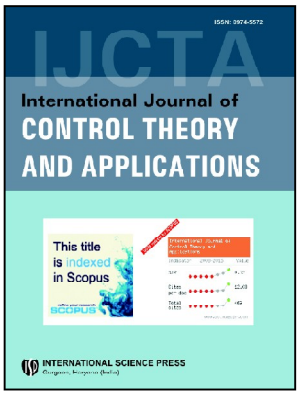

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 11 • 2017

A Survey of Fog Computing: Fog Node Security & Issues

B. Chanakya[#1] and Dr. P. Sai Kiran[#2]

[#1] PG Student, Department of Computer Science and Engineering, K L University, Vaddeswaram, Guntur, 522502, India
E-mail: bolledduc@outlook.com
[#2] Professor, Department of Computer Science and Engineering, K L University, Vaddeswaram, Guntur, 522502, India
E-mail: psaikiran@kluniversity.in

Abstract: Fog computing is a new paradigm introduced to overcome the issues of cloud computing. Fog doesn't replace cloud computing but it is an extension of the cloud computing. Fog provides data, storage and computation to the end users; it also supports an emerging concept called Internet of Everything (IoE). This paper mainly presents the issues and challenges of fog computing in a brief manner.

Keywords: Cloud Computing; Fog Computing; Internet of Everything; Fog Node

1. INTRODUCTION OF FOG COMPUTING

Fog computing brings the systematic positioning of computing, storage and networking resources between end points and to consistent clouds. It is similar to cloud computing but it's lower to ground, the new elements brought to the fog computing are sensitive to real time response, so that they can control critical resources like healthcare, traffic, energy, parking, etc..,. Fog computing is a new paradigm introduced to address the limitations of cloud computing and it mainly supports to Internet of Everything [1] [2] [3].

Fog computing is a geographically distributed computing architecture with a shared pool of resources that consists of heterogeneous device (one or more) connectivity at the edge of the network and backed up by cloud services. In general Fog computing defines the extension of cloud computing or it acts as an intermediate layer between cloud/data center and end devices. Fog computing doesn't have standard architecture where the research is still going on; figure 1 shows the overview of fog computing architecture [4] [5].

Fog computing resolves the many issues of cloud computing such as Latency, Data Security, Bandwidth, Wide Geo-Distribution, Mobility and Heterogeneity. It consists of fog nodes and fog servers which support dynamic strategy. Fog nodes are configured at the edge of the network which is reliable to end devices and these nodes are connected to dedicated fog servers where the real-time data is stored in a volatile manner [4] [5] [11] [12] [13].

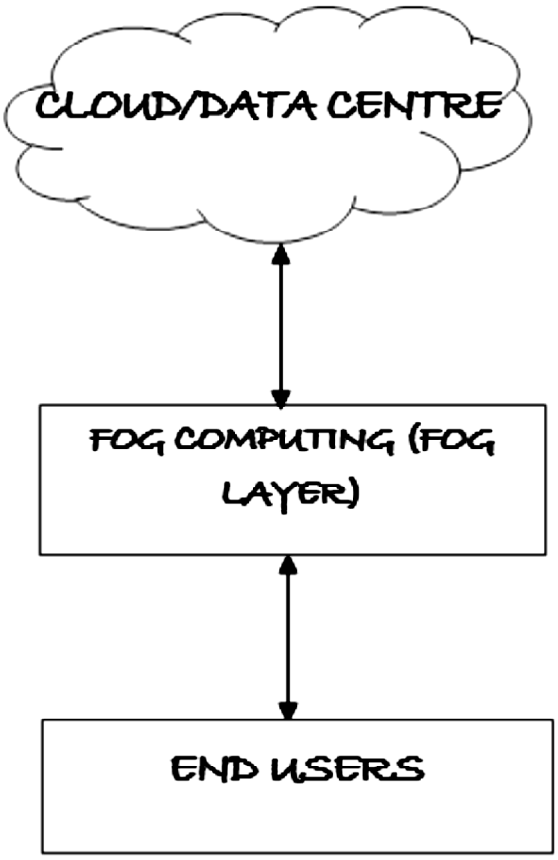

Figure 1: Overview of fog computing

2. CHALLENGES OF FOG COMPUTING

- ✓ ***Security:*** Provides security to the real-time transaction data and also to the stored data in cloud by using some trusted mechanisms. □
- ✓ ***Scalability:*** Based on On-Demand requests fog nodes can deploy easily and faster in any wide geo graphical locations. □
- ✓ ***Mobility:*** The connectivity between fog nodes and the mobile user should communicate randomly based on the movement of mobile user from any geographical location. □
- ✓ ***Interoperability:*** Fog computing able to provide services between two different environment and devices to communicate together effectively.
- ✓ ***Hierarchy:*** Fog computing should support cloud and also multiple tiers [6] [7] [8].

3. ISSUES IN FOG COMPUTING

As mentioned earlier, Fog computing is a new paradigm which was introduced to address or overcome the drawbacks of cloud computing. Even though Fog computing has many advantages, it falls short in these scenarios known as: Fog Node Security, Data Security, Network Security, security monitoring and management, Access Control, Intrusion Detection and general security & privacy issues. This paper mainly discusses the following concepts such as

3.1. Fog Node Security

Fog Node Security is a primary issue where Fog computing is an open platform which has a chance of attack by illegitimate users on Fog Node and the other problem in fog node is communication of fog nodes (Node-to-Node, Node-to-Device, and Node-to-Cloud). There are four categories in Fog node security they are: *Trusted Execution Environment, Data Security, Network Security and Physical Security* [10].

- ✓ ***Trusted Execution Environment:*** It starts from the root of hardware installation or execution in a trusted state. In this environment, the storage (volatile and non-volatile), boot of the device, hardware based environment and virtualization environment should be secured. There will be multi operating system environment which will follow the virtualization concept because of which some vulnerable information might spread into the fog node in real-time by illegitimate users or nodes [10].
- ✓ ***Data Security:*** Data in Rest the entire disk/cloud will be encrypted and the protection should be in granular and role based this data will be accessed by those only who have the device access permission [10].
- ✓ ***Network Security:*** Data in Motion represents network security; here the encryption should be done for both Data in Rest and Data in Motion. The required hardware is encrypted SoC device for high bandwidth and ISA for lower bandwidth. It also ensures WEP authenticated end points to wireless LAN and 802.1X LL encryption. In fog node, network security cannot be provided directly [10].
- ✓ ***Physical Security:*** Processor, SoC devices, board, Chassis level detection are to be secured. In this, there is a chance of occurrence for Intrusion Detection and Tamper-Proofing, so that users can monitor frequently [10].

3.2. Access Control

Access Control is one of the vital credentials for a security of the system to prevent the illegitimate users. In general, the access control mechanism is based on *Trust domain* because of which people are facing many issues. In order to overcome these issues, this paper recommends a two method access control credentials named as: Attribute-Based Access Control (ABAC) and History-Based Access Control (HBAC). By using these two methods the communication between any two heterogeneous devices can be secured. The major challenging issue in Access control is designed i.e. while designing, it should meet the design requirements and also it should be implemented in all the three tiers of Fog computing (Client-Fog-Server) [9].

3.3. Security Monitoring & Management

Fog nodes are widely & geographically distributed consisting of heterogeneous devices because of which it is difficult to know the malicious user or attacker. To overcome this issue Fog servers need to maintain the log information of the fog nodes based on their behaviour to know whether the fog nodes are attacked by attackers or not [10].

3.4. Intrusion Detection

Intrusion detection technique is deployed in every wide geographical fog nodes as well as cloud systems to protect from the illegitimate users or attackers. This system monitors the activities of the user to eradicate misuse of the data by attackers or illegitimate users. Attackers can attack Kernel based (Virtualization platform such as Operating System) and Network based. There are three types of Intrusion Detection techniques: Kernel-Based, Anomaly Based, and Stateful Protocol Analysis [9].

3.5. Man in the Middle Attack

In Fog computing while there is a transfer of data from one node to another node and Device to node, there is a possibility of Man-in-the-Middle attack. In this attack, the attacker may attack the packets and modified by the fake ones. It is difficult to provide both encryption and decryption mechanisms for mobile users because it consumes large amount of storage and battery. The main problem is communication protection between IoT devices-to-Fog node, Fog server-to-Fog Node, Fog Node-to-Fog Node (Immediate) and Fog server-to-Cloud [9][10].

4. CONCLUSION

This paper discusses challenges and issues in the context of fog computing, which is a new computing paradigm to provide elastic resources at the edge of the network to nearby end-users. Fog Computing is an emerging concept whereas it is in still research state.

REFERENCES

[1] Peter Mell and Timothy Grance, "NIST Definition of Cloud Computing", US Department of Commerce, Special Publication 800-145.

[2] Bar-Magen Numhauser, Jonathan, Fog Computing Introduction to a New Cloud Evolution. Spain, 2013

[3] "Fog Computing:" https://en.wikipedia.org/wiki/Fog_Computing.

[4] Maher Abdelshkour, "IoT, from Cloud to Fog Computing" blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing, 25 March 2015.

[5] MaciejKranz, "Fog Computing: Bringing Cloud Capabilities Down to Earth", blogs.cisco.com/digital/fog-computing-bringing-cloud-capabilities-down-to-earth, 10 August 2015.

[6] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, SateeshAddepalli, "Fog Computing and its role in the Internet of Things", in ACM 978-1-4503-1519-7/12/08, 17 August 2012, Finland.

[7] "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are", Cisco 2015.

[8] Rob Chandhok SVP and President, QIS and QIP Qualcomm Technologies, Inc. "The Internet of Everything What is it? What's driving it? What comes next?" , Qualcomm Technologies, 2013-2014

[9] Shanhe Yi, Zhengrui Qin, Qun Li, "Security and Privacy Issues of Fog Computing: A Survey", in Springer International Publishing, pp.685-695, August 2015.

[10] John K. Zao, "Security of IoT and Fog Computing: Emerging Challenges & Opportunities". https://youtube.com/watch?v=uLWvK8KcEis, 24 October 2016.

[11] V Krishna Reddy, Yerneni Sushmitha, K Thirupathi Rao "Distributed Authentication for Federated Clouds in Secure Cloud Data Storage" Indian Journal of Science and Technology (IJST), Vol 9, No.19, May 2016.

[12] V Krishna Reddy, K Deva Surya, M sai Praveen, B Lokesh, A Vishal, K Akhil "Performance Analysis of Load balancing Algorithms in Cloud Computing Environment" Indian Journal of Science and Technology (IJST), Vol 9, No.18, May 2016.

[13] B. V. S. Srikanth and V. Krishna Reddy "Efficiency of Stream Processing Engines for Processing BIGDATA Streams" Indian Journal of Science and Technology, Vol 9, No.14, pp: 1-10, April 2016.

[14] Eugen Petac, Andrea-Oana Petac "About Security Solutions in Fog Computing" Ovidius University Annals, Economic Sciences Series, volume XVI, Issue Jan 2016.