International Journal of Research in Advent Technology, Vol.7, No.6S, June 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Possible Solutions on Security and Privacy Issues in Fog Computing

Rashmi R, Dr R Ashok Kumar

Abstract—Fog computing isa new paradigm that'san add-on to cloud computing in the network. It has similar characteristics to cloud computing such as computation, storage, control, network functions. Fog is closer to end-users but different in that it is de-centralised architecture. This platform is suitable for real time low latency applications like Internet of Things (IOT) devices. This paper surveys the effect of security issues and privacy issues with possible solutions in fog systems.

Index Terms— Fog computing, cloud computing, Security threats, Privacy, Internet of Things

I. INTRODUCTION

The idea of Fog computing was first presented by CISCO in 2012. This platform refers to expanding cloud computing to the edge of an enterprise's network. Fog computing architecture is a scalable decentralized computing architecture different from cloud centralized architecture. Fog platform doesn't exist on its own, this acts an intermediate between end users and cloud platform to process the communication. The basic framework of fog platform is similar to cloud platform but its architecture supports sensitive low latency applications [1]. Fog platform uses many edge devices such as router, switches and hub for processing, analyzing, aggregating and transmitting data of latency aware applications that's why its named as fog computing [2].

Fog node can be any device that has the capacity of carrying out the computing, providing the storage, and does network connectivity. Fog system when compared to cloud system are relatively have small computing resources such as memory and storage but these resources can be enhanced on-demand.

With the fast growth of Internet of Things (IoT) requests, numerous challenges are faced by the cloud computing architecture such as high latency, low capacity, network failure and long distance (multiple hops) between cloud and end users. Fog computing has brought the cloud nearer to end user devices such as IoT Devices for addressing these challenges. It has offered processing of IoT information and storage close to IoT devices[3].

Manuscript revised May 13, 2019 and published on June 5, 2019
Rashmi R, Mtech *Student, Dept of Information Science & Engineering, BMS college of Engineering, Bangalore, India*
Dr R Ashok Kumar, *Associate Professor, Dept of Information Science & Engineering, BMS college of Engineering, Bangalore, India*

Different applications such as automation of home, monitoring of environment, traffic light that uses IOT devices are all connected physically. These applications generate huge data that are gathered. Features such as low latency, location awareness and geographic distribution are important for applications that are not supported by IOT. Fog computing and IOT are integrated together in-order to support these features[4].

Instead of sending information to cloud for analysis, storage and processing. Fog computing does all of these, this helps in improving the efficiency and decreases the amount of information that sent to cloud. Many companies such as CISCO, Dell, Microsoft Corp. have dedicated to explore and development of Fog. To enable scalability and interoperability feature, OpenFog Consortium workgroup are working to create an open architecture for Fog [5].

Fog platform has the following characteristics:

- Quick enough to respond to low latency applications.
- Can process large amount of data locally due to which performance increases.
- Services like storage, computation, memory are virtualized and are located at the edge of source premises.
- Supports Geographic distribution of Fog nodes.
- Software installation on Heterogeneous hardware.
- Support for Mobility and Location Awareness.
- Reduces Network Congestion.

Services provided by Fog are disrupted by malicious attack. These attacks can happen either internally or from external sources by consuming the resources. Thereby reducing bandwidth and interrupt the services provided by fog to genuine end users. In this paper we highlight security and privacy issues with possible solutions [6].

The paper is organized as follows: section II includes the connection among cloud and user devices, section III includes the literature survey, section IV includes the different types of attacks in fog platform, section V includes the security and privacy issues and finally section VI included the conclusion..

II. FOG ARCHITECTURE

Figure 1 depicts how communication happens between Cloud, Fog and End user devices. Fog platform lies nearer to end user devices rather than cloud. This is how fog nodes are linked to each other. Fog to Fog, Fog to cloud and Fog to End user devices are all communicating in bi-directional.

doi: 10.32622/ijrat.76S201913

- End user Devices / IOT devices – This consists of physical devices such as Mobiles, Sensors, actuators, tablets and others. These devices are provided with global positioning system [7].
- Fog Platform: This layer includes fog nodes and does computing via Gateways, Switches, Router and Access Points. Between fog nodes Storage and Computing facilities are shared [7].
- Cloud Platform: This platform includes Servers and Data Centers that has sufficient Storage and Computing resource[7]

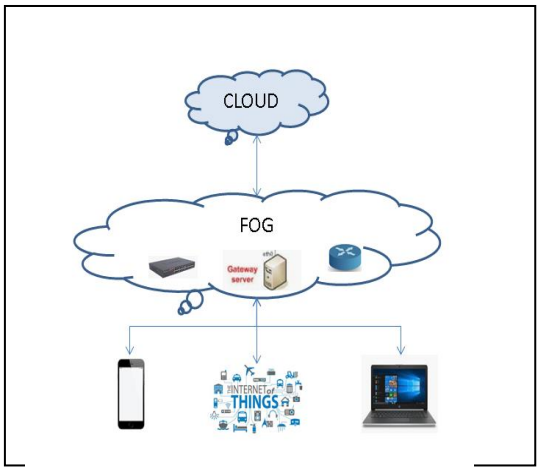

Figure 1: Fog Archiecture

This architecture is applicable to many applications such as smart cities, healthcare, transportation (smart cars and traffic control) , agriculture, hospital and financial services

III. Related Survey

A brief overview of different types of attacks are presented in [1]. Saad Khan, Simon Parkinson and Yongrui Qin author's have provided the security issues and possible solutions and recommendations for fog [2].Integration of IOT with Fog is explained in[3]. VM's can be attacked so a Conceptual smart pre-copy live migration method is proposed for VM's in [6] to choose when to advance with stop and copy stage. Open challenges and ongoing research in security and privacy issues are highlighted by author's in[5][7]. In order to support location privacy a secure positioning protocol was proposed in [8]. The authors in paper[9] have highlighted why data protection techniques of cloud cannot be directly applied to Fog.

IV. Security Threats In Fog

- . Access control issues: Unauthorized user gets the permission to acquire the data, change configuration and install software.
- Account Hijacking: In order to carry out malicious activity hijacking the user account. Phishing attack is used to steal user data.
- Denial of service (DOS): Prevents the genuine users from accessing the services or data.
- Eavesdropping: attackers tries to steal information from systems when transmitted over network.
- Forgery: Attackers imitate user's identity.
- Side channel attack: kind of hidden channel already exists in hardware through which attacker can access.
- VM based attack: a kind of malicious attack through servers, users could experience system failure.
- Impersonation attack: an attacker acts identical to reliable server. They provide services that are offensive to users by making the users to believe they are connecting to genuine fog nodes[3].
- Man-in-the-middle attack: an attacker establishes an momentary situation between the interactive nodes. Data is altered without revealing to the users while they are communicating the data with fog nodes[1].
- Data Tampering: Data is modified or deleted by unauthorized channels.
- Stealth attack: Attackers hide malware command over the network and control the fog services.
- Tampering Attack: Attacker can modify or drop or can delay the data that is being transmitted thereby degrading performance and efficiency [7].
- Spoofing: Attackers gains the access to system indicating that messages are sent from trusted host.
- Resonance attack: Improper data is transmitted to fog node by compulsory making the sensors to operate at diverse frequencies.
- Sniffing attack: Stealing of end users devices data when transmitted over the network.

V. Security And Privacy Issues

The following gives an understanding about the attacks, possible solution and impact on the features of Fog.

Authentication and Authorization

This is first step in establishing relation between End user devices/ IOT Devices and Fog nodes. Authorization identifies as "officially having accessing right" were as Authentication is "Action of proving". During the establishment phase access right and identity of the node which wants to connect is verified. For accessing storage and processing services, end users should get authentic to the Fog node. Traditional Public Key Infrastructure (PKI) along with certificates is not appropriate due to resource limitations of IOT devices [7].

Possible Threats:

- Man- in-the -middle attack
- Forgery attack
- Data Tampering
- Spoofing attack
- Stealth attack
- Access control issues

Impact:
Trusted end user data might get hacked by the attacker during communication and these devices might not get the required services.

Possible Solution:

doi: 10.32622/ijrat.76S201913

- Multicast authentication using Public-Key Infrastructure (PKI) [7]
- Diffie Hellman key exchange
- Intrusion Detection techniques
- Biometric-authentication-techniques:
  - Face-authentication, Finger-print authentication, Touch-based authentication.
- Certifying Authority (CA) [7]
- Fully homomorphism can be used to secure data

Virtualization

Virtualization can be hardware virtualization or software virtualization. Hardware virtualization refers to a virtual fog that allows Virtual Machines (VMs) to co-occur in a physical server (host) so that multiple entities to share the same physicalsystem. Software virtualization refers to multiple operating system images run at a same time on a piece of hardware. We can have virtual version of storage, network, data, memory and software virtualization, with the help of this delay and jitter can be decreased. Malicious VM's can take control over hardware and operating system and modify the services in fog without security.

Possible Threats:
- Denial of service (DOS) attacks,
- VM based attack
- Side channel attack
- Impersonation attack

Impact:
Failure of hosted server's result in absence of services provided by them and resources [4]**.**

Possible Solutions:
- Multi-Factor Authentication [2]
- Intrusion Detection system [2]
- Role-based access control model
- Attribute based encryption [2]
- User-based permission model [2]

Data Security

Data security is an important aspect in fog system. Data should be secured in fog system from unauthorized access. While data is getting processed in fog, it will undergo changes in its size, structure and validity of data. Fog nodes managed by different providers and individuals needs to be checked for trustworthiness.

Possible Threats:
- Denial of service (DOS) attack
- Data ownership issue
- Illegal data access
- Data altering and erasing attack
- Data replication and sharing [2]

Impact:
Corruption, deletion of data present in database system of fog nodes. Downtime caused to the trusted fog nodes.

Possible Solution:
- Encryption of sensitive data at end user devices then transfers it to fog nodes.
- Secure key management
- Data Masking
- Network Monitoring
- Policy enforcement

Wireless Network Security

Network acts as a bridge between fog nodes and end user devices and correspondingly between the fog nodes. Network should be secure from malicious attack, if that happens then it can spread malicious threats to connected parties and also damages the working of that network itself. Properly isolating the network can prevent the network from spreading if infected.

Possible Threats:
- Packet sniffing
- Denial-of-Service (DoS) attack,
- Man in the middle attack
- Resonance attack
- Gateway attacks were recognized as likely attacks on network infrastructure

Impact:
Wireless access points that are susceptible can compromise features such as privacy, accuracy, consistency, availability and reliability of data. Performance of the fog nodes are decreased by consuming the network resources such as bandwidth.

Possible Solution:
- Antivirus [2]
- Encryption and authentication [2]
- Deployment of intrusion detection system (IDS) [6]
- Cloud watcher – for network monitoring [2]
- Virtual Private Network (VPN) – Isolating the network from external attack [2]

Secure Communication

Secure Communication can be of three kinds between end user devices, Fog nodes and cloud.
- Communication between end user devices and Fog nodes.
- Communication within Fog nodes.
- Communication between fog nodes and cloud[10].

Possible Threats:
- Tampering attack
- Spamming attack

Impact:
Many bogus messages or wrong information can float around the network [2].

Possible Solution:

doi: 10.32622/ijrat.76S201913

- Homomorphic encryption techniques – Maintain data secrecy and protect identities of devices once uploading info from devices to cloud.
- Lightweight encryption or masking algorithms can also be used to protect the data secrecy.

Trust

All Devices in fog network should have certain level of trust on one node to one more node. Trust play mutual role in fog network for end user devices.

- End user devices should trust Fog nodes that they connect are genuine.
- End user devices that send data to fog nodes are indeed secure[5].

Possible Threats:

- Malicious attacks.

Impact:
Attacks causes sensors to be untrustworthy to avoid this trust evaluation method to provide reliable connection among sensors to fight against malicious attack

Possible Solution:

- Regionbased trust model – It's a trust communication amongst fog nodes at different region[5].
- Dynamic nature of end user devices and fog nodes uses opinion-based model[4].

Privacy

Preservation of privacy data is extra challenging as fog nodes are nearer with end users for collecting the sensitive information. Sensitive data are not retrieved or revealed to an illegal person is ensured by privacy [6].Fog systems must let users to specify the privacy attributes of the data that they own on the system [8]. Privacy can be distinguished in terms of End user privacy, Location privacy and Usage privacy.

Possible Threats:

- Eavesdropping or Sniffing attack
- Man-in-the-middle attack

Impact:
Sensitive data or personal information of end user can be hacked. In case of location privacy attackers may provide fake locations, so locations specified by one entity might not reliable.

Possible Solution:

- Public key infrastructure for encrypting the data block at end-user devices and decrypting that at fog nodes.
- Location verification protocols are used to support location property
- Host Firewall with Network Location Awareness[11]

Position based cryptography[8]

VI. CONCLUSION

Fog is a computing paradigm present at the edge of network to support end users. Cloud computing security features cannot be functional to fog computing because of its distinctive characteristics. This paper summarizes attacks, possible solutions on security and privacy issues in Fog computing. The major concerns in context to fog computing are considered in this paper.

.

REFERENCES

[1] A. Aljumah and T. A. Ahanger, "Fog computing and security issues: A review," *2018 7th Int. Conf. Comput. Commun. Control. ICCCC 2018 - Proc.*, no. Icccc, pp. 237–239, 2018.
[2] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, 2017.
[3] H. F. Atlam, "Fog Computing and the Internet of Things : A Review," pp. 1–18, 2018.
[4] "Fog-IOT." [Online]. Available: https://internetofthingsagenda.techtarget.com/ definition /fog-computing-fogging . [Accessed: 06-Mar-2019].
[5] P. Y. Zhang, M. C. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," *Futur. Gener. Comput. Syst.*, vol. 88, pp. 16–27, 2018.
[6] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. K. R. Choo, and M. Dlodlo, "From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework," *IEEE Access*, vol. 5, no. c, pp. 8284–8300, 2017.
[7] M. Mukherjee *et al.*, "Security and Privacy in Fog Computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.
[8] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for Fog Computing," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 799–806, 2018.
[9] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data Security and Privacy in Fog Computing," *IEEE Netw.*, vol. 32, no. 5, pp. 106–111, 2018.
[10] "Open Fog Consortium." [Online]. Available: https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf. [Accessed: 20-Mar-2019].
[11] "ScienceDirect."[Online].Available:https://www.sciencedirect.com/topics/computer-science/location-awareness. [Accessed: 10-Mar-2019].

.

doi: 10.32622/ijrat.76S201913