Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3502 - 3507
Received 15 April 2021; Accepted 05 May 2021.

An Audit of Fog Computing: Security, Challenges and its Solutions

A.SenthilAnandhi,

Assistant Professor,Karpagam College of Engineering,Coimbatore.

senthilanandhi1@gmail.com

ABSTRACT:

All most all the items in this world is related with the data without the data it is very tedious to perform any task. fog computing concentrates on decentralizing the data centric clouds and making it localized, fog computing uses the information which is mostly used and so that the size is minimum when compared to cloud computing, when any other data is needed, the information can be taken from cloud, fog acts like a connection hubfor user with cloud server. Edge computing and fog computing are similar but edge saves the monetary and time by streamlining the communication, reduces the failures in IOT application. This paper discusses the various taxonomiesrelated to fog computing and how they are processed, security threats, challenges and possible solutions and technologies used to solve in fog computing.

Keywords:
Fog computing - security - privacy issue-threats-solutions - challenges

1. INTRODUCTION:

When the computing is considered, storage of data has become very vast, for storing the huge volume of data requires switching the storage into the cloud computing. The fog computing is used for reducing the data fetchingtime while using the cloud computing. In fog computing, the copies of frequently used data reduce the access time. Fog computing layer makes the end nodes to closer with the computation, networks and devices which are used in IoT. Fog computing reduces the latency of the services.

Fog computing performs the collection, analyzing and processing of data in the cloud computing network with reduced data communication between user and thecloud. It further decreases the network latency and thereby improves the response time in most applications.

2. OVERVIEW OF FOGCOMPUTING:

CISCO introduced fog computing by extending the traditional cloud computing network with low latency. It allows multiple devices to connect to network at a time. Fogtechnology reduces data transmission to the cloud and thereby improves efficiency.

2.1 Fog node

Fog node is a physical devicewhereas fog computing is deployed.

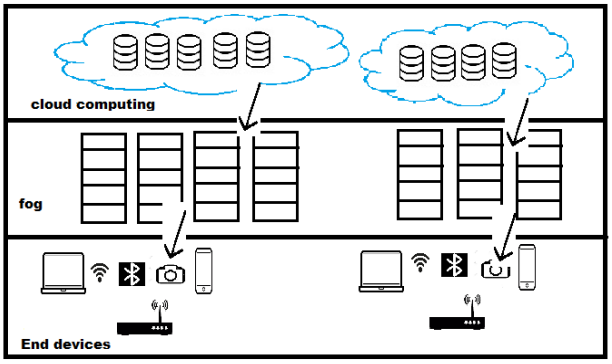
2.2. Characteristics of FOG COMPUTING:

- It is wide spread and it is available everywhere, the node can able to cope with all the mobile

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3502 - 3507
Received 15 April 2021; Accepted 05 May 2021.

devices and it can able to redirect to the nearest applications.

- Fog nodes can able to translate from IP to non-IP transport.
- Fog nodes are low and enable latency in predictable
- It can run on distributed part of cloud computing, and accessed by devices in wireless network
- It is located in cloud data centers near to the edge.



3. SECURITY CHALLENGES AND PRIVACY:

Fog computing stores the data at the edges for processing, so the fog server leads to incur the cost in maintenance and management. While privacy is concerned, fog uses the wireless network thus it may lead to chance of data leakage.

To overcome the problems in the fog computing new software is implemented to interact with the various hardware platforms as it is interacting in larger distributed networks [1]. Security solution for the cloud computing may not be suitable for the cloud computing as the fog works on widerlevel.The following are the various criteria to beconsidered:

1.Authentication:

Traditional PKI cannot be more efficient so the NFC can be used in fog.to overcome the major issue authentication techniques like facial recognition, finger print etc. can be used, but it takes larger time constraints.

2.Intrusion detection:

Intrusion detection can be achieved by signature based methods to observe the patterns and to check the already existing database.

3.Password based security:

- Low entropy
- Inadequate to keep password with all servers
- it is weak due to attack in offline attacks.

4.Stealth test:

ManInMiddle attack will consume some amount of resources in fog computing. To realize the MIM attack, the malicious code is implemented in the compromised system and comprising the gateway.[5].

5.Rogue Gateway:

Even user owned devices can be hacked by the malicious adversaries and deploy the entire systems.

6.Privacy Leakage:

Both adversaries the flow of information that traverse the edge data centers.

Privacy is subdivided as follows

data privacy, Location privacy and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3502 - 3507
Received 15 April 2021; Accepted 05 May 2021.

identityprivacy[21]

7.Privilege escalation:

External adversariescan take control of various services from the data centers.

8.Virtualization Infrastructure:

- **Misuse of resources** will target the local or remote entities other than the edge data centers where it is hosted.
- **Injection of information** the devices controlled by an adversary can be reprogrammed and gives the false information when it is queried.
- **Trust management**deals with how many partners is going to behave, the data maynot becorrect or service latency might be low.[7]

9. Control Centre:

The IoT devices will receive the data through the fog devices and it is processed according to the application to the application in control center.

Trusted authority: third party will bootstrap the system key materials and assigns the key for all the IoTdevices, fog and control center. [10]

10.Data Protection:

Region in data protection refers to junction where the collection of fog nodes and fog devices are grouped together. When a region receives the request to perform trusted connection to a newer region, it verifies and analyzes the request for getting the destination. Once both the address accepts then the trusted relationship is obtained.

Join/leave a region:

When the devices is used it has to be switched from one devices to another fog devices. While switching betweenfogoccurs, the node receives the request and accordingly it verify and analyze the identity. Further, the region LRD corresponding to leaving and joining regions are updated [22].

As the fog computing performs major features of cloud computing it inherits the high risks in collusion, impersonation. Collusion is one or more group join and trying to treat it as a genuine and attack IoTnodes. Impersonation refers to creating a impression of genuine server by network attacker. [21]

4. SOLUTIONS TO SECURITY PROBLEMS:

There are some possible solutions to overcome the problems which are occurred in the fog computing almost higher level of risks are reduced, but still there is a problem in wireless

The major problems occur in the following areas in fog computing: objectlayer, fog server and middle ware.

1.Object layer:

Object layer is used for sensing the data from physical data due to abundant of data from newly connected devices. Threats in object layer include Node capture, Spoofing attack, Signal jamming, Malicious data, Denial of services, Node outage, Replay attack and Sybil attack

Possible remediesto object layer:

The above problems can be solvedby performingauthorization, cryptographyand spectrum communication with correctjamming report, error correction and detection codes

2.Fog server:

As the fog server has to perform different tasks based on application. There are many protocols in this process including Message Queuing, telemetrytransport, constraint application protocol, extensible messaging and presence protocol and etc.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3502 - 3507
Received 15 April 2021; Accepted 05 May 2021.

Threats in Fog server:

- Sniffer/logger
- Phishing attack
- Injection
- Session hijacking
- Distributed Dos
- Node identification
- Information privacy
- Application specific vulnerability
- Social engineering

Possible remedies to Fog server:

- Safe program testing
- Antivirus software
- Cache development
- Boundary inspection and data encryption
- Risk assessment

3.Middle Ware:

Storage and processing will be performed in middle ware. In this layer there will be integrity, confidentiality, and availability issue

Threats in Middle Ware:

- Selective forwarding
- Sybil attack
- Black hole
- Worm hole
- Hello flood
- Acknowledge flooding
- Heterogeneity
- Scalability
- Data disclosure

Possible remedies to Middle Ware:

- Periodic password changing
- Firewall
- TLS/SSl Protocol
- Packet Authentication
- Link layer encryption
- IPSec Protocol
- Authentication /broadcasting
- Multipath Routing
- Password Management

The above mentioned are the major issues while handling the fog computing, although there are some possible solution's due to high volume to data is used there might not be full control over the data.[20]

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3502 - 3507
Received 15 April 2021; Accepted 05 May 2021.

5. FOG COMPUTING CHALLENGES:

- The fogdevices are connected and used globally, there is a chance of malicious data and risks added in it, keep track of huge volume of data is the biggest challenge.
- The security of sensing layer is limited.
- There is no acknowledge message for key models in IEEE 802.15.4 standards.
- Analog to digital converters are limited in lower range hardware.[20].
- Smart antenna helps in reducing the risk and sand boxing can protect the privacy in cloud .as it is wireless network, schedulingare performed based on fault tolerance and which may some time lead to failures. [16,19]

In addition to above mentioned there are few more challenges in fog computing they are:

- Cyber crime
- Secure CoAP
- Cross layer security
- Confidentiality
- 6LoWPAN

6.CONCLUSIONS:

Fog computing isthe new models for service providers and users, this model is to be used in a proper way for overcoming the security issues. As edge computing is upcoming version it provides the way for the distributed computing. The paper discussed the security issues, possible solutions and upcoming challenges. As the fog computing minimizes the time of the users and also improves the security, New protocols are to implemented because novel protocols automatic detection is not fully satisfied. The issues are to be overcome by proper method implementation for low latency.

7.REFERENCES:

1. Chiang M et al. “Clarifying fog computing and networking: 10 questions and answers. IEEE Commun Mag. 2017;55(4):18-20.

2.Shi, Heng, Nan Chen, and Ralph Deters. “Combining mobile and fog computing: using coap to link mobile device clouds with fog computing.”2015 IEEE International Conference on Data Science and Data Intensive Systems (DSDIS). Sydney, NSW, Australia: IEEE, 2015.

3.Yi S, Qin Z, Li Q. Security and privacy issues of fog computing: a survey. International Conference on Wireless Algorithms,Systems, and Applications. Cham, Switzerland: Springer; 2015.

4.Ionita M-G, Patriciu V-V. Secure threat information exchange across the internet of things for cyber defense in a fog computing environment. InfEcon. 2016;20(3):16-27.

5. Ibrahim MH. Octopus: an edge-fog mutual authentication scheme. IJ Network Sec. 2016;18(6):1089-1101.

6.Vishwanath A, Peruri R, He J(S). Security in Fog Computing Through Encryption. Int J InfTechnolComput Sci. 2016;5:28–36.

7.Roman, Rodrigo, Javier Lopez, and Masahiro Mambo. “Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges.” FuturGenerComputSyst 782018): 680–698.

8.Luan, Tom H., et al. “Fog computing: Focusing on mobile users at the edge.” arXiv preprint arXiv:150201815. (2015);6:1–11.
9.Salman, Ola, et al. “Edge computing enabling the Internet of Things.” 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). Milan, Italy:IEEE, 2015.
10.Lu R, Heung K, Lashkari AH, Ghorbani AA. A lightweight privacy preserving data aggregation scheme for fog computing enhanced IoT. IEEE Access. 2017;5:33023312.
11. Slabicki, Mariusz, and Krzysztof Grochla. “Performance evaluation of CoAP, SNMP and NETCONF protocols in fog computing architecture.”2016 IEEE/IFIP Network Operations and Management Symposium (NOMS). Istanbul, Turkey: IEEE, 2016.
12. Stojmenovic I, Wen S. The fog computing paradigm: scenarios and security issues. 2014 Federated Conference on Computer Science and Information Systems (FedCSIS). Warsaw, Poland: IEEE; 2014.
13.Zhang P, Zhou M, Fortino G. Security and trust issues in fog computing: a survey. FuturGenerComput Syst. 2018;88:1627.
14.Kumar, Praveen, Nabeel Zaidi, and Tanupriya Choudhury. “Fog computing: Common security issues and proposed countermeasures.”International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India: IEEE, 2016.
15. Lee, Kanghyo, et al. “On security and privacy issues of fog computing supported internet of things environment.” 2015 6th International Conference on the Network of the Future (NOF).
Montreal, QC, Canada: IEEE, 2015.
16. Hao Z et al. “Challenges and software architecture for fog computing. IEEE Internet Comput. 2017;21(2):44-53.
17.Khalid T, Khan AN, Ali M, Adeel A, urRehman Khan A, Shuja J. A fog based security framework for intelligent traffic light control system. Multimedia Tools and Applications, December 14. 2018;78:2459524615.
18.Mukherjee M, Matam R, Shu L, et al. Security and privacy in fog computing: challenges. IEEE Access. 2017;5:1929319304.
19.Liu Y, Fieldsend JE, Min G. A framework of fog computing: architecture, challenges, and optimization. IEEE Access. 2017;5:2544525454.
20. D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, “Secure and sustainable load balancing of edge data centers in fog computing,” IEEE Commun. Mag., vol. 56, no. 5, pp. 60–65, 2018.
21. Aljumah, A., &Ahanger, T. A. (2018). Fog computing and security issues: A review. 2018 7th International Conference on Computers Communications and Control (ICCCC).
22. Dang, T. D., & Hoang, D. (2017). A data protection model for fog computing. 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC). doi:10.1109/fmec.2017.7946404