Current Security Challenges in Internet of Things

Shital Pawar[1], Dr. Suhas Patil[2]
[1]*Ph. D. Research Scholar,* [2]*Professor*
Department of Computer Engineering, Bharati Vidyapeeth Deemed University College of Engineering, Pune. India

Abstract - Every day in Internet of Things large numbers of objects are to be transformed into smarter objects. In order to achieve a specific goal, these smarter objects communicate with each other and with an environment too. In consequence a global infrastructure network has been constructed that contribute and supports innovative and customized services to an individual and various businesses in heterogeneous application domains. As a result of which a system may composed of extremely large number of discrete devices that increases range of challenges such as integration, scalability etc. By considering such circumstances the critical issues which are widely acknowledged are security and privacy.

Keywords - IoT devices; Quality of service; Communication protocols; Privacy; IoT security.

I. INTRODUCTION

IoT has been evolved from the development of new relatively cheaper, flexible and smaller, wireless devices as well as variety of protocols which are used for communication .Till the upcoming year 2020, according to the recent prediction the quantity of devices in Internet of Things will rises to a great extent and we will have around 26 to 50 billion of devices connected using IoT. The rapid development observed in the field of IoT has resulted into providing the range of services which delivers information from different sources like actuators, surveillance cameras, monitoring sensors, home applications etc. As a result , a large number of heterogeneous applications has been developed in various domains such as traffic management, industrial automation, monitoring sensors, medical aids, home automation and many more[15][16]. The possibility of getting best service is the principal requirement in IoT irrespective of the dependency on non-functional requirements such as Quality of Service considered at runtime using design time service transformation or at only runtime only if the presently running service begins to degrade. In order to provide services for safe critical services like which are used generally in health care where a failure of such service can result into serious prime impact.

II. IOT SECURITY

Internet of things comprises of various objects, sensors, and smart nodes having an ability of communication among them without any human intervention. These objects when connected with other objects/things can function independently. The functionality of authorizing and obtaining different cloud recourses, analyzing and data extracting, delivering lightweight data, collecting data for making decisions [1] is provided by IoT nodes. one has to deal with challenging tasks at the time of IoT applications development due to specific reasons such as (i) Diversity of communication protocols ii) major difficulty in distributed computing iii) multiple number of languages for programming iv) limited frameworks and common guidelines available to manage communication of low level and simply implementation at high level [2].

As IoT devices and applications are connected to each other over an Internet so the risk of cyber-attacks increases which causes serious threat to privacy and security of data. In order to respond to any request raised middleware security is important for protocol communication in IoT. Due to increasing number of attacks, information leaks, vulnerabilities various researchers, cloud providers, and device manufactures are working to design a system for security. Purpose of designing such system is to identify new vulnerabilities, control information flow between different devices, to provide privacy and security to users and devices. Researchers are dealing with IoT privacy and security challenges, most of the studies are in their development stages so due to lack of applicability most of problems are remain unsolved [3]. Specifically in case of protocol communication scheduling of resources becomes very difficult. In case of lot of types of underlying protocols available, underutilization of resources becomes a major problem [4].

III. IOT SECURITY CHALLENGES

A. IoT Devices:

i). Currently available mechanisms are giving content/context oriented privacy and user oriented privacy. But networks of an IoT generally consist of autonomous nodes which collect information and needs privacy models which are object oriented. Furthermore Large number of privacy guidelines mandate informing users about how their private data is administered and managed. a big challenge in wide range of IoT networks is recognizing the nodes which may have an access to passively accumulated users private information[1].

Developing an architecture which deals with different challenges in IoT environment security is very essential. An IoT architecture not only address security problems which are previously covered but can handle challenges which are found by deploying devices of an IoT over SDN (Software Defined Networks)[1]

ii). An application of Internet of Things can be constructed from large number of wide range of services offered by number of devices that are possibly mobile

and/or resource constrained. While these allocations and services are continued to be worldwide so one of the important research question is how to estimate Quality of Service (QoS) at user side to guarantee an adaption, composition and optimal selection of various IoT services [5]. Author suggested one prediction approach which is based on a novel neighborhood prediction i.e. IoT Predict. This approach uses an equivalence computation mechanism. This collaborative approach needs no any supplementary acknowledgement of services, in an IoT that is necessary requirement for resource constrained devices. Author assessed an algorithm on Quality of Service dataset and revealed that finds higher prediction accuracy of QoS than other approaches based on state of art. So major challenges in an IoT is the devices are generally resource constrained.

iii). The model switch to an Internet of Things and publishing the edge computing idea have brought a great potentials for different IoT applications in future like smart transportation, smart home, smart grid, smart health and smart energy. It brought a stream of recent challenges of cyber security. We visualize that a great number of innovation and research opportunities will appear in combination of Cyber security + Internet of Things + edge computing + Artificial Intelligence [14].

IoT devices can also assist each other with various tasks relay on availability of their resources and an incentive strategy. Such a taks collaboration and unloading brings an additional security issues. One os the security issue is about software security. The codes of tasks are required to be built and written in such a way that they can be scheduled dynamically to execute on various systems such as the IoT devices and edge computing. However mostly IoT devices are resource constrained so it is necessary to discover some effective light weighted methods for access control, encryption and authentication.

iv). Researchers have focused on privacy and security requirements associated with flow of information in Medical Internet of Things (MIoT). In addition researchers have done deep study of available solutions to privacy and security issues, along with research issues and available challenges for future work. The volume of information managed by MIoT devices increases exponentially that means greater disclosure of sensitive and private data. The privacy and security of information gathered from various MIoT devices either at the time of transmission to the cloud or during information stored in cloud are significant unsolved issues. It means that the information must be transferred and stored securely. In order to assure its validity, integrity and authenticity and privacy of sensitive information, information must only be accessed by authorized person [16].

B. Communication protocols:

i). As IoT based services expands and method of connectivity progresses, a large number of objects and devices will become a part of IoT. An outcome of which huge amount of data will be produced so management of this data is becoming a huge challenge. In order to develop more applicable and realistic services, an effective resource management is necessary requirement the layer of data perception. 'Cloud of Things' (CoT) gives simplicity of management for the increasing contents of media and other data too. Except this, different features such as resource provisioning, service discovery, ubiquitous access, and service creation plays a crucial role which originates from Cloud of Things (CoT).

The reason behind this is to organize resources, implement data filtration, pre-processing and take necessary security actions. Further research can be done in middleware protocol management where variety of communication protocols can be taken under consideration such as XMPP, MQTT, CoAP etc. [4]

ii). Today's one of the major technical challenge is putting up a security into new computing standard. Although, what are the current security issues in IoT which we can deal with using available security principles? Which are new challenges and security issues in this space that needs novel security mechanisms? [12].

Diversity of communication protocols disturbs the network scanning operation which is a basic security practice. Therefore multiprotocol support system required to be developed.

iii). Researchers have examined IoT security for trustworthy internet services. Researchers have analyzed various security mechanisms like cryptography, Distributed Denial of Service (DDoS) attacks which targets IoT networks and features of various IoT circumstances. Aim of Denial of service (DoS) and Distributed Denial of Service (DDoS) attacks is to harm the resources and cause delays, interruptions, losses and reduces the performance of IoT services. So these attacks are nothing but threats in IoT. Such attacks must be detected and prevented independently for extremely available and reliable services in IoT [11].

C. Quality of service (QoS):

i). For tremendous IoT data acquisition, a 'gateway based data aggregation' approach is most regularly used for featuring actuator/sensor continuous access and supplying buffering / caching and pre-processing functionalities.

An author recommended a 'PSIoT-Orch' framework that is aware about Pub/Sub (Publish/Subscribe) Quality of Service (QoS). This framework directs IoT traffic and allots resources of network between consumers and aggregates for enormous traffic in IoT. 'PSIoT-Orch' framework plans data flows in IoT on the basis of their QoS requirements. Future development is required to minimize data transmission delay (e.g. Sensor data /commercial data need to be handled.)[6].

ii). Shifting to service with superior Quality of Service is not a easy task because when Quality of Service is taken into consideration several number of various factors essentially throughput and response time may be get affected by preference of user. There are some Quality of Service factors that are hard to quantify like functional stability and security of service. In IoT it is impracticable

to invoke all existing services for their evaluation due to rapid growth of these services. To estimate available state of art relevant to this research problem researcher conducted quantitative assessment approaches for Quality of Service prediction. Especially those which uses 'Matrix Factorization' (MF) for collective Quality of Service prediction. Researcher had conducted extensive experiments on the basis of large scale real world Quality of Service dataset. In addition to this transformation of this dataset more firmly estimated IoT services, to present the prediction accurateness of such approaches [7].

It is essential to consider number of possible techniques for data pre-processing and organizing similarity differences between the users (e.g. clustering, smoothing of data etc.)

IV. CONCLUSION

Everyday number of devices and objects are connecting to Internet of Things. Resulting system consists of huge number of diverse devices. Confidentiality and integrity of stored and transmitted data must be ensured. One of the critical aspects is users and their sensitive information. In IoT various applications and services uses the data from distinct data sources, so user must be aware about quality extent of data being retrieved and its security to make sophisticated decisions about their utilization. So it very important to assess different security measures of IoT. In this paper we have discussed current security challenges in IoT by considering different aspects like IoT devices, Communication protocols and Quality of Service.

V. REFERENCES

[1]. Conti, Mauro, et al. "Internet of Things security and forensics: Challenges and opportunities." (2018): 544-546.

[2]. Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo. "Internet of Things: A survey on the security of IoT frameworks." *Journal of Information Security and Applications*38 (2018): 8-27.

[3]. Zhou, Wei, et al. "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved." *IEEE Internet of Things Journal* (2018).

[4]. Aazam, Mohammad, et al. "IoT resource estimation challenges and modeling in fog." *Fog Computing in the Internet of Things*.Springer, Cham, 2018.17-31.

[5]. White, Gary, et al. "IoT Predict: collaborative QoS prediction in IoT." *2018 IEEE International Conference on Pervasive Computing and Communications (PerCom)(PerCom 2018), Athens, Greece*. 2018.

[6]. Moraes, Pedro, Rafael Reale, and Joberto Martins. "A Publish/Subscribe QoS-aware Framework for Massive IoT Traffic Orchestration." *arXiv preprint arXiv:1806.03157* (2018).

[7]. White, Gary, et al. "Quantitative evaluation of qos prediction in iot." *Dependable Systems and Networks Workshop (DSN-W), 2017 47th Annual IEEE/IFIP International Conference on*.IEEE, 2017.

[8]. Jalali, Mohammad S., et al. "The Internet of Things (IoT) Promises New Benefits–and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products." (2017).

[9]. Kim, Jun Young, et al. "Automated Analysis of Secure Internet of Things Protocols." *Proceedings of the 33rd Annual Computer Security Applications Conference*.ACM, 2017.

[10]. Esfahani, Alireza, et al. "A lightweight authentication mechanism for M2M communications in industrial IoT environment." *IEEE Internet of Things Journal* (2017).

[11]. Arış, Ahmet, Sema F. Oktuğ, and Thiemo Voigt."Security of Internet of Things for a Reliable Internet of Services." *Autonomous Control for a Reliable Internet of Services*.Springer, Cham, 2018.337-370.

[12]. Fernandes, Earlence, et al. "Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?." *IEEE Security & Privacy* 15.4 (2017): 79-84.

[13]. Xu, Teng, James B. Wendt, and MiodragPotkonjak. "Security of IoT systems: Design challenges and opportunities." *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press, 2014.

[14]. Pan, Jianli, and Zhicheng Yang. "Cybersecurity Challenges and Opportunities in the New Edge Computing+ IoT World." *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. ACM, 2018.

[15]. Aksu, Hidayet, et al. "Advertising in the IoT Era: Vision and Challenges." *IEEE Communications Magazine* (2018).

[16]. Sun, Wencheng, et al. "Security and privacy in the medical Internet of Things: A review." *Security and Communication Networks* 2018 (2018).