IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Security and Privacy Issues in Fog driven IoT Environment

Richa Verma[1]*, Shalini Chandra[2]

[1,2]Dept. of Computer Science, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India

Corresponding Author: richaverma042@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i5.367370 | Available online at: www.ijcseonline.org

Accepted: 09/May/2019, Published: 31/May/2019

***Abstract*-** Recently, the idea of Internet of Things is seeking much attention because of its vast potential in the area of wireless transmission. IoT interlinks plentiful of heterogeneous, geographically diversified devices which usually have scarcity of resources, and therefore rely on cloud for the same. Unfortunately, the Cloud enabled IoT suffer from various limitations say, high network latency with the increase in volume of data processed. Due to the above limitation, majority of latency sensitive applications tend to provide poor performance. To alleviate this problem, the concept of Fog Computing came into the picture, in which Fog level is introduced as an intermediary level between Cloud and IoT devices. IoT unlocks handful opportunities for various sophisticated applications such as home applications, wearable devices etc. and also allow sharing of data over internet. This data being shared contains large amount of sensitive information that should not be shared amongst the connected users. In this paper, firstly brief overview about fog computing is provided and subsequently various security issues pertaining to both Fog and IoT environment are defined.

***Keywords*-** Internet of Things (IoT), Fog Computing, Security, Privacy

I. INTRODUCTION

Over recent years, with the progress in development of wireless sensor networks, the innovations can be also be seen in Internet of Things (IoT) with wide variety of application still being created and executed daily [1]. The dependence of human life over machines has accelerated the growth in advancement of various smart devices. IoT provides countless scenarios for building application, which when implemented in daily life results in providing ease in every aspect of day to day activities. Sophisticated applications such as medical treatment, environmental monitoring system, Intelligent Transportation System, Smart Grid etc. are also not untouched by IoT. With the rapid and smart growth in IoT it is also limited by computing resources and low storage. Due to above mentioned limitations IoT deals with its technological issues by taking the advantages of powerful Cloud [2]. Cloud computing due to its low-cost, on-demand storage capacity, unlimited computing resources properties proves to be convenient and cost-effective solution to balance the technological constraints of IoT [3].

Cloud enabled IoT has drawn significant consideration due to its high potential. However, it also faces numerous drawbacks such as high network latency due to massive volume of data and centralized processing. Many time sensitive applications tend to give poor performance due to the latency generated by cloud. To deal with such issue Fog Computing immersed as a capable technique [4]. Fog layer is located between the cloud infrastructure and ground level IoT devices is presented to extend the storage, network services and computational capabilities to the edge of the network. The fog nodes are placed between the traditional centralized cloud at highest level and IoT devices at the lowest level. Hence the services and resources are made available closer to the end devices. And the delay induces because of cloud being at far apart can be reduced. Thus, the Fog-Enabled IoT guarantees low latency and ample amount of resource availability to the time sensitive applications [5]. With the growth in the expansion of IoT, new security issues come into play while the existing becomes more severe. Heterogeneity, increase in number of devices and wireless nature of network proves to be the major reason for such increase in security issues. The amalgamation of Fog and IoT in the heterogeneous networks, not only includes the existing security problems but also opens the door for certain newer set of problems such as heterogeneous network authentication, privacy protection problem, information management problem etc. [6].

The rest of the paper is organized as follows: Section II is about the overview of Fog Computing. Further, Section III describes the security and privacy issues prevalent in Fog Computing. Section IV describes the security and privacy

issues in IoT paradigm. Finally, the paper concludes with Section V.

II. OVERVIEW OF FOG COMPUTING

Fog computing environment is a new paradigm of computing that is considered to be the extension of cloud computing in which the computing capability is extended to the edge of the network. It is highly virtualized platform of resources that provides storage, networking services and computation to the edge of the network. Fog environment can be a said as backbone infrastructure for the IoT environment. It is basically a scenario in which large number of assorted ubiquitous and decentralized devices coordinates and communicate among themselves to perform storage and processing tasks without the interference of the any intermediary. The elementary advantage of fog computing is because of its edge location and thus supports various applications where latency requirement is low. Another important characteristic of fog computing is location awareness; the fog nodes infer its own location but also keeps track of end user devices to support mobility. The location awareness capability can be the ground breaking factor for location-based applications. Additionally, the interactions between fog and fog, fog and cloud become significant since fog can easily get local overview while the global handling can only be attained at a higher layer by cloud. Fig 1 depicts the placement of Fog with in the network. It shows a simple level hierarchy that illustrates the settlement of cloud at the highest level and fog at the middle level and IoT devices being at the lowest level.

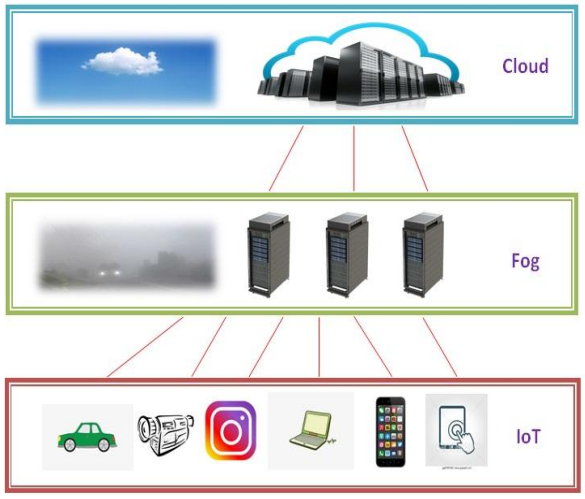

Fig 1: Location of Fog between Cloud and IoT devices

III. SECURITY AND PRIVACY ISSUES IN FOG COMPUTING

Although, the existence of Fog has created a wide difference in a way the IoT devices communicate in the network but with this positive side there also exist some challenges that are to be tackled in order to create a robust environment. Thus, in this section, possible security and privacy problems in fog computing are analyzed.

a) Authentication- Unlike cloud computing deployment where data centers are owned by the service providers, Fog computing deployment can have different service providers due to distinct deployment needs [8]. Considering the above fact there is a need to provide a mechanism to authenticate the fog nodes amongst each other and to IoT and Cloud level as well. Stojmenovic et al. [9] have also considered authentication as one of the major security issues of fog computing. The IoT device being resource constrained generally outsource the computational capacities from potential Fog nodes. This exchange of services also requires authentication mechanism to occur so as to provide a reliable communication path to work upon.

b) Access Control- Access control has been a dependable technique to guarantee the security of the arrangement and preserving the privacy of the user. In cloud computing access control is implemented cryptographically due to its outsourcing feature. Yu. et al. [10] has proposed a well-defined access control scheme for attribute-based encryption (ABE) in cloud. The major challenge that persists in Fog computing is to design an access control scheme in such a way that monitors all the spans between IoT-Fog-Cloud and also manages the resource constraint nature as well.

c) Rogue Node- A rogue fog node is an instance of the fog node that enacts to be genuine but it is actually not. It basically persuades the end user to connect to it and communicate data through it. Such nodes once connected to the network, can easily manipulate the incoming and outgoing requests between the connected entities, tampers the user's data stealthily and can also launch further attacks. The fake fog node that managed to enter the network can prove to a great cause of breach in user's data security and privacy. Han et al. [11] have proposed a measurement-based method which enables a client to avoid linking with the rogue access point (AP). In Fog environment the impact of rough node is doubled as the creation and deletion of virtual files is dynamic hence make it hard to blacklist any node.

d) Location Privacy- In fog computing, the location privacy mostly denotes to the location privacy of the fog nodes. As a fog node generally shed its load to the nearest for node, the node to which the load is shed now has an idea about the location of the fog node that has shed its load. Furthermore, if a fog node uses multiple fog nodes to offload then whole path trajectory of the

network can be revealed. If this process occurs in chain then a rough knowledge about the complete network can be easily traced out. Wei et al. [12] has introduced a trusted third party to generate fake ID for each end user and if any breach occurs the offender can be easily tracked us the given ID's.

e) Intrusion Detection- Intrusion detection techniques are generally deployed in fog system to combat attacks such as flooding attack, insider attack, attack on Virtual Machines, port scanning etc. In fog computing, IDS can be positioned on fog node system side to perceive the intrusive activities by analyzing and monitoring logfile, user login information and access control information. Shi et al [13] have presented a cloudlet mesh-based security framework that can detect the intrusion to the distant cloud safeguarding communication among clouds, mobile devices and cloudlets. In fog computing, it delivers new prospects in investigating a way in which fog computing can help with intrusion detection on both the centralized cloud side and client side.

IV. SECURITY AND PRIVACY ISSUES IN IOT

Although the IoT plays a prime role in delivering a wide collection of services more efficiently and effectively to end user, but it could posses some security and privacy challenges as well. IoT architecture is comprised of three layers; comprehensive perception layer, reliable transmission layer and intelligent processing layer. In this section we summarize the major security and privacy challenges that exist in IoT environment.

a) Security issues in perception layer-

Perception layer or sensor layer attains object related information at any point of time. The sensor nodes are rich in variety and have high heterogeneity. Due to their simple structure and processor they don't have security preserving ability. Some common types of attacks that occur in this environment are as follows [14]: -

- *Fake Node and Malicious Data*: In this the attacker manages to add a node to the system, and injects the malicious code or data. They consume the potential of the nodes and destroys the entire network.
- *Timing Attack*: In this the attacker attacks by analysing the time incurred for executing encryption algorithm, so as to obtain key information from the network.
- *Routing Threats:* In this, the attacker creates a routing loop that resists the flow of data packets in the network. In such attacks the attacker extends or shorten the communication path, and thus increases the end-to-end delay.

b) *Security issues in network layer*- In network layer the reliable transmission is assured that transfers the data in safe and secure manner. This layer basically deals with the data at motion in an insecure environment (wireless and wired both) therefore, security plays major role at this layer [15]. Some of the security issues are as follows: -

- *Compatibility issue*- Heterogeneity makes interoperability, security, and organization of network becoming worse. The existing network security architecture is designed keeping in view the perspective of persons, and does not necessarily applicable for the communication among the machines and hence cause compatibility issue.
- *The Cluster Security Problems:* As IoT has large number of devices. So, any existing authentication, authorization techniques can not be applied to such vast network as it may create a complete blockage in the network.
- *Privacy Disclosure*: With the development of technology and enhanced technical skill of hackers, the hackers now can easily get access to the potential data and can easily collect the sensitive information from it.

c) Security issues at application layer-This layer basically acts as the mediator that analyses the data collected by the sensors and process the data before submitting to the terminal application [16]. The major security concerns possible to occur at this layer are:

- *Data Protection and Recovery*: The data being communicated over the channel contains user private data. The existing data management schemes are not robust and can cause loss to the user's sensitive data. IoT is comprised of vast range of nodes, the mass management of the wide range is also the major reason for such breach.
- *Data Access Permissions, Identity Authentication:* IoT permits a wide collection of nodes to connect to the network. so, in order to avert user intervention an effective authentication mechanism has to be created. Any kind of illegal activity such as spam, malicious information identification must be taken in account while creating such mechanism.
- *Dealing with Mass data:* Due to the deployment of large number nodes and bulk of data being transmitted the security and data loss issues can be very frequent. The mismatch between the processing ability and adapting ability can lead to network interruption and loss of user's data.

V. CONCLUSION

In this paper, it is found that sensor, a fog node and cloud constitute a fog computing environment. The development of the security mechanism is being an indispensable part of the IoT environment. This paper expounds certain problems pertaining to both IoT and Fog environment. Heterogeneity and mass deployment are the two basic issues that make

handling the security in IoT difficult. An extended work can be done in this a field, that deals with the above stated issues efficiently and effectively.

REFERENCES

[1] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in Future Internet – FIS 2008 Lecture Notes in Computer Science Vol. 5468, 2009, pp 14-28.

[2] A. Alshehri and R. Sandhu, "Access Control Models for Cloud-Enabled Internet of Things: A Proposed Architecture and Research Agenda," 2016.

[3] C. Puliafito, E. Mingozzi, and G. Anastasi, "Fog computing for the internet of mobile things: issues and challenges," in Smart Computing (SMARTCOMP), 2017 IEEE International Conference on, 2017, pp. 1-6: IEEE.

[4] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the first edition of the MCC workshop on Mobile cloud computing, 2012, pp. 13-16: ACM.

[5] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," IEEE Communications Surveys & Tutorials, 2017.

[6] Geng Yang, Jian Xu, etc.: Security Characteristic and Technology in the Internet of Things. J. Journal of Nanjing University of Posts and Telecommunications (Natural Science). 30(4) (2010)

[7] Vaquero, L. M., & Rodero-Merino, L. (2014). Finding your way in the fog: Towards a comprehensive definition of fog computing. ACM SIGCOMM Computer Communication Review, 44(5), 27-32.

[8] Yi, S., Qin, Z., & Li, Q. (2015, August). Security and privacy issues of fog computing: A survey. In International conference on wireless algorithms, systems, and applications (pp. 685-695). Springer, Cham.

[9] Stojmenovic and W. Sheng, "The Fog Computing Paradigm: Scenarios and Security Issues," Federated Conference on Computer Science and Information Systems (FedCSIS), pp.1-8, Sept. 2014.

[10] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In 2010 Proceedings IEEE (pp. 1-9). IEEE.

[11] Han, H., Sheng, B., Tan, C. C., Li, Q., & Lu, S. (2009, April). A measurement based rogue ap detection scheme. In *IEEE INFOCOM 2009* (pp. 1593-1601). IEEE.

[12] Wei, W., Xu, F., & Li, Q. (2012, March). Mobishare: Flexible privacy-preserving location sharing in mobile online social networks. In *2012 Proceedings IEEE* (pp. 2616-2620). IEEE.

[13] Shi, Y., Abhilash, S., Hwang, K.: Cloudlet mesh for securing mobile clouds from intrusions and network attacks. In: Mobile Cloud 2015)

[14] Li, S., & Zhang, K. (2008). Principles and applications of wireless sensor networks.

[15] Xueguang Yang, Fengjiao Li, Xiangyong Mu, etc.: Design of security and defense system for home based on Internet of things. J. computer application. 30(12):300-318 (2010)

[16] Antonio J. Jara, Miguel A. Zamora, Antonio F. G. Skarmeta.: HWSN6 Hospital Wireless Sensor Networks Based on 6LoWPANTechnology: Mobility and Fault Tolerance Manageme nt. C. In: International Conference on Computational Science and Engineering, 879-884 (2009)

Authors Profile

Shalini Chandra is working as Assistant Professor in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, UP. Her research area is software security and software quality.

Richa Verma is pursuing PhD in Computer Science from Department of Computer Science, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, UP. She is Gold Medallist in Master's in Information Technology from same University in 2017. Her research interests are in the areas of Network Security, Fog computing and IoT Security.

