ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

Survey on Security issues of Fog Computing

Rahul Neware, Nishi Walde

P.G. Student, Department of Computer Science & Engineering, GHRCE Nagpur, Maharashtra, India

U.G. Student, Department of Electronics & Telecommunication, SBJCER Nagpur, Maharashtra, India

ABSTRACT: Fog computing is one of the most essential paradigms used in contemporary international as an extension to cloud computing. Like Cloud Computing, it provides information storage, manipulation and computation of data, however to the threshold of the network, i.e. To the consumer give up. This studies paper offers with the risk to protection problems, especially with location privateness and records confidentiality. The manner carrier companies as well as government can access customers facts is covered. Furthermore the misconceptions approximately the rights of users are discussed. Finally the idea of decoy method with some modification for location and information privateness is likewise blanketed.

KEYWORDS: Fog Computing, Cloud Computing, Security, Privacy.

I. INTRODUCTION

The recognition of smart gadgets related everywhere are shaping the destiny of the cutting-edge international, The way technologies are being evolved along with smart metering machine,[2] clever wearable gadgets, smart towns as well as huge scale sensor improvement are making the entirety smarter and related, described as Internet of matters (loT), According to new studies from International Data Corporation (IDC), "The worldwide Internet of Things (loT) marketplace will grow from $655.Eight billion in 2014 to $l.7 trillion in 2020 with a compound annual growth rate (CAGR) of 16.9%,Devices, connectivity, and IT offerings [1] will make up the general public of the loT market in 2020." Usually we understand, there are many troubles confronted by way of smart gadgets consisting of battery difficulty, garage, gradual reaction time as well as computation energy which in the long run lowers the exceptional of the tool and usual revel in by the user. In order to overcome such issues faced by means of the clever devices, fog computing is acknowledged as an assuring computing popular, that can deliver records to the brink of the network! To the consumer result in a manner such that there is higher[5] first-class reassured of infrastructure, platform and software as nicely as at low relative value.

Cloud and fog computing are the 2 software program paradigm that can't completely overtake one another as each are equally vital. Hence, Fog computing is a now not complete solution. Even there are numerous issues which are unsolved as Internet of things (loT) applications require most vital data approximately the person along with geo-distribution, mobility help, region focus as properly as low latency, More Importantly Fog (Edge) Computing is proposed to allow computing directly at the fringe of network in order that data may be transferred right away to billions of offerings and packages which can be related. A manner to study the layers of fog computing is to keep in mind it as a virtual platform this is located among the cloud centers and the devices as shown in Fig, 1, Typical example of fog computing devices is Wireless Sensors and Actuators Networks (WSANs), Google glass, cell base stations etc, Fog Computing supports a spread of different services and alertness consisting of big information analysis, internet content transport, and augmented reality, [10]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

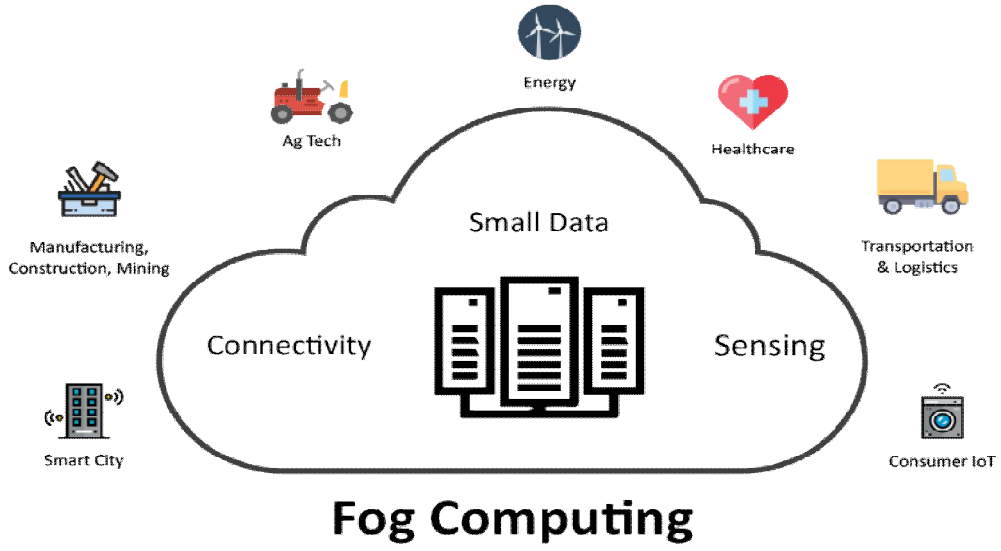

Fig. 1 Fog Computing components

Though fog is an essential extension of cloud computing, so there are some safety and privateness issues which can be unavoidable and feature a high-quality impact on it. Since those [3] issues if no longer well sorted will only effect the advertising of fog computing. We can see the assessment of laaS adoption in public, hybrid and personal cloud in Fig. 2. As Fog is in its growing section, and is proposed in context to Internet of factors, safety troubles are inherited with the aid of it from the cloud. While some problems are inherited even as there are new troubles that occurs because of distinct feature of fog computing together with area focus, low latency, mobility help required, massive no. Of geo-disbursed nodes and unique sorts of fog node and community.[11].

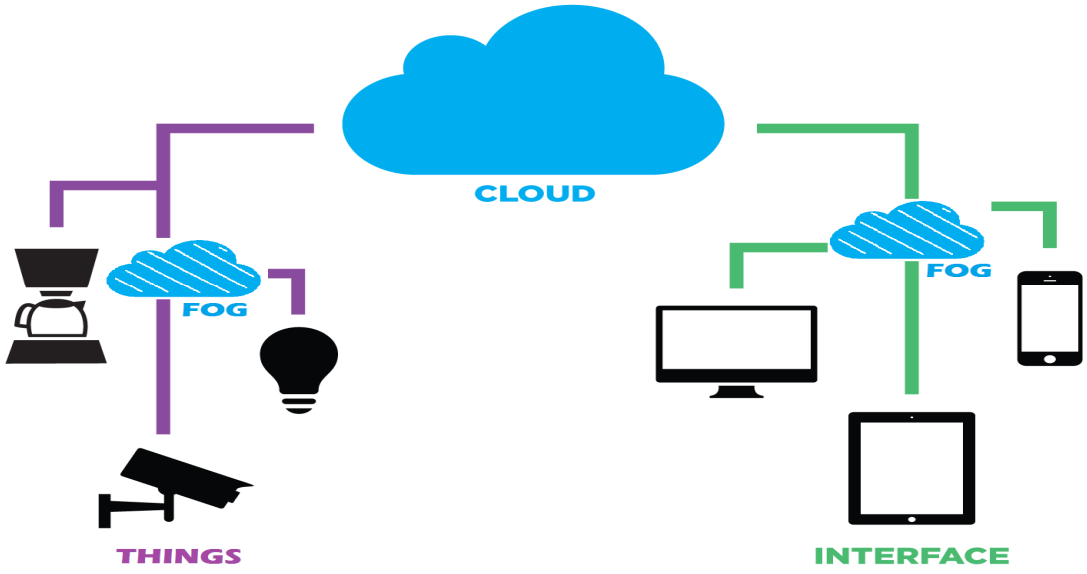

Fig. 2 Fog layer after Cloud

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

II. OVERVIEW

Here, we are able to provide an overview of fog computing. It is assumed that readers are acquainted with the cloud and cell cloud computing and if feasible can discuss with extraordinary web sites on internet. Fog computing extends the cloud computing so it can be in the direction of the things that produce and act on Internet of things (loT) records. These matters which are at user-end are referred to as fog nodes and may be used anywhere inside a community connection. Fog nodes are those gadgets with the capacity to compute, shop and may be linked to a network connection. For Example switches, routers and video surveillance camera and so forth. Keeping the vision in thoughts, a short definition became proposed at some point of 2014 as a case in which a completely large variety of heterogeneous (from time to time autonomous and wireless) ubiquitous in addition to decentralised gadgets speak with every different and gadgets capable of cooperating with every different and processing records without the involvement of 1/3 parties. Most of these responsibilities are for supporting the functions of fundamental network or services that are new as well as those programs which run in a sandboxed environment[12]. Users leasing part of their devices [1] to host those services get incentives for doing so. In truth those definition are contradictive in nature however the time period fog computing isn't always in any respect a fuzz phrase. Fog computing has its own advantage but there are many disadvantage which we are able to be focussing in our paper.

III. SECURITY ISSUES OF FOG COMPUTING

3.1 Data Security Issue:

In fog Computing User's control to information is overtaken via fog node, subsequently the identical safety troubles rise up of cloud computing. Data Integrity cannot be maintain as facts can be lost or also can be modified. The information which is uploaded to the fog node can also be used by the 1/3 celebration. There are various strategies which can [5] be used to offer statistics Integrity, confidentiality and verifiability which includes aggregate of homomorphic encryption and searchable encryption. These strategies make certain that purchaser does now not keep statistics on untrusted server. Cao et al has made schemes the usage of the LT code which considers the storage(1ess) a primitive factor, additionally the information can be retrieve in a miles quicker way and for this reason the communication cost will become low. There are always new demanding situations in fog computing associated with the designing of the [9] storage device which can cope with the dynamic operations in a much faster way and takes less area.

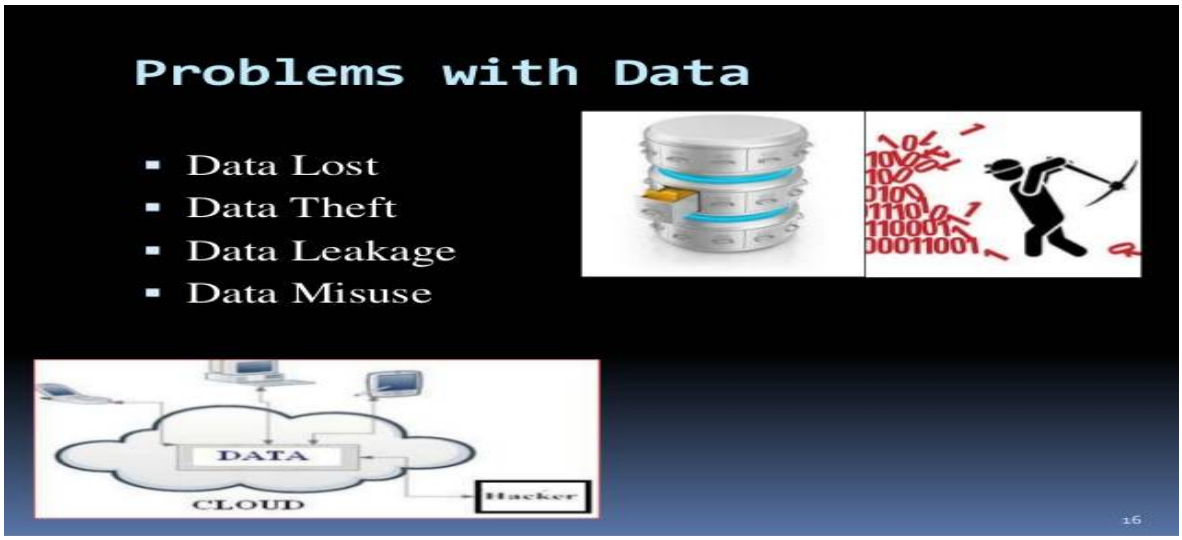

Fig 3.1 Data Security issues in Fog Computing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

3.2 Network Security Issue:

Development of wireless technology has led to the bigger issues in security. Fog computing is effected in a comparable approaches like other wireless technology is affected. Various examples of such attacks are sniffer, spoofing, jamming and so on. These assaults usually take region among the fog node and the centralized machine . Generally, we are sure to agree with the configurations generated by means of our network administrator, which separates [8] the normal records traffic from our community. Hence it brings numerous burden to the community manager. Furthermore fog nodes are at the brink of the network, which most effective will increase the weight of the network manager. SDN (Software Defined Networking) can be used as an technique for the network manager to work at the low degree of abstraction for the community offerings. It can assist in control, growth scalability of network as well as reduce value with regards to fog computing. We can use Network Monitoring and Intrusion Detection System [2] to observe the traffic, Traffic Isolation and Prioritization device can be used to save you attack through shared assets, Network resource get entry to control system facilitates to get get entry to control on SDN (Open Control), Network Sharing System can help the fog node router tobe open to visitors considering the security problems as properly.

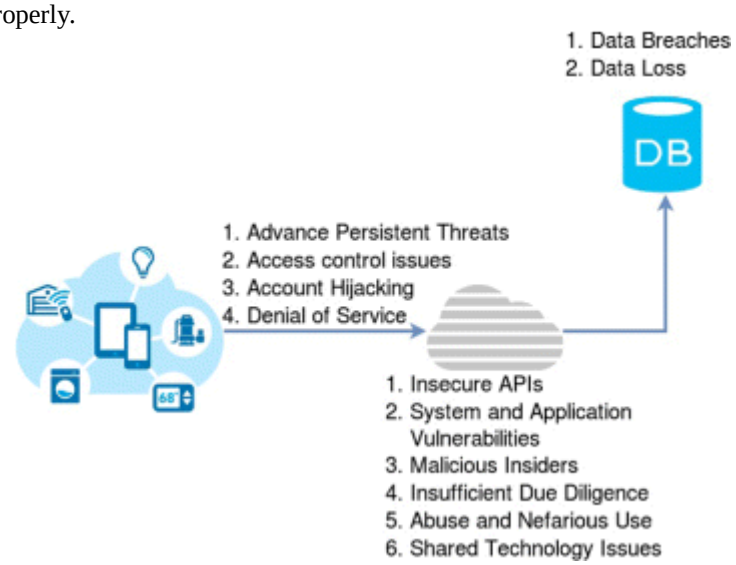

Fig. 3.2 Network Security issues Fog Computing

3.3 Privacy Issues:

The way privateness of a person isn't always sustained had made this difficulty of great problem. Not simplest the service provider however the reality that Government too is involved in it makes it extra tough. In truth it even come to be simpler for the 1/3 birthday celebration to advantage access to the user's private information, vicinity and so on. And as a result the person turns into attack-susceptible. Due to statistics shipping at the brink of fog node, it will become lot easier to accumulate all the important data of a user. This is one of the maximum tough trouble in fog to preserve the privateness of a user.

3.3.1 Data Privacy:

There are many facts's privacy preserving algorithm available within the marketplace but maximum of them makes use of the concept of aid prohibition at the edge devices. We recognize commonly fog node collects all the important information generated for its green use and because of it homomorphic encryption [3] idea can be utilized. Even when the fog nodes collects data it has all the vital data such as while the user is at home, who else is with him and so forth. We should make sure that this facts have to not be added to the 1/3 birthday party. One feasible solution is to generate greater dummy site visitors and load them to the fog nodes, so that nobody can identify the unique records.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

3.3.2 Location Privacy:

Privacy of vicinity commonly refers to vicinity privateness of the consumer at the threshold of fog computing. As the information is brought to the cease ofthe fog node, it can be used to discover how a long way the person from different fog nodes is. Moreover, if the customer is using many fog services, possible without difficulty realize the course statistics has taken and for this reason our privacy place is at risk. Usually fog purchaser chooses the closest fog server, and as a result can without problems be prone to attacks because the fog nodes recognise the place of the client. One such technique of preventing the violation of location privacy in fog computing is "identity obstruction". In it the fog node can't without difficulty identifY exactly the closest fog consumer amongst many others. There are lots of methods available to use identification obstruction method as an instance, we use a 3rd birthday celebration faux id generator at each end person so that fog consumer has many options available to select fog node from. Basically, fog c1ient[2] does now not use the closest fog node at his/ her very own will however certainly the fog node is selected based on a few standards which includes load stability, reputation, latency and many others. Hence the fog node has best tough idea approximately vicinity of fog patron but now not actual vicinity. Furthermore even after using obstruction approach fog consumer isn't relaxed as its region nevertheless can be jotted down by way of intersecting multiple fog nodes in an area considering that fog consumer uses multiple fog nodes of an area. The idea of fog computing at person quit can offerrich data about the network, its traffic records, its client records which can be used for optimization. The location statistics may turn out to be risky for both facet - purchaser end as well as fog nodes. One can without difficulty get the vicinity of client give up if it is a fog node and of fog node if it's a client quit. Although it's very critical for green strolling of devices. Similarly each fog and cloud plays an crucial function in place privateness as fog can deliver an overview locally even as cloud offers globally.

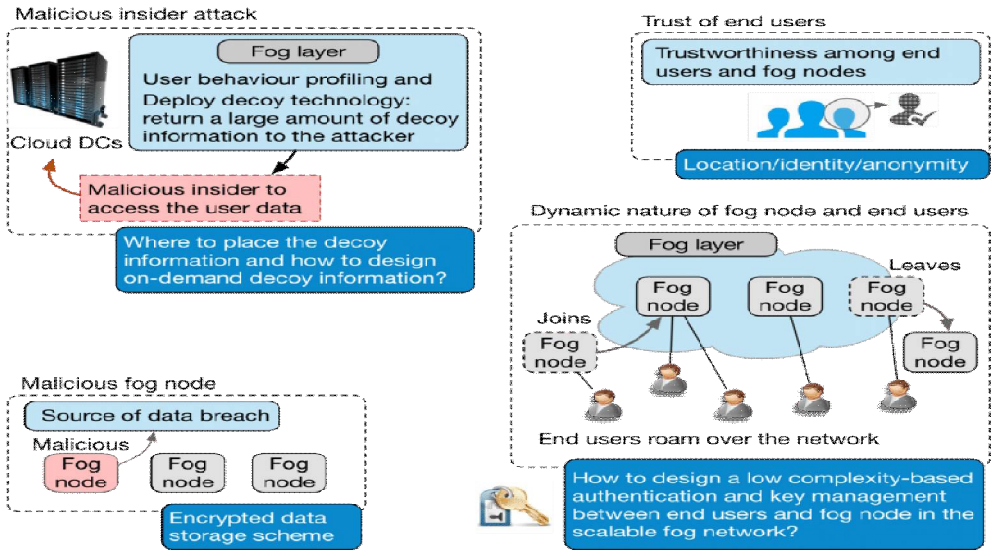

Fig 3.3 Privacy issues in Fog Computing

3.4 Access Control Issue:

Access manipulate is one the maximum crucial device to guarantee the device ' s safety and maintain the user's privateness. Although commonly get admission to manipulate is labelled to the identical domain however due to the distributive nature of cloud computing, it is applied cryptographically. There are many proposed strategy to reap tremendous solution. One of them is of Yu et al in which the access manage is primarily based on Attribute-based totally encryption (ABE). There are even theories in which coverage primarily based get entry to control

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

mechanism is implemented to address the heterogeneous nature of fog computing. It is always a tough task to keep in thoughts useful resource constraints and but design the get right of entry to control structure for the fog.

IV. CONCLUSION

We have discussed most common security hazard to fog computing on this studies paper. We have evaluated the Terms and conditions furnished by way of exclusive cloud carrier vendors and have concluded that most of the storms said are only aiming to steal user's privateness. We have lightened the standards of facts and area privacy and identified new methods the provider companies in addition to government are misusing.

REFERENCES

1. Shanhe Yi, Zhengrui Qin, and Qun Li ," Security and Privacy Issues of Fog Computing: A Survey" 2014.
2. Stojmenovic, I. , Wen, S.,'The fog computing paradigm:Scenarios and security issues." ln: FedCSIS. IEEE (2014)
3. Christof Kauba,Stefan Mayer," When the Clouds Disperse Data Confidentiality and Privacy in Cloud Computing" 14. July 20 I 3.
4. Saniket M. Kudoo, ProfDilipMotwani," Fog Computing: Data Theft Detection in Cloud with Behaviour Pattern & Decoy Stuff' International Journal of Innovative Research in Computer andCommunication Engineering, VoI. 4, Issue I, January 2016
5. Salvatore J. Stolfo," Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", position paper
6. RajashriRaut,.MadhuriWaj e,. Sayali Kulkarni, Ajay K. Gupta," Fog Computing using Advanced Security in Cloud" VoI. 3 Issue 2, February2014.
7. Kshamata, Prachi, Unathi," Fog Computing Future of Cloud Computing". IJSR(International journal of science and research). [8] Niranjanamurthi, Kavitha P 8." Research study on Fog Computing For secure Data Sercurity" Volume no.5, Special Issue(OI), February 20 I 6.
9. Monjour Ahmed, Mohammad Ashraf Hossain," Cloud Computing and Security issues in the cloud" IJNSA
10. Kevin Hamlin, Latifur Khan,"Security Issues For Cloud Computing" Technical Report UTDCS-02-10.
11 . K. ChandraHasan," Research Challenges and Security Issues In Cloud Computing" International Journal of Computational Intelligence and Information Security, March 2012 VoI. 3, No. 3.
12. Osama Harfou shi, Badel Alfawwaz," Data Security Issues and challenges in cloud computing: A conceptual analysis and revi ews" voI. 6, No. I February 20 I 6.

BIOGRAPHY

Rahul Neware is a Post Graduation (MTech) student in Computer Science & Engineering Department, G. H. Raisoni College of Engineering. He received Bachelors of Engineering (Information Technology) degree in 2015 from DBACER, Nagpur, MS, India. His research interests are Cyber Security, Cloud Computing, Fog Computing, Cyber Physical System and Distributed Operating System.

Nishi Walde is a Bacholer of Engineering (B.E.) student in Electronics & Telecommunication Department, S. B. Jain College of Engineering & Research. Her research interests are Fog Computing, Cyber Physical System and Robotics.