International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Security Analysis with Fog Computing

Mohit Sharama[1], Dr. Manish Jha[2]

[1]M. Tech Scholar, CSE Department, IITM, Sonipat, Haryana
[2]Professor, CSE Department, IITM, Sonipat, Haryana

Abstract
With numerous benefits of cloud storage such as cost savings, accessibility, scalability etc., users around the world tend to shift their invaluable data to cloud storage. As the data generation rates are increasing, it is a tedious task for cloud storage providers to provide efficient storage. Cloud storage providers uses different techniques to improve storage efficiency and one of leading technique employed by them is de duplication, which claims to be saving 90 to 95% of storage,. Data De duplication technique evolved as an simple storage optimization technique in secondary then widely adapted in primary storage as well as larger storage areas like cloud storage area. Now, data de duplication is widely used by various cloud storage providers. Data once deployed to cloud servers, it's beyond the security premises of the data owner, thus most of them prefer to outsource their in an encrypted format.

Keywords: Fog Computing, Edge Computing, Mobile Cloud Computing, Cloud Computing

I. Introduction

In Fog computing, services can be hosted at end devices such as set-top-boxes or access points. The infrastructure of this new distributed computing allows applications to run as close as possible to sensed actionable and massive data, coming out of people, processes and thing. Such Fog computing concept, actually a Cloud computing close to the 'ground', creates automated response that drives the value. Both Cloud and Fog provide data, computation, storage and application services to end-users. However, Fog can be distinguished from Cloud by its proximity to end-users, the dense geographical distribution and its support for mobility . We adopt a simple three level hierarchy as in Figure 1.

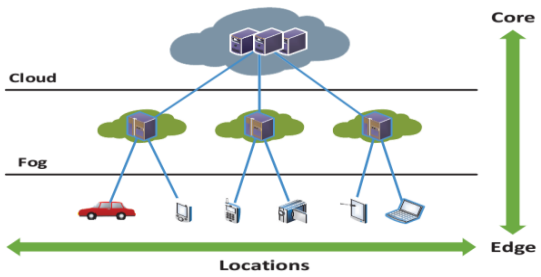

Fig 1: Fog between edge and cloud.

In this framework, each smart thing is attached to one of Fog devices. Fog devices could be interconnected and each of them is linked to the Cloud. In this article, we take a close look at the Fog computing paradigm. The goal of this research is to investigate Fog computing advantages for services in several domains, such as Smart Grid, wireless sensor networks, Internet of Things (IoT) and software

defined networks (SDNs). We examine the state of-the-art and disclose some general issues in Fog computing including security, privacy, trust, and service migration among Fog devices and between Fog and Cloud. We finally conclude this article with discussion of future work. Fog computing is a distributed computing paradigm that acts as an intermediate layer in between Cloud data centers and IoT devices/sensors. It offers compute, networking and storage facilities so that Cloud-based services can be extended closer to the IoT devices/sensors [1].

Fog computing to create large geographical distributions of Cloud-based services. Besides, Fog computing facilitates location awareness, mobility support, real-time interactions, scalability and interoperability [3]. Thereby, Fog computing can perform efficiently in terms of service latency, power consumption, network traffic, capital and operational expenses, content distribution, etc. In this sense, Fog computing better meets the requirements with respect to IoT applications compared to a solely use of Cloud computing [4].

The rest of research paper is design as follows. The overall previous work is described in Section II. Section III describes the methodology used for proposed work. Result analysis describe in section IV. Finally, Section V describes the conclusion of paper.

II. Previous Researchers

Peter, Nisha et al. (2024) In this paper, fog Computing is a technology that extends cloud computing and services to the edge of the network. The different characteristics of fog are low latency and location awareness, wide-spread geographical distribution, mobility, very large number of nodes, predominant role of wireless access, strong presence of streaming and real time applications and heterogeneity.

Dubey, Harishchandra, et al. (2024) In this paper, the size of multi-modal, heterogeneous data collected through various sensors is growing exponentially. It demands intelligent data reduction, data mining and analytics at edge devices.

Zhanikeev, Marat et al. (2023) In this paper, evolving from hybrid clouds to true cloud federations and, ultimately, fog computing will require that cloud platforms allow for--and embrace--local hardware awareness.

Yi, Shanhe et al. (2023) In this paper, despite the increasing usage of cloud computing, there are still issues unsolved due to inherent problems of cloud computing such as unreliable latency, lack of mobility support and location-awareness.

Shi, Yingjuan et al. (2022) In this paper, fog Computing is a new architecture to migrate some data center's tasks to the edge of the server. The fog computing, built on the edge servers, is viewed as a novel architecture that provides the limited computing, storing, and networking services in the distributed way between end devices and the traditional cloud computing Data Centers.

Luan, Tom H., et al. (2021) In this paper, with smart devices, particular smartphones, becoming our everyday companions, the ubiquitous mobile Internet and computing applications pervade people daily lives.

Yi, Shanhe et al. (2021) In this paper, despite the broad utilization of cloud computing, some applications and services still cannot benefit from this popular computing paradigm due to inherent problems of cloud computing such as unacceptable latency, lack of mobility support and location-awareness.

Truong, Nguyen B., et al. (2021) In this paper, vehicular Adhoc Networks (VANETs) have been attracted a lot of research recent years. Although VANETs are deployed in reality offering several services, the current architecture has been facing many difficulties in deployment and management because of poor connectivity, less scalability, less flexibility and less intelligence.

Wang, Yifan et al. (2021) In this paper, although Fog Computing is defined as the extension of the Cloud Computing paradigm, its distinctive characteristics in the location sensitivity, wireless connectivity, and geographical accessibility create new security and forensics issues and challenges which have not been well studied in Cloud security and Cloud forensics.

Loke, Seng W et al. (2020) In this paper focuses on services and applications provided to mobile users using airborne computing infrastructure.

Bitam, Salim et al. (2020) In this paper, cloud computing is a network access model that aims to transparently and ubiquitously share a large number of computing resources. These are leased by a service provider to digital customers, usually through the Internet.

III. Frame Work of Research

The main objectives of research work are to Study Fog Computing and its data depuplication issues in detail. A new hybrid encryption-based scheme for data de duplication in fog computing is to be propose to evaluate the performance of proposed scheme using various parameters. The proposed methodology is given in fig 2

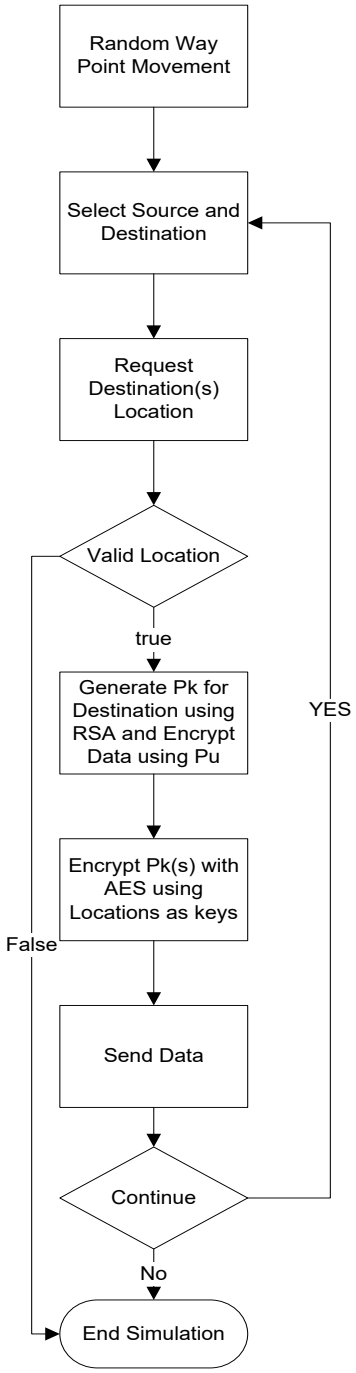

Fig 2 Proposed Workflow of De-duplication process

In both the anonymous and authenticated models, clients begin the ingestion process by transforming a file into a set of parts. This is often accomplished using a content-based partitioning procedure which produces parts based on the contents of the file. The advantage of this approach is that it can match shared content across files even if that content does not exist at the multiple of a given, fixed offset. The algorithm selects parts based on a threshold value A and a sliding window of width w that is moved over the file. At each position k in the file, a fingerprint, $F_{k,k+w-1}$, of the window's contents is calculated. If $F_{k,k+w-1} > A$, then k is selected as a part boundary. The result is a set of variable sized parts, where the boundary between parts is based on the content of the data.

Both file partitioning and encryption occur on the client. There are a number of benefits to performing these tasks on the client, as opposed to the server. First, it reduces the amount of processing that must occur on the server. Second, by encrypting parts on the client, data is never sent in the clear, reducing the effectiveness of many passive, external attacks. Third, a privileged, malicious insider would not have access to the data's plaintext because the server does not need to hold the encryption keys.
Clients encrypt parts using *RSA Encryption*, using RSA, clients use an encryption key deterministically derived from the plaintext content to be encrypted; and our system use a crypto- graphic hash of the plaintext as the key using AES. Since identical plaintexts result in the use of identical keys, regardless of who does the encryption, a given plaintext always results in the same ciphertext.

$K = hash(\text{part})$

Compared to other approaches, this strategy offers a number of advantages. if each user encrypted using his own key, the amount of storage space saved through deduplication would be greatly reduced because the same part encrypted using two different keys would be would result in different ciphertext (with very high probability). Second, attempting to share a random key across several user accounts introduces a key sharing problem. Third, a user that does not know the data plaintext value cannot generate the key, and therefore cannot obtain the plaintext from the ciphertext. This point is especially important since, in contrast to an approach where the server encrypts the data, even a root level administrator does not have access to a part's plaintext value without the key. Sharing files could also be accomplished by using the authorized user's symmetric key to encrypt the AES key, and appending this encrypted key to the part location. While similar to the authenticated model's strategy, this approach suffers from a number of disadvantages. First, any information that identifies the user's key in the list is breaking anonymity. Second, even if an key of the file part was used to hide the user's identity, the list would still leak the number of users that have access to the file. Third, the use of location references provides a level of coarse grained revocation. A part location can be created and encrypted with a new part location key.

IV. Result Analysis

Following table describes the simulation parameters for IoT mobility in MATLAB, each node properties is defined in MATLAB Structure.

Parameter	Value
Node POSITION_X_INTERVAL	10-30
Node POSITION_Y_INTERVAL	10-30
Node SPEED_INTERVAL	0.2-2.2
Node PAUSE_INTERVAL	0-1
Node WALK_INTERVAL	2.00-6.00
Node	-180-180

DIRECTION_INTERVAL	
SIMULATION_TIME	500
Number of Nodes	20
Public Key Encryption	RSA
Private Key Encryption	AES

This speed surmounts the symmetric encryption problem of managing secret keys. As on the other hand, this unique feature of public key encryption makes it mathematically less prone to attacks. However, asymmetric encryption techniques are slower than symmetric techniques, because they require more computational processing power. As it can be seen from above fig the encryption time does not increases too much when number of nodes increase as seen in above figure 3. So does the decryption process as seen below.

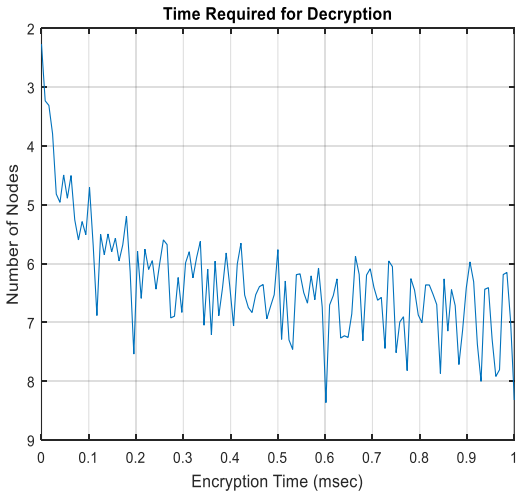

Fig 3 Time Required in Deduplication Process

Table 1 Deduplication time complexity for Base paper and Proposed RSA-AES Hashing Scheme

Data Chunks	Base paper	RSA-AES
1 KB	1.1	0.858
10 KB	3	2.34
100 KB	5.2	4.056
1 MB	7.2	5.616
10 MB	8.45	6.591
100 MB	12.01	9.3678
1 GB	23.484	18.31752

Table 1 gives the comparison table of different scheme. This table shows that improved result as compare to base paper.

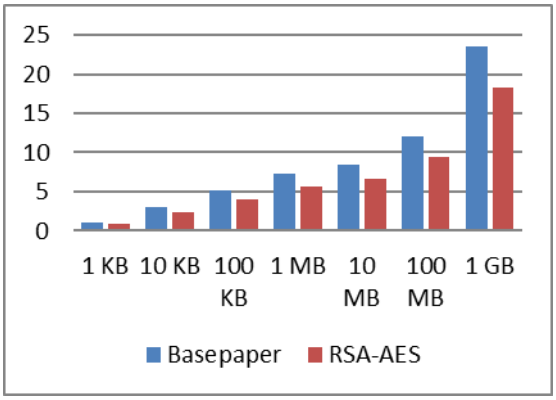

Fig 4 RSA-AES Hashing vs. base paper Computation Complexity for various chunks of data

Computation complexity is given in the figure 4. It gives in various chunks of data.

V. Conclusion

Many principles and protocols, given by various authors, have been proposed in this report that will help in deduplicating Fog network. Introduction of the dynamic variable cipher security certificate protocol is given. This protocol uses key matrices concept. In this protocol we make use of key matrices and store same key matrix at all the communicating nodes. Thus when plain text is encrypted to cipher text at the sending side, the sender transmits the cipher text without the key that is to be used to decrypt the message. In spite, the sender sends the co-ordinate of the key matrix where the key is stored.

References:

[1]. Dastjerdi, A., Gupta, H., Calheiros, R., Ghosh, S., Buyya, R.: Chapter 4 - fog computing: principles, architectures, and applications. In Buyya, R., Dastjerdi, A.V., eds.: Internet of Things: Principles and Paradigms. Morgan Kaufmann (2016) 61 – 75

[2]. Sarkar, S., Misra, S.: Theoretical modelling of fog computing: a green computing paradigm to support iot applications. IET Networks 5(2) (2016) 23–29

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

[4]. Sarkar, S., Chatterjee, S., Misra, S.: Assessment of the suitability of fog computing in the context of internet of things. IEEE Transactions on Cloud Computing PP(99) (2015) 1–1

[5]. Garcia Lopez, P., Montresor, A., Epema, D., Datta, A., Higashino, T., Iamnitchi, A., Barcellos, M., Felber, P., Riviere, E.: Edge-centric computing: Vision and challenges. ACM SIGCOMM Computer Communication Review 45(5) (2015) 37–42

[6]. Varghese, B., Wang, N., Barbhuiya, S., Kilpatrick, P., Nikolopoulos, D.S.: Challenges and opportunities in edge computing. Proceedings of the IEEE International Conference on Smart Cloud (2016) 20–26

[7]. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: Vision and challenges. IEEE Internet of Things Journal 3(5) (Oct 2016) 637–646

[8]. Hu, Y.C., Patel, M., Sabella, D., Sprecher, N., Young, V.: Mobile edge computinga key technology towards 5g. ETSI White Paper 11 (2015)\

[9]. Klas, G.I.: Fog Computing and Mobile Edge Cloud Gain Momentum Open Fog Consortium, ETSI MEC and Cloudlets. (2015).

[10]. Cau, E., Corici, M., Bellavista, P., Foschini, L., Carella, G., Edmonds, A., Bohnert, T.M.: Efficient exploitation of mobile edge computing for virtualized 5g in epc architectures. In: 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). (March 2016) 100–109

[11]. Ahmed, A., Ahmed, E.: A survey on mobile edge computing. In: the Proceedings of the 10 t h IEEE International Conference on Intelligent Systems and Control (ISCO 2016), Coimbatore, India. (2016)

[12]. Mahmud, M.R., Afrin, M., Razzaque, M.A., Hassan, M.M., Alelaiwi, A., Alrubaian, M.: Maximizing quality of experience through context-aware mobile application scheduling in cloudlet infrastructure. Software: Practice and Experience 46(11) (2016) 1525–1545 spe.2392.

[13]. Sanaei, Z., Abolfazli, S., Gani, A., Buyya, R.: Heterogeneity in mobile cloud computing: taxonomy and open challenges. IEEE Communications Surveys & Tutorials 16(1) (2014) 369–392

[14]. Bahl, P., Han, R.Y., Li, L.E., Satyanarayanan, M.: Advancing the state of mobile cloud computing. In: Proceedings of the third ACM workshop on Mobile cloud computing and services, ACM (2012) 21–28

[15]. Satyanarayanan, M., Lewis, G., Morris, E., Simanta, S., Boleng, J., Ha, K.: The role of cloudlets in hostile environments. IEEE Pervasive Computing 12(4) (2013) 40–49

[16]. Peter, Nisha. "Fog computing and its real time applications." International Journal of Emerging Technology and Advanced Engineering (IJETAE) 5, no. 6 (2024): 266-269.

[17]. Dubey, Harishchandra, Jing Yang, Nick Constant, Amir Mohammad Amiri, Qing Yang, and Kunal Makodiya. "Fog data: Enhancing telehealth big data through fog computing." In Proceedings of the ASE BigData & Social Informatics 2024, p. 14. ACM, 2024.

[18]. Zhanikeev, Marat. "A cloud visitation platform to facilitate cloud federation and fog computing." Computer 48, no. 5 (2023): 80-83.

[19]. Yi, Shanhe, Cheng Li, and Qun Li. "A survey of fog computing: concepts, applications and issues." In Proceedings of the 2015 Workshop on Mobile Big Data, pp. 37-42. ACM, 2023.

[20]. Shi, Yingjuan, Gejian Ding, Hui Wang, H. Eduardo Roman, and Si Lu. "The fog computing service for healthcare." In Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), 2015 2nd International Symposium on, pp. 1-5. IEEE, 2022.