International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4
ISSN: 2454-4248
235 – 238

Robust Data De-duplication Security in Fog Computing

Anu
Assistant Professor (Resource Person),
Department of Computer Science, UIET,
MDU, Rohtak, Haryana, India

***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,. So now days the data de-duplication has been broadly used in the cloud storage providers. As if the data is being deploy to the cloud servers than the data is not in the reach of owner security premises and everyone want to outsource that data in the encryption form.

Keywords: *Fog computing, edge computing, mobile cloud computing,*

*****

I. Introduction

In for computing, we can get the services at the ending points like set top boxes and the various access points from where services can be taken. Thus this new distribute application run in such a way that it is close to the sensible actions and the huge data which is got from the peoples, processes and the various things. These fog computing concepts are basically a form of cloud computing which runs adjacent to the ground and generates the automated responses which drive the values. As we know that both the fog and cloud computing facilitate the data, computation methods, storage space and various services for the applications to the users. Beside these similarities these two methods can be classified by the proximity to the end users, on the basis of narrower geographical distribution and about the mobility support. Thus we agreed a basic three level hierarchy as in Figure 1.

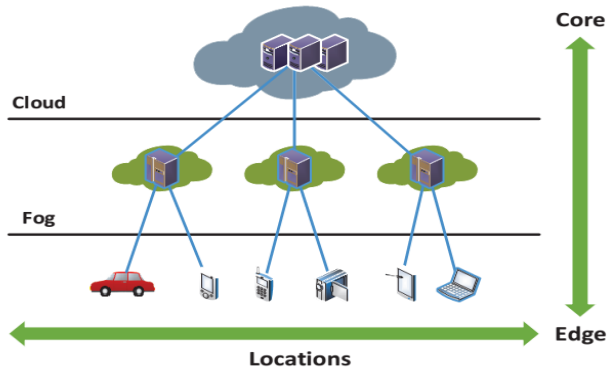

Fig 1: Fog between edge and cloud.

As in framework shown above, every new thing is attacked to the fog devices. As this is observed from fig. 1 that every fog devices is inter-connected to each other and they connect to the cloud. In this paper we discuss about the cloud computing paradigm in details. Thus main aim of this article is to study about the effects of fog computing on the services provided by various domains like smart grid, WSN,

IoT and the SDNs. Thus here we inspect the various factors of fog computing and analyze the various issues of fog computing like security and service transfer between the fog devices and then between fog and cloud. Then we make the conclusion of this article on the basis of its future scope and work. Basically fog computing is a paradigm which serve as a intermediate layer between the cloud and the user data points and sensors. It offer computing, and storage services so that we can extend the cloud base services close to the IoT devices and the sensors. [1] basically fog computing is used for generating the huge geographical distribution of the cloud based services by acting as the middle layer between cloud and data points and provides evenly services by distribution. Besides this the fog computing provides the location knowledge, mobility support and the real time interaction. [3].

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 proposedwork. Result analysis describe in section IV. Finally, Section V describes the conclusion of paper.

II. Frame Work of Research

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

As this has been observed that in both the anonymous and authenticated model the file has been transferred in parts. Usually we perform this by the use of content based

 ISSN: 2454-4248
235 – 238

separation process that generates the parts on the basis of content stored in files. The main feature of this method is that by this we can share the content throughout the files even in those cases when the data is not available at the multiple of a given, constant offset. Thus the algorithm thus used select the threshold vales A and the sliding window of *w* which moves over the file. As the every location of the k present in the file. The result thus obtained is a set of variables size, in which the boundaries among the parts has been relied on the content present in data.

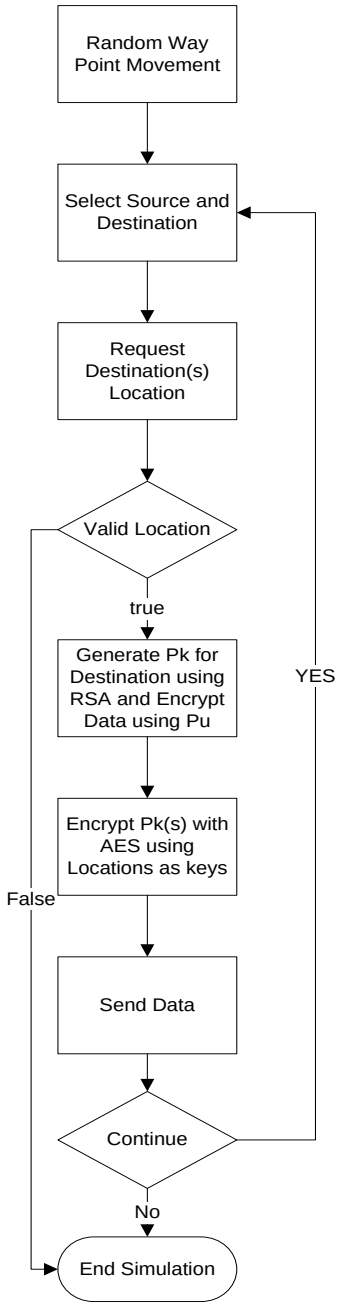

Fig 2Proposed Workflow of Deduplication process

If $F_k,k+w-1 > A$, then in this case k is choose as a part boundary. Thus the results obtained is a set of variables size, in which the boundaries among the parts has been relied on the content present in the data.

As the file separation and encryption has been performed in the client. When we perform these task on the client rather than server there are number of benefits we observed, Firstly it minimize the extent of processing is being occurred at the server. Secondly, when we encrypt the parts on the client the data is not transmitted in the clear, thus is secure the data from many external and passive attack effectively. The third benefit is that f any malicious behavior is present inside the system than it can not get admittance to the data of plaintext because in this case the server doesn't have any requirement to need to embrace the encryption keys.

Clients encrypt parts using *RSA Encryption*, using RSA, thus client used a encryption key which is derive from the plaintext content to be encrypted. As we use the identical plaintext for the identical keys, on the basis of whichever done the encryption, thus the provided plaintext provides the results in the similar ciphertext.

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

When we compare the present approach with other approaches, than a number of advantages has been found in present approach. if every user encrypt by his own key than by this the storage space taken by the de-duplication has been saved upto a much extant because if the same part is being encrypted by the two keys than it would produce two ciphertext. Secondly when we attempt to share the random key across the various users then it generates the sharing issues. Third, the user doesn not have any knowledge about the data plaintext that is can not generate the key, and thus it can not obtain he plaintext from the ciphertext. This have the more importance as in opposite to a approach in which the server encrypt the data even the root level administrator can not access the plaintext without key. We can also share files by using the authorized user's symmetric key to encrypt the AES key, and on the basis of this encrypted key to the part location. Like authenticated strategy this also have various limitations. Firstly, any such data which can identify user key from the list is a breakinganonymity. Secondly when f key is employed for hiding the user identification, , even then we can know about the extent of users that have permission to access the files. From the list.

Result Analysis

Following table describes the simulation parameters for IoT.

ISSN: 2454-4248
235 – 238

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 DIRECTION_INTERVAL	-180-180
SIMULATION_TIME	500
Number of Nodes	20
Public Key Encryption	RSA
Private Key Encryption	AES

Additionally such a unique feature of the public keyencryption makes this method computationally more secure from the attacks. this different feature of the public key encryption makes it mathematically secure to the attacks. As we observe that the un0syymmetric encryption method are much slower than the symmetric ones. This is because these they demand the higher power for the computation process. As we observe from the above figure than when we increase the number of node then there are not any significant changes in the encryption time. So does the decryption process as seen below.

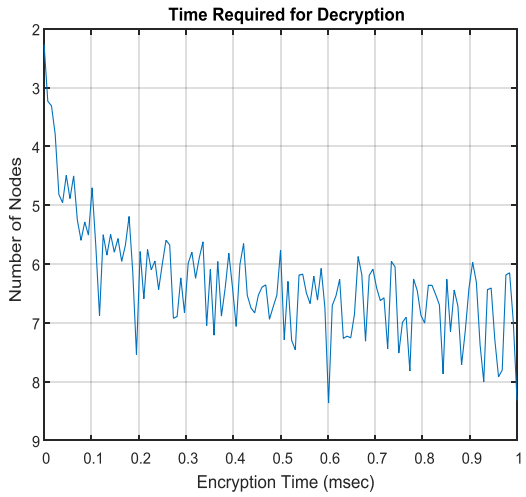

Fig 3 Time Required in Deduplication Process

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.

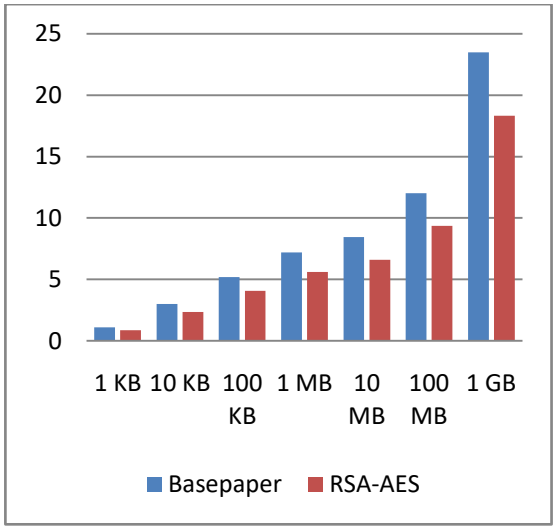

Fig 4 RSA-AES Hashing vs. base paper Computation Complexity for various chunks of data

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

III. Conclusion

Many principles and protocols, given by various authors, have been proposed in this report that will help in deduplicating Fog network. Also the introduction of the dynamic variable cipher security certificate protocol has been given. In this protocol we uses key matrices concept. In this concept we use the identical key matrices and also save the identical key matrices at the whole communicating nodes. Thus when the plaintext is encrypt to the cipher text on the sending direction, the transmitter transmit the cipher text without any key which is being used to decrypt the message.

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

 ISSN: 2454-4248
235 – 238

[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 (2015): 266-269.

[17]. Dubey, Harishchandra, Jing Yang, Nick Constant, Amir Mohammad Amiri, Qing Yang, and KunalMakodiya. "Fog data: Enhancing telehealth big data through fog computing." In Proceedings of the ASE BigData&SocialInformatics 2015, p. 14. ACM, 2015.

[18]. Zhanikeev, Marat. "A cloud visitation platform to facilitate cloud federation and fog computing." Computer 48, no. 5 (2015): 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, 2015.

[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, 2015.