Fog Computing: Security & Privacy Issues

Ramanpreet Kaur
Dept of Computer Science
GGN Khalsa College, Ludhiana ,Punjab

Abstract- *Fog computing is an emerging paradigm that extends the Cloud Computing to the edge of the network, thus enabling a new breed of applications and services. Similar to cloud computing but with distinct characteristics, fog computing faces new security and privacy challenges besides those inherited from cloud computing. This research paper deals with the threat to security issues, especially with location privacy and data confidentiality. The existing security and privacy measurements for cloud computing cannot be directly applied to the fog computing due to its features, such as mobility, heterogeneity, and large-scale geo-distribution. This paper provides an overview of existing security and privacy concerns, particularly for the fog computing. The way service providers as well as government can access users data is covered.*

Keywords- Fog, security, privacy ,cloud, edge

I. INTRODUCTION

The term "Fog Computing" was introduced by the Cisco Systems as new model to ease wireless data transfer to distributed devices in the Internet of Things (IoT) network paradigm [1],[2].Fog Computing can be described as a cloud-like platform provides services like data storage ,computation, processing, communication and application services, but fundamentally different from cloud because it follows decentralized approach. Fog computing reduces latency, provides location awareness, and supports high-density wireless networks. Fog systems are capable of processing large amount of data locally, operate on-premise, are fully portable, and can be installed on heterogeneous hardware. Fog infrastructure uses distributed computing environment that allows applications to run as close as possible to end user. In Fog computing, services can be hosted at end devices such as set-top-boxes or access points. These features make the Fog platform highly suitable for time and location-sensitive applications. However, Fog can be distinguished from Cloud by its proximity to the end users, the dense geographical distribution and its support for mobility [1]

II. LITERATURE REVIEW

If implemented as expected, fog will provide a number of non-trivial benefits and offer myriad opportunities for new applications (Zhu et al. 2013). Some defining characteristics of fog are edge location, awareness, and low latency. These features would support streaming video, gaming, distributed computing, monitoring, and control applications. Further, fog will be geographically distributed. This means that moving vehicles, robots, and autonomous systems will be able to receive high quality streaming content even as they pass between proxies and access points, because fog nodes will be positioned along roadways, highways, and cellular phone towers. Fog will also support large-scale sensor networks. These sensors may be dispersed in remote areas for environmental monitoring or they may be used for controlling industrial systems such as power grids, water treatment facilities, and factories (Hong et al. 2013). Fog will provide enhanced support for mobile devices. It is expected that fog applications will be optimized for direct communication with mobile devices. These applications will decouple host identity from geographic location. Further, fog will support near-real-time interaction. Instead of waiting for batch processing in a data center, fog nodes will provide compute services in close proximity to end devices. To sum, the addition of the fog platform provides location awareness, geographic distribution, and reduced lag.

III. NEED OF FOG COMPUTING

In the past few years, Cloud computing has provided many opportunities for enterprises by offering their customers a range of computing services. Current ‘pay-as-you-go’ Cloud computing model becomes an efficient alternative to owning and managing private data centers for customers facing Web applications and batch processing [6]. Cloud computing frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. However, this bliss becomes a problem for latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements [1].When techniques and devices of IoT are getting more involved in people’s life, current Cloud computing paradigm can hardly satisfy their requirements of mobility support, location awareness and low latency.

Fog computing is proposed to address the aforementioned problem [5]. As Fog computing is implemented at the edge of the network, it provides low

latency, location awareness and improves quality-of-services (QoS) for streaming and real time applications. Typical examples include industrial automation, transportation and networks of sensors and actuators. Moreover, this new infrastructure supports heterogeneity as Fog devices include end-user devices, access points, edge routers and switches. The Fog paradigm is well positioned for real time big data analytics, supports densely distributed data collection points and provides advantages in entertainment, advertising, personal computing and other applications.

IV. CHARACTERISTICS OF FOG COMPUTING

Fog Computing is a highly virtualized platform that provides compute, storage, and networking services between end devices and traditional Cloud Computing Data Centers, but not exclusively located at the edge of network. "Edge of the Network" implies a number of characteristics that make the Fog an extension of the Cloud.

- **Location awareness and low latency**: The origins of the Fog can be traced to early proposals to support endpoints with rich services at the edge of the network, including applications with low latency requirements (e.g. gaming, video streaming, augmented reality).
- **Wide Spread Geographical distribution**: In sharp contrast to the more centralized Cloud, the services and applications targeted by the Fog demand widely distributed deployments. The Fog, for instance, will play an active role in delivering high quality streaming to moving vehicles, through proxies and access points positioned along highways and tracks.
- **Large number of Nodes**: Fog environment includes very large number of nodes, due to wide spread geographical distribution.
- **Mobility:** It is essential for many Fog applications to communicate directly with mobile devices, and therefore support mobility techniques.
- **Support Real-time system interactions:** Fog applications involve real-time interactions rather than batch processing.
- **Heterogeneity:** Fog nodes support the feature of heterogeneity that allows different nodes with different factors to come and work together in an environment.
- **Interoperability:** Seamless support of certain services (streaming is a good example) requires the cooperation of different providers. Hence, Fog components must be able to interoperate, and services must be federated across domains.
- **Support for on-line analytic and interplay with the Cloud**. The Fog is positioned to play a significant role in the ingestion and processing of the data close to the source.

V. SECURITY & PRIVACY ISSUES IN FOG

According to above mentioned characteristics Fog is considered as one step ahead of cloud. However Fog computing still has some security and privacy issues that need immediate attention.

Authentication

Authentication of Fog nodes is one of the important security requirements in fog network. Fog network is a collection of various nodes which needs some authentication mechanism to differentiate between authorized and unauthorized node. It becomes a formidable challenge as the devices involved in the network are constrained in various ways including power, processing and storage. Traditional authentication mechanisms using certificates and Public-Key Infrastructure (PKI) are not suitable due to the resource constraints of IoT devices [7]. In essence, like storage and processing services, authentication also needs to be offered as a service whereby a device that needs them would have to get authenticated to the fog node with the help of the intermediary that may be the Certifying Authority (CA). This model of operations would prevent unauthorized nodes from becoming part of the fog network. In addition, this would also allow the fog nodes to restrict service requests from malicious/compromised nodes.

A. Data Issues

Security of data is the vulnerability in the cloud which affects the data and causes more insecurity for the information which has been stored in the servers. When the data is available in unauthorized hands, it makes more impact on the sensitive data. Data are more precious piece of fact. Any issues to the data can bring down the organization and cause huge effect and crisis in the company.

Data breach

Data breach is an important issue which comes under the category of protection of sensitive data from unauthorized users. Data breach leads to the concept of leakage of personal, private or sensitive data to the user who is not authorized and can misuse the information that can lead to a huge loss for the owner of information. The cloud providers are accountable to protect their consumer's data. Service

providers can use encryption mechanism and decoy techniques to authenticate the user. So that only the authorized user is allowed to access the information.

Data loss

Data loss is another threat in data threat category. Data loss is actually losing of the data due to data deletion, data corruption, and fault in the data storage or unavoidable causality. In 2013, around 44 percent of cloud service providers have attacked by brute force method which lead towards data loss and data leakage [15].In both cloud and the fog level to avoid the threat is we need to have data backup and data recovery technique.

B. Network Issues

With the use of cloud computing in business perspective, Internet becomes an important part in determining how effectively the communication of cloud works, with end users. Therefore, the cloud providers are responsible to handle various network security issues. When we are not providing enough security to the network it causes vulnerabilities and results internetwork issues. Most harmful network hazards in cloud computing are account hijacking, and denial of service attacks.

Account Hijacking

Account Hijacking is a network related problem for the cloud computing. Account Hijacking is the process where the attacker is trying to hack the account in order to steal the identity of the particular user. Multi-level authentication at different levels is the solution to avoid account hijacking. Identity management for the user should be very strong, Network monitoring [5], Data Leakage Prevention Technology [8] Vulnerability Detection Technology [8].

Denial of Service

(DoS) is an attack that denies the communication or the network resource for the particular user. There occurs delay in communications between the end user and cloud services. Intrusion Detection System (IDS) is the most popular method of guard against this type of attacks [8].Alternative method for securing cloud from DDOS incorporates utilizing intrusion detection system in VM. In this system when an IDS identifies as an unusual rise in inbound traffic, the targeted applications are moved to VMs hosted on alternative data servers.

C. Environmental Issues

Environmental issues are another important threat in security. Cloud providers are the controlling authority of various cloud data centers and for providing services to the end users. Excluding service provider problems, few issues are particular to cloud computing for example providing insecure interfaces and APIs to users, malicious cloud users, shared technology vulnerabilities, misuse of cloud services and insufficient due diligence

Insecure Interface and API'S

Cloud providers basically provide their APIs to third party to give services to customers. Weak APIs leading to the third party having opportunities to access security keys and sensitive information in cloud. With the security keys, the encrypted customer data in cloud can be read which results in, Loss of data Integrity, Confidentiality and Availability. Authentication mechanism and access control can avoid the problem in cloud level [4].In the fog layer we have to use the cryptographic hash function MAC MD5 HMAC.

Shared Environment Technology Vulnerabilities

In Cloud computing the communication is provided by sharing of infrastructure, platform and software. If number of users is sharing this infrastructure then there is a need to protect the data from other users as well so that their data cannot interfere with each other.

Insufficient Due diligence

When customers has lack of knowledge regarding security methodology, Auditing, Log details, and Data storage, Data access, which leads in generating unspecified threat profiles in cloud. In certain cases, the developers and designers of applications might not be aware of their effects from deployment on cloud that can result in operational and architectural issues [7].

Malicious insiders

This issue is also called as the insider's threat. It is the most common threat in the cloud environment. The main reason for this issue is the curiosity of the employee to know sensitive information about different consumers. The employees try to steal the consumer's information to misuse. The prevention for this problem could be providing different access control for the employees. This is well known way to overcome this issue [4].

Lack of knowledge of cloud services

Many of the cloud users might not have enough knowledge to use the cloud services. In such scenarios there is a possibility, the cloud users try to misuse the cloud services and violate the contract provided by the cloud providers. The cloud users need to know the basic knowledge to handle the cloud servicers in order to avoid the abuse of cloud services issues. The service level agreement must incorporate the important polices of the organization need to be followed by the consumers. The cloud computing is more popular; due to its vulnerabilities it has numerous issues. The issues need to be solved in order to provide secure platform for the users. It is really challenging to provide security for the cloud computing. There are fewer solutions are available for certain issues. The table below explains all the details regarding various issues and causes for the problems, available solutions in both the cloud and Fog computing. The threat column defines the top level issues and the cause column states the reasons for the problems. The cloud solution and fog solutions defines the various available solutions for the threats.

User Privacy

Privacy of user's sensitive and confidential data is a challenging issue in Fog environment. In Fog computing all nodes are placed near the end user as close as possible i.e all network devices lie in close proximity which gather the sensitive information of the user like identity, location of end user. As Fog infrastructure is based on decentralized approach, the Fog nodes are distributed in a large geographical area which is difficult to handle and manage. In addition, this type of network opens the doors for intruders very easily because of lack of control & authentication. The intruder once inside the network can steal user's privacy data that is exchanged among entities. Increased communication among the three layers that constitute the fog architecture can also lead to privacy leakage.

VI. CONCLUSION

The fog computing paradigm will support the next generation of applications and services. Enterprises with a competitive edge in cloud computing try to shift towards Fog. It is expected that implementation costs will be less for organizations that already possess the in-house talent required to support a cloud computing system. While cloud computing offered the advantage of cost savings, fog enables a new breed of applications. Once a new application or service achieves critical mass, it will be difficult to lure users onto other platforms. When considering a strategy which includes early adoption of this emerging capability, potential costs and benefits should be carefully weighed. The benefits of fog computing are: reduced response time, geographic proximity data, and support for the internet of things. It is expected that fog nodes will be owned and administered by a service provider, with organizations paying for the privilege to host their applications. The fog computing paradigm will likely see deployment over the next 3-5 years. This provides ample time for the development of a fog strategy for attaining competitive advantage. Although many of the implementation details surrounding fog have yet to be established, this research makes reasonable projections and assumes conservative security implications. The goal is to provide foundation for considering security before software is published and to throw light on some major weak areas of fog computing that needs to be identified and resolved for better deployment.

REFERENCES

[1] F.Bonomi, R.Milito, J.Zhu, and S.Addepalli, "Fog computing and its role in the Internet of Things," in ACM SIGCOMM Workshop on Mobile cloud Computing, Helsinki, Finland, 2012, pp. 13--16.

[2] J.K. Zao, T.T. Gan, C.K. You, C.E. Chung, Y.T. Wang, S.J.R. Mendez, T.Mullen, C.Yu, C.Kothe, C.T. Hsiao, S.L. Chu, C.K. Shieh, and T.P. Jung, "Pervasive brain monitoring and data sharing based on multi-tier distributed computing and linked data technology," Frontiers in Human Neuroscience, vol.8, no. 370, pp. 1--16, 2014.

[3] Dr. Jordan Shropshire"Extending the Cloud with Fog: Security Challenges & Opportunities"

[4] Ivan Stojmenovic, Sheng Wen, Xinyi Huang and Hao Luan "An overview of Fog computing and its security issues"

[5] Bonomi F. "Connected vehicles, the internet of things, and Fog computing". The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA, 2011; 13–15.

[6] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. "A view of cloud computing". Communications of the ACM 2010; 53(4):50–58.

[7] Mukherjee M ,Rakesh matam"Security and Privacy in Fog Computing: Challenges"

[8] Archana Lisbon A, Kavitha"A Study on Cloud and Fog Computing Security Issues and Solutions"

[9] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli "Fog Computing and Its Role in the Internet of Things