IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue-9, April 2019 E-ISSN: 2347-2693

Fog Computing and its Security Issues

Keerthi T.R.[1*], Mohit Agarwal[2]

[1,2]Dept. of Computer Application,Dayananda Sagar Institution, Bangalore, India

Corresponding Author: keerthichouts@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si9.8790 | Available online at: www.ijcseonline.org

***Abstract*—** Fog Computing is another worldview that increases the Cloud storage through figuring assets on the edges of a system. It is clearly well described as a cloud-like stage containing comparative information, computation and application administrations, yet is on a very basic level diverse in that it is decentralized. Furthermore, Fog computing are equipped for preparing a lot of information locally, work on-premise and are completely convenient. It can be on mixed equipment's. These highlights make the Fog stage extremely reasonable for time and area for touchy applications. For instance, Internet of Things (IoT) Devices having lot of information and its required rapidly process for working. This large area of usefulness driven applications increases numerous confidentiality issues with respect to information, virtualization, isolation, organize, malware and observing. This paper reviews existing papers on Fog figuring applications to resolve regular security holes. Comparable advancements like Edge figuring, Cloudlets and Micro-server farms having same incorporated to give a comprehensive audit process. Most of Fog applications are roused by the longing for usefulness and end-user prerequisites, while the confidentiality aspects are frequently disregarded or measured as a bit of hindsight. This paper also determines the effect of those security issues and conceivable solution, giving prospect security-pertinent headings to those responsible for designing, emerging, and preserving Fog systems.

***Keywords*—**Iot, Cloud, Fog, localized, Edge computing, Decoy, Hashing.

I. INTRODUCTION

Fog computing is a localized computing architecture where the data is processed and stored between the origin and a cloud infrastructure. This outcomes in the minimization of information transmission overheads, and subsequently, improves the execution of figuring in Cloud stages by lessening the necessity to process and store extensive volumes of unnecessary information. The Fog processing worldview is to a great extent propelled by a ceaseless increment in Internet of Things (IoT) gadgets, where a consistently expanding measure of information (concerning volume, assortment, and speed) is created from a regularly growing cluster of gadgets.

Since the Cloud figuring, is not at all "one-measure fit-all" Solution. Still there are uncertain issues since IoT applications more often than not require versatility support, redistribution, area mindfulness and low inertness. Fog Computing, edge figuring, is planned to empower processing legitimately at the edge of the system, which can convey new requests and administrations for billions of associated gadgets. Fog gadgets are generally set-top-boxes, passages, street side units, cell base stations, and so on. End gadgets, fog and cloud are shaping a three layer progressive administration conveyance demonstrate, supporting a scope of utilizations, for example, web content conveyance , increased reality , and huge information examination. A Conceptual architecture of fog computing is shown in figure1

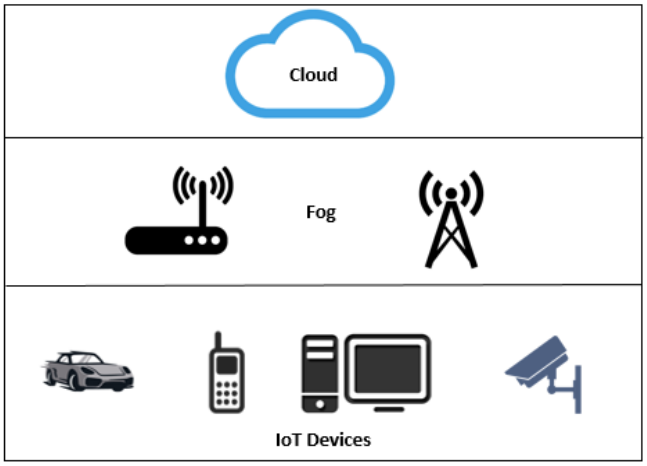

Figure 1 Conceptual architecture of Fog

Since fog is regarded as a non-irrelevant expansion of cloud, few security and protection issues with regards to cloud computing, can be anticipated to compulsorily effect on fog

computing. Security and protection issues will slack the advancement of fog infrastructure if not very much tended to, as indicated the way that 75% of IT Executives and Chief Information Officers dismiss cloud in term of the dangers in security and protection. As fog processing is still in its starting stage, there is little work on security and protection issues. Since fog infrastructure is proposed with regards to Internet of Things (IoT), and started from cloud figuring, security and confidentiality issues of cloud are acquired in fog computing. While a few problems can be tended to utilizing existing plans, there are different issues confronting new difficulties, because of the particular qualities of fog infrastructure, for example, heterogeneity in fog hub and fog connection, prerequisite of versatility support, vast scale geo-circulated hubs, area mindfulness and low dormancy.

In this paper, we will examine a few security and confidentiality issues in Fog infrastructure, by auditing existing work of Fog infrastructure and related in basic domains, to distinguish security and privacy issues.

II. WHY FOG?

Fog infrastructure isn't substitution of distributed computing. The Fog infrastructure is actualized at edge of the system, it gives edge area, location mindfulness, low idleness, support for versatility and quality-of-services (QoS) for gushing and genuine applications. The Fog computing worldview is very much situated for constant enormous data diagnostic, thickly conveyed information accumulation focuses, and gives focal points in stimulation, personal computing and different applications.

A. Advantages

- Confidentiality control**:**With fog infrastructure, you can more likely control the dimension of security. You can process and break down delicate information locally instead of having to sending them to a unified cloud for investigation. By keeping the procedure local, the IT group can screen, track, and control any gadget that gathers or stores information.
- Improve business productivity:Working pair with different artificial intelligence (AI) technologies, fog infrastructure can possibly spare your business time and cash by diminishing your IT directors' burden.
- Data privacy: Security is among the most vital parts of business. Fog computing enables you to associate different gadgets to a system. For what reason is this advantage? Instead of one concentrated area that may end up powerless, movement happens between different nearby endpoints, making it simpler to distinguish dangers, for example, tainted documents, potential hacks, or malware. Furthermore, the threats are recognized a lot before and can be contained at the gadget level as opposed to tainting or taking a chance with the entire system.

B. Disadavantages

- Encryption algorithms and security approaches make it progressively troublesome for arbitrary gadgets to trade information. Any slip-ups in security algorithms lead to exposure the information to the hackers
- The entire idea of fog computing appears to be perplexing and confounding. A framework that incorporates numerous gadgets that store and examine their own information and that could be found anyplace, whenever adds multifaceted nature to a system that once sent every one of its information to a centralized area.
- To accomplish more data consistency in the fog computing is testing and requires more efforts.
- Power utilization is more in fog hubs contrast with integrated cloud engineering.

III. FOG COMPUTING AND COMPARABLE TECHNOLOGIES

Despite the fact that the word Fog computing was first introduced by Cisco, comparative ideas have been inquired about and created by different gatherings. The following of details such three technologies, including a portion of their key contrasts with Fog frameworks.

A. Edge computing

It performs limited preparing on the gadget utilizing Programmable Automation Controllers (PAC), which can deal with information handling, stockpiling and communication. It represents leverage over Fog processing as it diminishes the purposes of disappointment and makes every gadget progressively autonomous. In any case, a similar component makes it hard to oversee and aggregate information in huge scale systems, for example, IoT.

B. Cloudlets

It is a center piece of 3-level hierarchy "mobile gadget - cloudlet - cloud". There are four noteworthy traits of Cloudlet: altogether self-overseeing, has enough process control, low end-to-end dormancy and expands on standard Cloud innovation. Cloudlet contrasts from Fog computing as application virtualization isn't reasonable for nature, expends more assets and can't work in offline mode.

C. Micro data server

It is a little and completely useful server containing various servers and is fit for provisioning numerous virtual machines. Numerous technologies, including Fog computing, can profit by Micro server as it diminishes dormancy, upgrades dependability, moderately convenient, has worked in security conventions, spares transfer speed utilization by pressure and can oblige numerous new services.

IV. SECURITY ISSUES

A. Man-in-the-Middle Attack:
A man-in-the-middle attack is a type of attack where attacker enter into the communication between two persons, harms both persons and access all information that the persons were trying to communicate each other.

B. Harmful Fog Node Problem:
In process to providing fog services to user, fog process received data from the IoT devices. If the work pressure is large it will be divided and manipulation by many fog hubs. If in between few nodes are harmed by harmful user it very difficult to providing ensure of data. So, before processing start, nodes must trusted for which authentication protocol is needed.

C. Malicious Searching Technique in fog infrastructure:
After the nodes settled, hybrid searching technique is useful to search harmful code inside the nodes. It can be combination of Signature- Based Detection technique and Role based searching technique.

D. Information Executive issues:
While nodes are distributed and rearranging order makes difficult to know where the data is stored. So, if the user want to give with the same place and it will be very difficult for user to know whether the node gives same services. Few nodes having same files may waste space.

V. PURPOSED TECHNIQUES

There are two approaches we can use for securing fog computing environment

A. By using Decoy Information and Client behaviour profiling.
 Approach:
Decoy network: Decoy information, such as decoy documents, honeypots and other bogus data that can be used for searching abnormal access to data that can be made on demand and to 'poison' the ex-filtrated data. The decoy will confused to the attackers to understanding that they have ex-filtrated important data, but actually they don't have that data. When the unauthenticated access to cloud is watched, decoy data is back by the cloud and send in such way that appears normal.

Client behaviour profiling: It is relied upon that permission to a client's data in cloud will display an easy-going methods for access. Client profiling is natural innovation that can be connected to show how, how much, when the client get to a data in cloud. Such "normal Client" can be consistently checked to decide if anomalous access to a user's data is emerging. This strategy is normally utilized in fraud identification applications

There will be two main modules:
User and Admin where User can login, upload, search, view and download the data and Admin can manage the users along with log details, can upload decoy and manage files.
Modules:
User Validating
Admin
Record Access Module
Information Access Module
Decoy Module

B. By using Cryptographic Hashing Algorithm.
A Cryptographic hashing algorithm can be used as securing the data in which the input data is variable length and output will be fixed length size string. The string is called as digested message. Hash functions are continuously using for checking integrity and error detection of sent and receive messages

The popular hashing algorithm are - MD which is also known as Message Digest and SHA which is also known as Secured Hashing Algorithm

VI. CONCLUSION

Stealing data attack is major issues for cloud service providers. In fog infrastructure we presented new approach which can solve the security problem in fog computing in few aspects. Using decoy technology which can reduce the insider attack in cloud. Using cryptographic hashing algorithms we can secure the data. However as we know that is not solution of security problems but it can be reduce attacks that happening on regular bases.

REFERENCES

[1] Lee, Kanghyo, et al. "On security and privacy issues of fog computing supported Internet of Things environment." Network of the Future (NOF), 2015 6th International Conference on the. IEEE, 2015.
[2] Wang, Yifan, Tetsutaro Uehara, and Ryoichi Sasaki. "Fog computing: issues and challenges in security and forensics." Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual. Vol.3, IEEE, 2015
[3] Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." International Conference on Wireless Algorithms, Systems, and Applications. Springer International Publishing, 2015.
[4] Ben-Salem M., and Stolfo Angelos D. Keromytis, "Fog computing: Mitigating Insider Data Theft Attacks in the Cloud," IEEE symposium on security and privacy workshop (SPW) 2012.
[5] Arwinder Singh, Abhishek Gautam, Hemant Kumar, Er. C.K. Raina. "Decoy Technology in Fog Computing" International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 6, Issue 3, March 2017
[6] Thanh Dat Dang and Doan Hoang; A Data Protection Model for Fog Computing; IEEE Conference; 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC); 2017 IEEE; pp. 32-38.

[7] Hany F. Atlam, Robert J. Walters and Gary B. Wills; Fog computing and the internet of things: A Review; Big Data and Cognitive Computing; 2018,2,10; doi:10.3390/bdcc2020010
[8] Shubha Brata Nath, Harshit Gupta, Sandip Chakraborty, Soumya K Ghosh; A survey of fog computing and communication: Current researches and future directions; IEEE Communication Surveys and Tutorials; April 2018
[9] Sai Keerthi.Tulluru, Dr.Anuradha S.G. "Fog Computing a Paradigm: Scenarios And Security Issues"International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018
[10] Blesson Varghese, Nan Wang, Dimitrios S. Nikolopoulos and Rajkumar Buyya; Feasibility of Fog Computing; arXiv:1701.05451v1 [cs.DC] ; 19Jan 2017.
[11] Pengfei Hu, SahraouiDhelim, Huansheng Ning and Tie Qiu; Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues; ELSEVIER Journal of Network and Computer Applications 98 (2017); DOI: 10.1016/j.jnca.2017.09.002; September 12, 2017
[12] Chiang, Mung, and Tao Zhang. "Fog and IoT: An overview of research opportunities." IEEE Internet of Things Journal 3.6 (2016): 854-864.

AUTHORS PROFILE

Ms. Keerthi T R pursued Bachelor of Computer Applications from Banglore University in year 2013 and Masters of Computer Applications from Visvesvaraya Technological University in year 2016. She is currently working as Assistant Professor in the Department of Computer Applications, Dayananda Sagar College of Arts, Science and Commerce. She has taken up online NPTEL courses on the filed Cloud Computing and Data Base Management Systems. She has attended National seminar on Block Chain Technologies. Her main area of research interests are IoT, Data Mining and Big Data Analytics. She has 2 years of teaching experience.

Mr Mohit Agarwal is pursuing Bachelor of Computer Application from Dayananda Sagar College of art science and commerce in year 2016-2019. He is participated more than 5 hack-a-thon in the field of Block chain technology, cloud and transformation. He has published more than 7 research paper in reputed international journals including IEEE and it's also available online. He has taken up online NPTEL courses on the field cryptography, IoT, python and Java.

