Fog Computing and Its Role in the Internet of Things: Concept, Security and Privacy Issues

Muhammad Saad
Computer Engineering Department
Sir Syed University, Pakistan

ABSTRACT
The Internet has evolved in ways that we could never have imagined. In the beginning, advancements occurred slowly. Today, innovation and communication are happening at a remarkable rate. Now days, Internet has become the most important aspect of our life. Starting from desktop late 90s when one use to go to the device to resolve the problem to the era of smart devices early 20s when everybody carry the devices in its pocket to the new emerging era of internet of everything where we are going to connect each and every non connected device present on the planet.

Even though cloud computing has played an efficient role in the computation and processing of these data, however, challenges, such as the security and privacy issues still cannot be resolved by using cloud computing. To overcome these limitations, the term fog computing has emerged to provide computing resources at the edge of the network. Fog computing is the extended version of cloud computing having the same data storage and computation capabilities but is fundamentally distributed in nature by providing services at the edge of the network.

In this paper, I have given the brief description about the Fog computing, elaborate its complicated architecture, highlighted few feasible application and mentioned about the current security and privacy issues with the recommended security measures which we are going to face while deploying internet of things in to live environment.

General Terms
Security, Encryption, Algorithm, Threats.

Keywords
Fog computing, Internet of things (IoT), Interoperability, Cache Attacks, Malware Protection.

1. INTRODUCTION
We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material. Cloud based computing infrastructure has become an important platform since they provide virtual servers with all the necessary services like storage, application, network, bandwidth and other hybrid facilities. As IoT is evolving very rapidly, the use of cloud computing services has become common and with the passage of time as devices are becoming online to control and manage their data with quick access without any delay has become a challenging task for the current cloud computing platform. In order to achieve the above mentioned requirements, the new technology namely Fog computing has been evolved. The term FOG was first introduced by Cisco.

This technology enables the execution of the data at the edge of the network. Due to this type of architecture it will automatically improve the quality of service as it will result in reduction of delay while transmitting of data from source to destination. With the lack of control over data and deficiency of transparency give rise to many security concerns, which cause insecurity for organizations that want to 'cloudify' their IT infrastructure [1].

Like Cloud structure, a Fog structure is composed of Infrastructure, Platform, and Software-as-a-Service along with the addition of Data Services. The technical structural design of a Fog infrastructure is shown in figure 1.

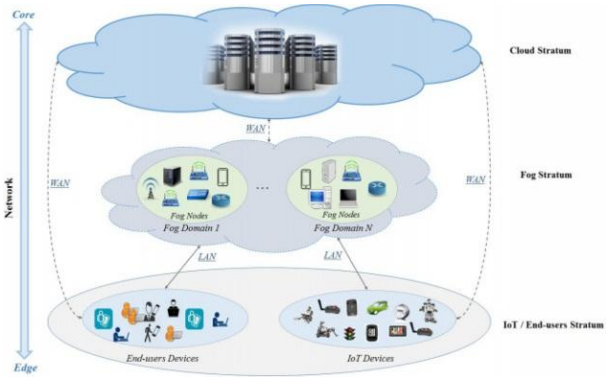

Fig 1: Technical Structural Design of a Fog Infrastructure

Fog Computing in IoT provides large complementary to the previous cloud computing services [2]. Currently, there is a substantial effort focusing on security and privacy in IoT applications across many businesses in which the IoT can be deployed [3].

2. FOG COMPUTING STRUCTURE
Fog computing is the distributed model which expands the old fashioned cloud computing platform to the edge of the network. Fog Computing offers the computation, storage, monitoring, and services capabilities at the edge of network [4]. Here we will discuss the current Characteristics and architecture of fog computing.

2.1 The hierarchical structural design of fog computing
In a couple of years, a numerous architectures have been recommended for fog computing. Fog computing spreads cloud service to the edge of the network by including fog layer between end devices and cloud [5]. Figure 2 shows the hierarchical architecture of fog computing. The hierarchical architecture is based on the following three layers:

2.1.1 Terminal layer:
This layer is located at the end user. It involves various IoT devices such as smart vehicle, smart traffic system, smart

lightening system etc. This layer is used to extract the data of physical entities and conveying these resulted data to upper layer for processing and storage.

2.1.2 Fog layer:

This layer is situated on the edge of the network. Fog computing layer involves a large number of fog nodes, which normally includes routers, gateways, special fog servers, etc. Fog nodes are also attached with cloud data center by central network, and are responsible for communication and collaboration with cloud to get excellent computing and storage proficiencies.

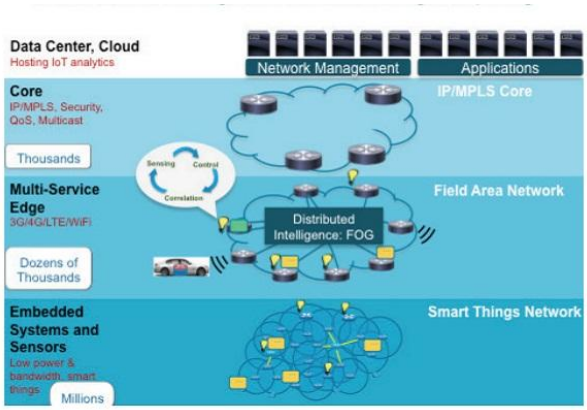

Fig 1: Hierarchical Architecture of Fog Computing

2.1.3 Cloud layer:

This layer includes several special servers and high performance storage devices which provides numerous application facilities such as smart city etc. It has excellent storage and computing capabilities to support for wide computation exploration and permanently storage of an massive amount of data.

2.2 The Features Of fog Computing

The core characteristic of fog computing is to process data at the edge of the network [6]. Furthermore, there are lots of other advantages and characteristics which are listed below:

2.2.1 Low latency and real time interactions:

Due to the availability of the computing resources at the edge of the network, fog computing enables low latency and real time interaction between the user end devices and the fog nodes [7].

2.2.2 Save bandwidth:

Only particular portion of valuable data is transported to the cloud, and maximum unnecessary data doesn't need to be transmitted over the Internet which saves bandwidth utilization.

2.2.3 Mobility support:

Fog nodes in fog layer support both the static and mobile computation resource platform. For example it can be deployed at any bank or at any moving car or train.

2.2.4 Interoperability:

Fog Computing has heterogeneous nature. Fog nodes and end devices come from diverse providers and are usually deployed in the different environments. Fog computing must be able to interoperate and cooperate with different providers to manage with wide range of services and effortlessly support certain services.

3. FOG SUPPORTED APPLICATIONS

The Cisco Fog model can be observed in a comprehensive and integrative manner as an enabler of numerous advanced technologies. Fog computing have now been occupied to enhance the usability and potential of Cloud platform. With the beginning of such extensive applicability, the Fog and its similar platforms like Edge computing [8], Cloudlets and Micro-data centers are likely to attacks that can compromise Confidentiality, Integrity, and Availability (CIA) [9].

3.1 Advance persistent threats (APT)

The main objective of this attack is to compromise the company's infrastructure by the stealing the confidential data.

3.2 Access control issues (ACI)

The core objective of this attack is to compromise the security by unauthorized installation of software and by changing configuration.

3.3 Account hijacking (AH)

The core objective of this attack is to compromise the security of the user account through phishing techniques.

3.4 Denial of service (DoS)

The core objective of this attack is to shut down the server or any intermediate device by applying continuous pinging's.

3.5 System and application vulnerabilities (SAV)

This includes bugs which come from the use of malicious software's that attackers can use to compromise the system security.

4. CURRENT SECURITY SOLUTIONS

The security issues facing fog system is a newborn research area, and only limited solutions are available to sense and prevent malicious attacks on a Fog platform. The mentioned below are the few security solutions for fog computing.

4.1 Privacy preserving in fog computing

Stabilizing privacy in fog networks consists of the following precise steps to protect sensor data between Fog network and end user device: They gather sensor data and execute features; they Implement Public Key Infrastructure for encoding each data block; they transmit isolated data to Fog node, where data packets are decrypted and rearranged. The system also contains a feature reduction capability for reducing data communication with Fog nodes to help reduce risk [10].

4.2 Authentication in fog platform

Based on the existing state of authentication in Fog platform, Fog platforms are missing demanding authentication and protected communication protocols as per their design and requirements. In a Fog platform both security and performance factors are measured in conjunction and mechanisms such as the encryption practices known as fully homomorphic [11]. As homomorphic encryption allows normal procedures without decrypting the data, the reduction in key distribution will maintain the confidentiality of data.

5. SUGGESTED SECURITY MEASURES AND FUTURE CHALLENGES

While the deployment of this new technology we have to face a lot hurdles and problems. Some of them are discussed below:

5.1 Data encryption

5.1.1 Recommendation

The data need to be secured from the source to the destination while communicating among three proposed layers of Fog computing.

5.1.2 Future challenges

In order to control the greater resource distribution problems of encryption, only complex data should be encoded for example patient data in healthcare systems etc. The Advanced Encryption Standard Algorithm should be used to overcome this problem.

5.2 Avoiding cache attacks

5.2.1 Recommendation

The cryptographic key used in cache management system should not be exposed which will breach confidential information.

5.2.2 Future challenges

Fog system makes use of innovative cache techniques which leads to the disclosure of confidential data. To overcome this, a security solution should be included in the fog system.

5.3 Network monitoring

5.3.1 Recommendation

A licensed network management tool should be used in order to monitor the whole network by applying appropriate ACL policies.

5.3.2 Future challenges

As fog computing is going to handle data of billions of device so, it is a big challenge to handle this massive amount of data of different isolated devices.

5.4 Software updates and malware protection

5.4.1 Recommendation

The software's and prototype which the developer has embedded in the circuitry, to make sensors and controllers work accordingly should be updated on time when required [12].

5.4.2 Future challenges

If a patient health report is hacked by the hacker this would cause a great security breach and will cause many people to do suicide. This problem can be overcome by deploying cyber threat techniques in our network to avoid this type of security breach.

6. CONCLUSION

In this paper, I have given the brief description about the Fog Computing impact on internet of things, elaborate its complicated architecture, highlighted few feasible application and alert about the issues which we are going to face while deploying internet of things in to real environment. Moreover, I have suggested the proposed plan to how to get rid of those highlighted issues. While adopting all these techniques we can easily avail the benefits of internet of things. In Short, fog computing is the future of the cloud in the IOT world.

7. REFERENCES

[1] S.N.U.H. Shirazi, A Gouglidis, A. Farshad, and D.Hutchison, "Review and analysis of mobile edge computing and fog from a security and resilience perspective," IEEE Journal on Selected Areas in Communications, 2017.

[2] S .Kahvazadeh, V .B. Souza, X. Masip – Bruin ,E. Marn-Tordera, J.Garcia,and R .Diaz, "Securing combined fog-to-cloud system through sdn approach," in Proceedings of the 4th Workshop on Cross Cloud Infrastructures & Platforms.ACM,2017,p.2.

[3] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for internet of things services," IEEE Internet Computing, vol. 21, no. 2, pp. 16–24, 2017.

[4] A. Munir, P. Kansakar, and S. U. Khan, "Ifciot: integrated fog cloud iot architectural paradigm for future internet of things," arXiv preprint arXiv: 1701.08474, 2017.

[5] Z. Su, F. Biennier, Z. Lv, Y. Peng, H. Song, and J. Miao, "Toward architectural and protocol-level foundation for end-to-end trustworthiness in cloud/fog computing," IEEE Transactions on Big Data, 2017.

[6] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted internet of things," IEEE Cloud Computing, vol. 4, no. 1, pp. 34–42, 2017.

[7] Y.-Y. Shih, W.-H. Chung, A.-C. Pang, T.-C. Chiu, and H.-Y. Wei, "Enabling low-latency applications in fog-radio access networks," IEEE Network, vol. 31, no. 1, pp. 52–58, 2017.

[8] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," Computers & Security, 2017.

[9] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: Architecture, key technologies, applications and open issues," Journal of Network and Computer Applications, 2017.

[10] M. Oppitz and P. Tomsu, "Fog computing," in Inventing the Cloud Century. Springer, 2018, pp. 471–486.

[11] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," Journal of Cloud Computing, vol. 6, no. 1, p. 19, 2017.

[12] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," Journal of Cleaner Production, vol. 140, pp. 1454–1464, 2017.