IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13305

A Survey of FOG Computing

E.P. Priyadharshini[1], S. Jothipriya[2]

PG Student, Department of Computer Science, R.B. Gothi Jain College for Women, Chennai-600057, India.[1,2]

Abstract: Fog is a layer between the cloud and end users and it extends the services provided by the cloud computing to the network edge. Fog computing follows the distributed network architecture and closely associated with IOT (Internet of Things). Security is the main challenge in the fog due to the password compromise. To overcome the password compromise additional authentication credentials are needed to login. Round Trip Latency (RTL) based scheme increases the protection of traditional password authentication between clients and authenticators and extra profiling features are needed to defense against password compromise. In this paper, extended latency based authentication is proposed that includes the keystroke dynamics along with the latency to effectively protect from the same location attacks

Keywords: Fog, Cloud, Keystroke, authentication, RTL.

I. INTRODUCTION

The massive increase of connected devices in the cloud gives the new idea of computing known as Fog Computing. It has the characteristics like cloud in terms of storage, networking, computation etc. In addition Fog supports location awareness, mobility and sensitive services. Fog computing which is developed by CISCO that made the IOT as popular one and that incorporates the real life applications such as vehicles, buildings and smart grids. With the increased processing, efficiency and capacity of networks in fog computing should necessary to check the issues like security, privacy, authentication and resource management. Fog computing is an extended version of cloud computing and it has unique security concerns. This article focuses on the security concerns of fog computing and will propose the possible solution to this issues.

II. FOG ARCHITECTURE

Fog has the three tier architecture and it employs the intermediate between cloud networks. The first tier includes the real life devices such as cameras, buildings, vehicles and homes etc. Second tire includes the storage, computation, processing and handle the latency requests at the spot and responds to the end nodes. The top most layer consist core devices like data centers and it is connected to second tier servers by using broadband technologies

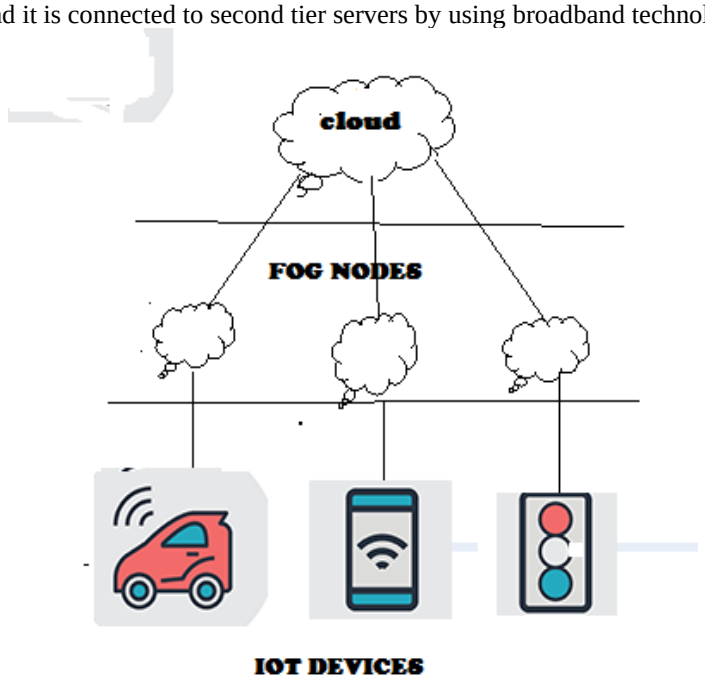

Fig 1: Fog Architecture

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024
DOI: 10.17148/IJARCCE.2024.13305

III. CHARACTERISTICS

3.1. Decentralization and Geographical Distribution

In fog, nodes are deployed in several places and geographically distributed, its architecture is decentralized. To manage the services and computing resources there is no central servers. , fog nodes are collaborate and self-organizing to provide end users with real-time IoT applications.

3.2. Real Time Interaction

Fog computing supports real-time interaction rather than batch processing. Real-time processing includes gaming, real-time stream processing and augment reality etc.

3.3. Save Storage Space

To avoid the storage of improper and unrelated data to the whole network, fog computing is the best solution and it saves the storage space and also decrease the latency.

3.4. Mobility support

It is the main application of fog computing which is directly communicated with the mobile devices through the use of protocols.

3.5. Close to end user

To avoid the delay in data transmission fog allows data to be closer to user than in remote data centers.

IV. SECURITY IN FOG

Security mechanisms must handle all the security issues. There are so many proposed techniques have been introduced to tackle the new threats. . Existing Security mechanisms are authorization and authentication, access control, IDS, virtualization, fault tolerance and recovery etc.

4.1. Authentication and Authorization:

The initial step of security in fog computing is to identify each node whether it is authenticated node or not. In FC authorization and authentication are important because authorization identifies the legitimate users and authentication allows who can do what. Fog consists billions of devices connected to the network and every node identified to ensure the security and to define the privileges to every node. So it is very important to authorize and authentiacate the nodes to protect from the security issues.

4.2. Access Control Mechanism

It allows the different nodes in fog to get different authorization. If there is no authorization mechanism then any users can enter into the fog network and can access the resources. If any user wants to access any resources in fog some policies should be needed to control the data and services. So access control mechanism should be needed to ensure the authorization.

4.3 Intrusion Detection System

It prevents from illegal access and generates alerts when unauthorized intrusions occur. In fog so many attacks are there like flooding attack ,internal attack etc. Intrusion detection system employs to protect from this type of attacks.IDS recognize sniffing activities and verifying access control mechanisms, log files and login information to prevent from malicious attacks.

4.4 Privacy

It is an another aspect of security mechanism. Fog users can share their information to whom they want. privacy of data and location of users are efficiently handled by fog computing and ensures the system to be reliable and secure.

4.5 Data Protection

Due to the vast information processing the number of IOT devices increases. When the IOT devises senses data , it shares the data with the nearby fog nodes. It is difficult to handle large amount of data in IOT devices, so the data is divided and forwarded to multiple fog nodes for processing. The light-weight encryption and decryption techniques are supported by fog for the data protection.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13305

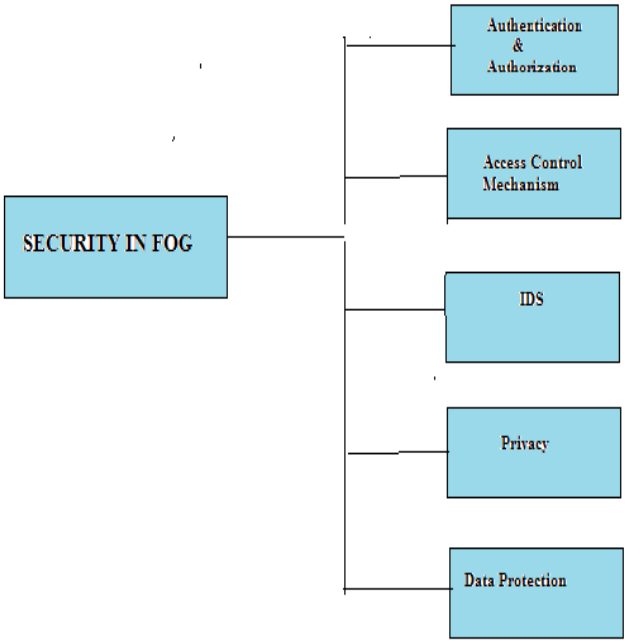

Fig 2: Security mechanisms in Fog

V. AUTHENTICATION SCHEME IN FOG

Authentication is an important issue for the security of Fog computing since services are offered to massive-scale end users by front Fog nodes/servers.

a) Traditional PKI-based authentication [3] is not efficient and has poor scalability for Fog users at the Edge of the network.

b) Biometric authentication [4] in mobile computing and Cloud computing, such as fingerprint authentication, face authentication, touch-based or keystroke-based authentication. However, such techniques take relatively long execution time and their security level is always constrained by time complexity, especially when high security level is needed.

c) Intrusion detection techniques can also be applied in Fog computing [5]. Intrusion in smart grids can be detected using either a signature-based method in which the patterns of behavior are observed and checked against an already existing database of possible misbehaviors. Intrusion can also be captured by using an anomaly-based method in which an observed behavior is compared with expected behavior to check if there is a deviation. The work in [6] develops an algorithm that monitors power flow results and detects anomalies in the input values that could have been modified by attacks. The algorithm detects intrusion by using principal component analysis to separate power flow variability into regular and irregular subspaces.

d) Password-based authentication techniques [7]have many applications in the Cloud, however, they are not a good idea when it comes to Fog computing due to several reasons: (i) Passwords are characterized by their low entropy, and in order to amplify this entropy to establish session keys, extensive modular arithmetic computations are needed. (ii) Fog users at the Edge of the network communicate with many Fog servers in different Fogs. It is inadequate to keep a password with each server. Moreover, it is not a good idea to keep one common password for all servers.

VI. CONCLUSION

This article discussed the various security aspects and its demerits in fog computing. Though there are so many security mechanisms are in fog there is some need in security. So many researches are also done related to authentication, IDS, Privacy, Virtualization etc and the proposed system implemented the authentication of users are done through the Round Trip Latency based scheme. Users profiles are created based on the location and keystroke dynamics also included as additional credentials to authenticate in fog computing.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13305

REFERENCES

[1]. 1. Bushra Zaheer Abbasi, Munam Ali Shah (2017), "Fog Computing: Security Issues, Solutions and Robust Practices", Researchgate.

[2]. 2. Gohar Rahman and Chuah Chai Wen (2018), "Fog Computing, Applications, Security and Challenges, Review", International journal of Engineering & Technology.

[3]. 3. F. M. Salem, M. H. Ibrahim and I. I. Ibrahim,Non-interactive secure and privacy preserving protocol for inter-vehicle communication networks, inIEEE Seventh International Conference on Information Technology: New Generations, pp. 108-113,2010.

[4]. 4. S. Bouzefrane, B. Mostefa, F. Amira, F. Houacine and H. Cagnon, Cloudlets authentication in NFC based mobile computing, in 2nd IEEE InternationalConference on Mobile Cloud Computing, Services,and Engineering, pp. 267{272, 2014.

[5]. 5.C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Pateland M. Rajarajan, A survey of intrusion detectiontechniques in cloud, Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42-57, 2013.

[6]. 6.J. Valenzuela, J. Wang and N. Bissinger, Real-timeintrusion detection in power system operations,"IEEE Transactions on Power Systems, vol. 28, no. 2,pp. 1052-1062, 2013.

[7]. 7.C. C. Lee, C. H. Liu and M. S. Hwang, Guessingattacks on strong-password authentication protocol,"International Journal of Network Security, vol. 15,no. 1, pp. 64-67, 2013.

[8]. Chen, L., Tokuda, N., and Nagai, A. A new differential LSI space-based probabilistic document classifier. Information Processing Letters, 88(5):203–212, 2003

[9]. Díaz, I., Ranilla, J., Montañes, E., Fernández, J., and Combarro, E. Improving performance of text categorization by combining filtering and support vector machines. Journal of the American Society for Information Science and Technology (JASIST), 55(7):579âˇA ¸S–592, May 2004

[10]. Drucker, H., Wu, D., and Vapnik, V. Support vector machines for spam categorization. IEEE Transactions on Neural Networks, 10(5):1048–1054, 1999.

[11]. Deng, Z.-H., Tang, S., Yang, D., Zhang, M., Li, L.-Y., and Xie, K.-Q. A comparative study on feature weight in text categorization. In Proc. of the Advanced Web Technologies and Applications, 6th Asia-Pacific Web Conference, APWeb 2004, pages 588–597, Hangzhou, China, Apr. 14–17, 2004. Springer-Verlag New York, Inc.

[12]. Napoleon D. and Praneesh M. "Detection of Brain Tumor using Kernel Induced Possiblistic C-Means Clustering", volume no.3, issue no.9, pp 436-438, 2013

