Nat. Volatiles & Essent. Oils, 2021; 8(4): 14497-14505

NVEO
Natural Volatiles &
Essential Oils

Data Security In Fog Computing Using Biometric Crypto system

P. Arul [1] and N. Shanmugapriya [2]

[1]Research Supervisor, Assistant Professor, Department of Computer Science, Government Arts College (Affiliated to Bharathidasan University, Trichy-24), Tiruchirappalli-620022, Tamil Nadu, India.

[2] Assistant Professor, Department of Computer Science, Government Arts College
(Affiliated to Bharathidasan University, Trichy-24), Tiruchirappalli-620022, Trichy, Tamil Nadu, India.

ABSTRACT–In spite of the wide utilization of cloud computing,some applications and services still cannot benefit from this popular computing model due to innately problems of cloud computing such as undesirable latency,lack of mobility support and location awareness.As a result, FogComputing is currently entice many researchers as it brings cloud services closer to the end users. The Internet of Things (IOT),current digitized intelligent connectivity domain, demands realtime response in many applications and services. This furnishFog Computing a suitable platform for achieving goals ofautonomy and efficiency. Fog computing is still emit paradigm that demands further research.Among all the other issues customary in fog computing,security is the one of the blazing issues. The fog, existence closer to the end user, is more vulnerable than the cloud. The Biometric cryptography key is used to secure the scrambled data in the fog environment. The Biometric cryptography technique uses fingerprint, voice or iris as a key factor to secure the data encryption and decryption in the cloud server. Advanced biometrics are used to safeguard sensitive documents and valuables. A more instantaneous problem is that databases of personal information are targets for hackers. Biometric technology offers very constrain solutions for security. In the face of risks, the systems are convenient and hard to duplicate. Additionally, these systems will continue to develop for a very long time into the future.

Index Terms - Fog Computing, Cloud Computing,Biometric, Internet of Things.

INTRODUCTION

The term “fog” arrived from the meteorological sector which brings the cloud near to the earth. Like this, Fognodes bring down the resources of cloud computing to the edge nodes. This term “fog” is connected with the Ciscocompany, and the term was framed by the Company’s manager, Ginny Nichols and listed as “Cisco Fog Computing”and it is called by the common people as Fog computing.A Fog Computing framework is distributed over the network with a variety of the different number of devices. These devices universally attached at the terminal of the network to provide adaptable communication, storage services, collaboratively variable and computation. Fog Computing gives many advantages in different areas such as real time, low latency, high response time, and especially healthcare applications. It is somewhere in-between the cloud data centers and user devices located at the ground (or at the base level).The topologies of FC are the main characteristics which differentiate it from the other technologies. In Fog Computing,the nodes are geographically distributed,perform computations, and provide better storage space and better network services[1]. However, due to high latency and privacy gap in CC, FC came into the pictureto solve these health-related issues.

Fog computing provides all the provisions to the end-users to use the services and resources of cloud computing. Itpermits to do temporary computations at the edge layer.Whereas edge nodes and sensors (IoT devices) are the dataproducers present at the ground level and the fog nodes are deployed closer to the edge nodes to limit the network traffic between the end devices and the cloud servers. Due to this limited distance, fog nodes are exposed to attackers. Once the fog nodes are compromised, then the privacy of the information will get affected [2]. To avoid this some security mechanisms like encryption is required. To avoid this some security mechanisms like encryption is required. In practical, it is hard to process the large volume of data generated by the multiple IoT devices which sends the same to the fog nodes. At this stage, data aggregation technique with homomorphic encryption is incorporated to avoid network traffic [3]. This will reduce the communication overhead when the data are
sent to the cloud control center via the fog nodes. When using this technique, security and privacy issues also tackled with high extension. Also, this technique will help you to decrease the utilization of network bandwidth [4].

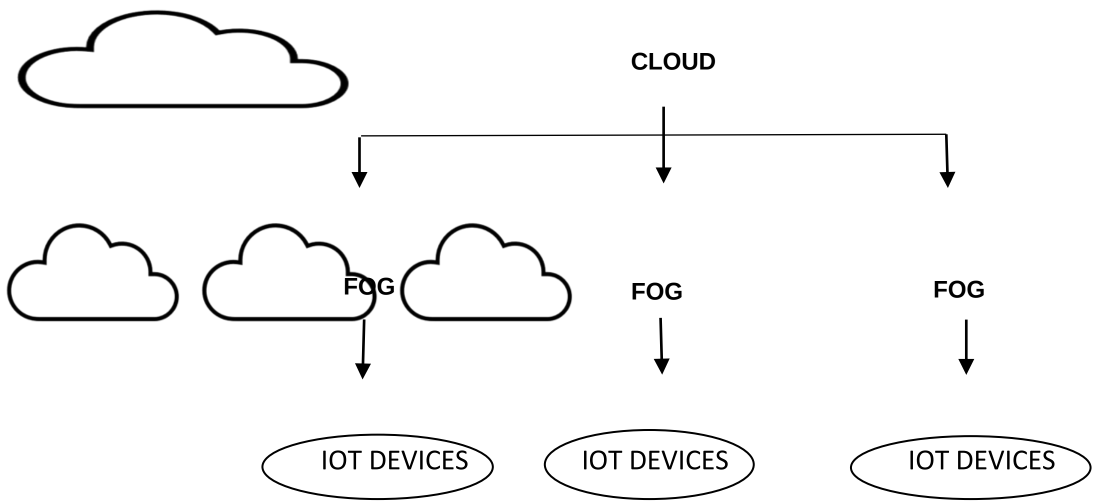


Fig 1 : Cloud-Fog-Architecture

I. COMPARISON OF CLOUD AND FOG COMPUTING

In this topic, it describes the main diversity between cloudand fog computing [5].

- The cloud is a centralized structure, whereas fog hasdistributed structural design.
- The cloud nodes or cloud servers are located at aremote place, whereas fog nodes are located at veryclose to the edge.
- When compared with the processing of data, cloudprocesses the data at far away from the source, butthe fog nodes are very near to the sources.
- The computing potential is very high in the cloudwhen compared to fog.
- The required number of nodes for cloud is limited,but in fog computing it is unlimited.
- In cloud computing, the scrutiny of data takes moretime, while in fog computing it completes in a shortperiod.
- In cloud computing the latency is high, and in fogcomputing it is low.
- In cloud computing, it is connected via the internet,whereas fog computing uses different protocols andstandards.
- Cloud computing has fewer security features whencompared to fog computing.

Table 1. Comparison of Results between Cloud and Fog.

Investigated Aspect	Traditional Cloud	Fog Computing
Prediction Latency	5 seconds	1.5 seconds
Webpage display	8 seconds	3 seconds
Internet Traffic	75 Kbps	10 Kbps
Hardware used	Amazon Web Server	Raspberry Pi

II.STRUCTURE OF FOG COMPUTING

The Fog structure consists of the Infrastructure (IaaS), Platform(PaaS), and Software-as-a-service(SaaS), with the Data Services, much like the cloud computing systems. For the IaaS structure, which was founded by Cisco, it uses a Linux or a Cisco IOS networking system wherein any router or a switch can be converted into a fog node having computing, storage,and networking facilities [6], [7]. This structural architecture of fog networking is depicted in Figure 2. These nodes can become one using a Peer-to-Peer network or a Master-Slave architecture or by making a Cluster. However, for the PaaS structure, the operator used is Cisco DSX, which makes a connection between SaaS and other forms of IoT systems. It enables easy application management, automation of policies,and sustains many programming languages. The service of thegiven data in this structure also determines the correct place foranalyzing data which require some form of action to be taken on them by enhancing security as the data is made anonymous Merits and Demerits in Fog Computing.

In fog computing, it includes of several merits and demerits based on its architecture. Table. 2 shows the important merits and demerits of fog computing.In this article, several details about fog computing areanalyzed in a detailed manner as working principle, merits anddemerits of fog, comparative study about cloud and fog, as anextension, discussed various security breaches and privacyproblems in fog computing, how to prevent and maintain theprivacy and integrity of data and how it is developed by theresearchers in the fog computing.

TABLE.2

MERITS	DEMERITS
The volume of data during transmission is minimized.	It holds the geographical location, which is increase the vulnerability.

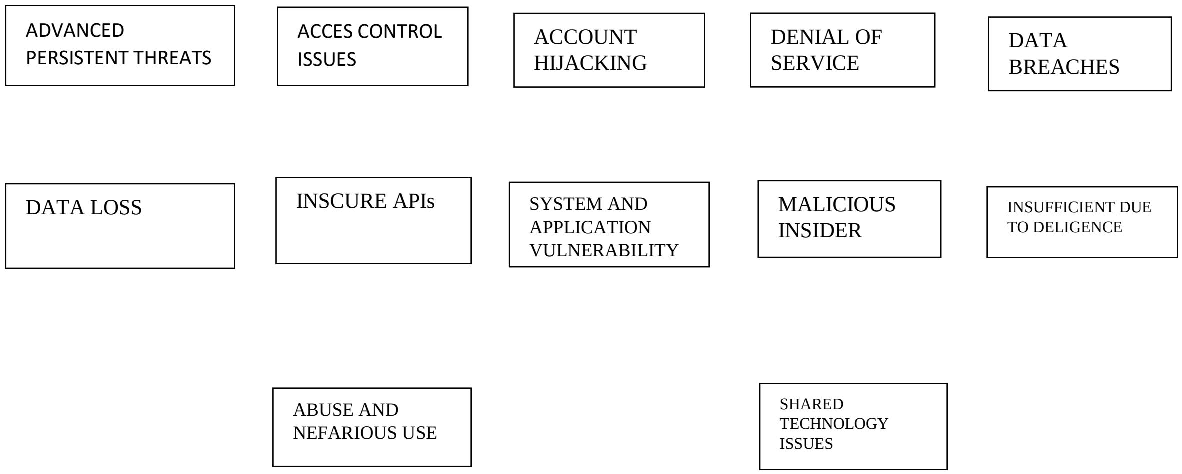
It protects the high usage of network bandwidth.	Possibility of IP spoofing, a man in middle attacks.
Improve the response time while communication.	Concerned about privacy issues, trust & authentication.
Increase the security by providing the resources at the edge.	It requires additional expenses to acquires edge devices like routers, hubs gateways, etc.
Maintain mobility	Difficult to implement.
Reduce the network time delay while data transfer.	Less scalable

Fog should do is network switching betweenloT and the Cloud. Here the Fog will act as an intermediary between end devices and the Cloud, and should providepushing service to both, while ingesting acquired data andupdating processed data onto the Cloud for long-time storageand deeply digging in parallel. Thus the prime function of theFog is to achieve local data processing, storing and computingin devices of weak performance metrics.Owing to its recent introduction and emergence, there is noavailable standardarchitecture regarding Fog-based resourcemanagement. [8] presents a simple model for this purpose, bytaking into account resource prediction, resource allocation,and pricing in a realistic and dynamic way, while alsoconsidering customers' type, traits, and characteristics.

III. NEED FOR SECURITY PROTECTION IN FOGCOMPUTING

As mentioned above, the increasing use of fog technology inthe various walks of social and industrial areas has increasedthe pressure on the developers to create a safe threat proofsystem for a more efficient and reliable network for datastorage and processing. With the rise in cyber threat andother malwares, this task is proving to be more difficult,as the traditional fog node creation does not include an inbuiltsecurity protocol as these secure measures are addedon later in the devices [9]. However, in view of the newtrend, the developers have initiated the inclusion of preprocessedsecurity protocols to furnish a stronger and safer fogcomputing unit for its use. This was achieved by shifting thefocus from better storage and processing system to a securitycentricdevice generation.

TYPES OF SECURITY THREATS



IV. RELATED WORK:

In 2016 Vishwanath et al, implemented the AES algorithm with various datasets to ensure the data security in the fog computing. This research makes another level of security and creates difficulty for the attackers to get the data. Also, various performance measures of the encryption technique are analyzed to ensure the accuracy of the entire data present in the datasets. These provide more advantage to the deployed system. But the weakness is AES key size is limited to a fixed size[10].

In 2018 Zang et al. describes the various architectures of Fog computing and identify the possible security and trustissues. Also investigate the solutions to overcome those issues and specify the real challenges present in security and trust in Fog Computing. In this paper, the drawback is it needs some new protocols and interfaces to ensure the security and trust, but it is very poor to automate the identification of security and trust vulnerabilities. [11]

In 2018 Zang et al. proposed a method named as pallier encryption scheme for protecting the privacy of thedata. This scheme ensures that the data inserted is only from genuine IoT devices. Also, it ensures the data packets are not disclosed to any others. It is observed that the data gathering from IoT devices are not affected even if some fog nodes are failed to transmit the data. This is a major advantage of this method. And the problem is,these security results are not enough to protect the CIA of fog platform[11].

In 2019 Shen et al proposed a scheme to protect the privacy and collusion opposing data aggregation for dynamicgroups. Also develop a strong data encryption, aggregation and decryption schemes in fog computing. The demerit of this scheme is it requires a third party assistance for data aggregation. [14].

Data security is oneof the key challenges in the big data era [2]. In thiscontext, securing the data in cloud computing invokedthe efforts of crypt-analysts, network security experts,software security engineers, and many others, anddata breaches are still occurring within cloud computing[3]. In fact, the data security issue is aggravatedin the case of fog computing [4]. Delivering Securityas-a-Service (SECaaS) was proposed to ensure endto-end system security including fog nodes, network,and data security [5].

V.PROBLEM STATEMENT

Fog computing paradigm extends the storage, networking, and computing facilities of the cloud computing toward the edge of the networks while offloading the cloud data centers and reducing service latency to the end users. However, the characteristics of fog computing arise new security and privacy challenges. The traditional cloud-based security mechanisms include the use of heavyweight cryptosystems, which are not suitable for direct application in the fog computing. Fog computing is vulnerable to security attacks because it is designed upon traditional networking component.Therefore, it has become indispensable to address the fog security and privacy issues.The proposed solution targets fog devices that are computationally constrained and thus, not capable of preforming intense computations; they are capable of performing very basic operations and lightweight encryption.

VI. PROPOSED SYSTEM

In our proposed cryptographic solution is based on Biometric key-dependent approach, which allows for a good compromise between the security level and computational complexity.A new key is generate to encrypt the Fog data with help of AES algorithm integrated with biometric data to ensure the data security.Biometrics is rapidly becoming a key piece of the security infrastructure and multifactor authentication – providing quick and easy verification, audit logs, and analysis. These systems are proving critical as the industry continues to scale and become more complex – and we should expect even bigger things in the years ahead.While biometrics provide non-repudiation and convenience, traditional cryptography provides adjustable levels of security and can be used not just for authentication, but also for encryption.In the proposed solution, the collected data at one fog node is encrypted, and dispersed in a random manner to its n neighbor fog nodes. We also adopt consistent hashing scheme the encrypted data is distributed to another fog node. It can be considered as a lightweight solution and it can be adapted according to the fog limitations in terms of power, storage, and computations.

VII .CONCLUSION AND FUTURE SCOPE

Fog computing is an emerging area for IOT applications. Through making full use of the geographically distributed network edge devices, the fog paradigm pushes more and more applications and services from cloud to the network edge. It greatly reduces the data transfer time and the amount of network transmission, and effectively meet the demands of real-time or latency sensitive applications and ease network bandwidth bottlenecks. Fog is attractive target for cyber-attackers since the fog contains huge volumes of sensitive data from both Cloud and IOT devices. In this manner, more research is required to improve fog security. In this paper, we focus on the fog computing technology. The architecture, challenges of fog computing and its security issues. Based onthe survey, one of the key challenge is data security. In this research concluded with new biometric secret key using AES algorithm to create a secure network where all the IOT data can be privately stored and shared in the current.

REFERENCES:

[1].Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on mobile cloud computing (pp. 13–16). New York: ACM.

[2].Jia, W., Zhu, H., Cao, Z., Dong, X., & Xiao, C. (2013). Human-factorawareprivacy-preserving aggregation in smart grid. IEEE Systems Journal, 8(2), 598-607.

[3].Wang X, Wang L, Li Y, Gai K(2018) Privacy-Aware Efficient Fine-Grained Data Access Control in Internet of Medical Things Based FogComputing. IEEE Access 6(1):47657–47665.

[4] Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H.: Cloudletsauthentication in nfc-based mobile computing. In: MobileCloud. IEEE(2014).

[5] Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fogcomputing: architecture, key technologies, applications and openissues. Journal of network and computer applications, 98, 27-42.

[6] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi,“Iot survey: An sdn and fog computing perspective,” Computer Networks, vol. 143, pp. 221 – 246, 2018.
article/pii/S1389128618305395

[7] C. B. Tan, M. H. A. Hijazi, Y. Lim, and A. Gani,“A survey on proof of retrievability for cloud data

integrity and availability: Cloud storage state-of-the-art,issues, solutions and future trends,” Journal of Networkand Computer Applications, vol. 110, pp. 75 – 86, 2018.
[Online]. Available: http://www.sciencedirect.com/science/
article/pii/S1084804518301048

[8] Y. Guan, J. Shao, G. Wei, and M. Xie, “Data security andprivacy in fog computing,” IEEE Network, vol. 32, no. 5, pp.106–111, September 2018.

[9] ETSI: Mobile-edge computing. http://goo.gl/7NwTLE (2014).

[10] Vishwanath, A., Peruri, R., & Jing (Selena) He. (2016). Security in fogcomputing through encryption. DigitalCommons@ Kennesaw StateUniversity.

[11] Zhang, P., Zhou, M., & Fortino, G. (2018). Security and trust issues inFog computing: A survey. Future Generation Computer Systems, 88, 16-27.

[12] Zhang, Y., Zhao, J., Zheng, D., Deng, K., Ren, F., Zheng, X., & Shu, J.(2018). Privacy-preserving data aggregation against false data injectionattacks in fog computing. Sensors, 18(8), 2659.

[13] Shen, X., Zhu, L., Xu, C., Sharif, K., & Lu, R. (2020). A privacypreservingdata aggregation scheme for dynamic groups in fogcomputing. Information Sciences, 514, 118-130.

[14] B. A. Martin, F. Michaud, D. Banks, A. Mosenia, R. Zolfonoon,S. Irwan, S. Schrecker, and J. K. Zao, “Openfogsecurity requirements and approaches,” in 2017 IEEE Fog.

[15] Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-preserving multikeywordranked search over encrypted cloud data. TPDS 25 (2014)

[16] Wei J, Wang X, Li N, Yang G, Mu Y(2018) A Privacy-Preserving FogComputing Framework for Vehicular Crowdsensing Networks. IEEEAccess 6(1):43776–43784.

[17]https://www.sam-solutions.com/blog/fog-computing-vs-cloudcomputing-for-iot-projects/World Congress (FWC), Oct 2017, pp. 1–6.