need a wide range of mechanisms and services and also trust and identity management in the IOT architecture.
4	Cyber Security - IoT	2017	Encryption Algorithm, MQTT. Use of html and JavaScript for web console and remaining Api calls are implemented in python flask	Provides information about various security attacks. Proposed a method to secure the IoT solution from device cloning and exposing the sensitive data.	Authentication, encryption and clone detection is done in few seconds. As it is very secure provides efficient solutions.	Security mechanism is accomplished but the cost is little more which need to be reduced.
5	Secure Authentication Scheme for IoT and Cloud Servers	2015	ECC based mutual authentication Hypertext transfer protocol.AVISPA tool is used for automated verification of protocol	Proposed a secure ECC based mutual authentication between embedded HTTP client devices and Cloud servers to provide secure communication.A formal verification of protocol is performed by AVISPA tool, which confirms protocl security in presence of intruder.	Protocol security is robust against various security attacks with low computational cost.	It can be more reliable.
6	Algorithm Feasibility on IoT Devices with Memory and Computational Power Constraints	2019	Verification between devices and server id done using multiple key passwords.	Proposed protected vault which is a common key between IoT devices and Server. IoT session is used to change the password between the devices after successful completion of each session. Performance analysis and security analysis is done by comparing cryptographic algorithm which is implemented on Aurdino device.	Protected against side channel attack.	Collection of password is changed after every successful attempt this makes the process time taking and unreliable.
7	An Authentication Model for IoT Clouds	2015	cloud computing and IoT devices are combined to provide better services. Work on several use cases with Identity/Service Provider(IdP/SP).	Presents an authentication model for IoT clouds which allows user and manufacturers to access IoT devices in a secure way. Several use cases is based on IdP/SP.TPM is developed.	An efficient model to provide security in IoT based cloud computing. Safe and secure authentication is done between users/manufacturers with IoT cloud provider and IoT devices.	The implementation part must needed to complete
8	Securing IoT for Smart Home System	2015	AllJoyn framework, Elliptic curve cryptography(ECC) for authentication process	proposed system uses a gateway to give an efficient authentication process and also an interace for the user via Android device	for authentication, this process can be once performed for each device	More improvement is needed to perform the procedure as the current method of entering Device ID, authentication procedure is inconvenient for the user.

IV. DATA SECURITY ISSUES AND CHALLENGES IN IOT:

A. Nowadays maximum devices are IoT enabled devices which results in huge challenges in organizing and managing a single device.

B. Data protection: In Internet of Things environment, there is need to protect the personal data for retrieval of data and processing a large volumes of data.

C. Data authentication: In IoT environment, the authentication of data is required for source data.

D. Data usage: for the data usage it is mandatory to address the data through the security channel attack.

E. Performance: The performance of Internet of things environment need to be enhanced by increasing latency and capacity.

V. CONCLUSIONS

The topic "Internet of Things" is becoming one of the demanding and hot topics for the research work in every field. As millions of devices are connected to internet and communicating with each other, communication channel need to be secure. Security in IoT is also very important in making IoT successful. User focus on using IoT because of faster and automatic services but ignore security aspects of IoT devices, IoT server and communication channel. In this paper, we have presented five layered architecture of IoT, characteristics of IoT based on security requirements, IoT elements and IoT security standards. This paper also presented a review of previous paper based on the authentication of IoT devices and IoT server. Also focus on the data security issues and challenges.

REFERENCES

[1] https://en.wikipedia.org/wiki/Internet_of_things

[2] https://apiumhub.com/tech-blog-barcelona/iot-security-issues/

[3] Keyur K Patel, Sunil M Patel," Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", 2016 IJESC, pp. 6122-6131.

[4] https://www.linkedin.com/pulse/internet-things-iot-characteristics-kavyashree-g-c

[5] https://designmind.frogdesign.com/2014/08/internet-things-six-key-characteristics/

[6] https://www.i-scoop.eu/internet-of-things-guide/iot-platform-market-2017-2025/

[7] Burhan, M., Rehman, R.,Khan, B., Kim, B.-S. (2018)." IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey".

[8] https://spgcontrols.com/elements-of-iot/

[9] Otmane El Mouaatamid, Mohammed Lahmer, Mostafa Belkasmi," Internet of Things Security: Layered classification of attacks and possible Countermeasures",2016, http://www.revue-eti.net

[10] Muhammad Bilal, "A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers", https://arxiv.org/ftp/arxiv/papers/1708/1708.04560.pdf

[11] Trusit Shah, S. Venkatesan. "Authentication of IoT Device and IoT Server Using Secure Vaults", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, pp. 819-824, IEEE

[12] Se-Ra Oh, Young-Gab Kim, "Development of IoT security component for interoperability", 2017 13th International Computer Engineering Conference (ICENCO), pp. 41-44,IEEE.

[13] Shantanu Pal,Michael Hitchens, Vijay Varadharajan, "On the Design of Security Mechanisms for the Internet of Things", 2017 Eleventh International Conference on Sensing Technology (ICST).

[14] Swapnil Naik, Vikas Maral, "Cyber Security – IoT", 2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT),(pp 764-767) IEEE

[15] Sheetal Kalra, Sandeep Sood, "Secure authentication scheme for IoT and cloud servers", 2015, Pervasive and Mobile Computing, 24, pp. 210–223.

[16] Anusha Medavaka, "Algorithm Feasibility on IoT Devices with Memory and Computational Power Constraints", International Journal of Science and Research (IJSR), Volume 8 Issue 5, May 2019, (pp 1815-1820).

[17] Luciano Barreto, Antonio Celestiy, Massimo Villariy, Maria Fazioy, Antonio Puliafito, "An Authentication Model for IoT Clouds", 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 1032-1035

[18] Santoso, F. K., & Vun, N. C. H., "Securing IoT for smart home system", 2015 International Symposium on Consumer Electronics (ISCE).