International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Fog Computing Application for Cloud Servers

Anirudh Dwivedi[1], Gaurav Gangrade[2], Swatipriya Chourasia[3], Aayushi Mundhada[4], Mrs. Deepali M. Gohil[5]
[1, 2, 3, 4, 5]*Computer Department, D.Y. Patil College Of Engineering, Savitribai Phule Pune University*

Abstract: ***In order to reduce the burden of maintaining big data, more and more enterprises and organizations have chosen to outsource data storage to cloud storage providers. Moreover, all the advantages of cloud computing are taken into consideration while storing sensitive data on the cloud. Cloud users cannot trust only on the cloud service provider for the security of their sensitive data stored on the cloud.***
In this paper we are making use of fog computing to overcome the problem with the semi-trusted cloud service provider, while user will upload the file and the file will be uploaded on the fog node, here the fog node performs the encryption of the uploaded file and then divide the file into blocks and hash of the data will be computed. And only 5% of data will be stored on the fog device then the remaining 95% data will be forwarded to the cloud on the cloud we are again going to perform encryption of the data to make it more secure and the data will be divided into the blocks and stored on the cloud with the computing the hash of the data. It maintains the privacy of the stored data due to double encryption of the data and also the file is stored on two different locations so if CSP tries to access the file then he cannot get whole data.
Keywords: Three Layer Privacy Preserving, Cloud Storage, Fog Computing, Data Encryption, Data Block Hash Generation.

I. INTRODUCTION

With the rapid development of network bandwidth, the volume of user's data is rising geometrically. User's requirement cannot be satisfied by the capacity of the local machine anymore.
Therefore, people try to find new methods to store their data. Pursuing more powerful storage capacity, a growing number of users select cloud storage. Information outsourcing and sharing have become ubiquitous in our life as cloud computing assures to elastically store and process a large amount of data.
The data stored on the cloud mainly contains secret and sensitive information.
Some of the amazing benefits of cloud computing like on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [7] make it more reliable. But there are certain privacy issues in traditional systems when outsourcing data on to the cloud as Cloud Server Provider (CSP) will take place of the user to manage the data. In consequence, the user does not actually control the physical storage of their data, which results in the separation of ownership and management of data. The CSP can freely access and search the data stored in the cloud. Meanwhile, the attackers can also attack the CSP server to obtain the user's data. The above two cases both make users fell into the danger of information leakage and data loss.
The existing privacy protection schemes are generally based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of the cloud server. In order to solve this problem fog computing is used.
Fog computing [8][9] [10] is an extended concept of cloud computing which is composed of a lot of fog nodes[11]. These nodes have a certain storage capacity and processing capability.
Fog computing enables a wide range of benefits, including enhanced security [9], decreased bandwidth, and reduced latency [8][12]. These benefits make the fog as an appropriate concept for many IoT services in various applications. Fog computing is usually a three-level architecture; the utmost is cloud computing layer which has powerful storage capacity and computes capability. The next level is the fog computing layer. The fog computing layer serves as the middle layer of the fog computing model and plays a crucial role in transmission between cloud computing layer and sensor network layer. The fog nodes in fog computing layer have certain storage capacity and compute capability.
This study makes use of fog computing to overcome the problem with the semi-trusted cloud service provider. A user first will upload the file and file will be uploaded on the fog node, here the fog node performs the encryption of the uploaded file and then divides the file into blocks and hash of the data will be computed. When data owner wants to access the data then firstly the fog will access the stored data in decrypted from the Cloud and then merge all the blocks and by decrypting the file we can get the original data.

II. LITERATURE SURVEY

Li Hui et al. [1] focus on the enabling and critical cloud computing security protection techniques and surveys on the recent researches in these areas. Different fine-grained cloud data access control mechanism such as, secure search over encrypted cloud data, outsourced data integrity auditing, secure deletion for cloud data, etc., which ensure that cloud users enjoy the convenience the cloud offers in a privacy-preserving way is explained. In addition, further, point out some unsolved but important challenging issues and hopefully provides insight into their possible solutions. To build users' confidence in such cloud storage service paradigm, tons of attention.

Yang Li et al. [2] propose to use multiple mobile sinks to help with data uploading from WSNs to Cloud. An efficient algorithm is intended to schedule the multiple mobile sinks, with several provable properties. We conduct extensive simulations to evaluate the performance of the proposed algorithm. The results show that our algorithm can upload the data from WSNs to Cloud within the limited latency and minimize energy consumption as well.

Jonathan Chase et al. [3] solve a stochastic integer programming problem to obtain optimal provisioning of both virtual machines and network bandwidth when demand is uncertain. The given solution can minimize users' costs and provides superior performance to alternative methods. We believe that this integrated approach is the way forward for cloud computing to support network-intensive applications.

Q. Hou, et al. [4] gives two schemes for different application scenarios i.e the distributed file system or the operating system. The given virtual machine monitor, conventional attacks and attacks from cloud administrators. In one scheme, every chunk of user's file is protected, so the privacy of every chunk is guaranteed. Secondly, the complete file is protected, and the privacy of the whole file is guaranteed not all chunks. The visual projection of the SSL secure connection and secure virtual machine are evaluated. In consideration of the privacy of the user's data, the overhead can be tolerated.

III. PROPOSED SYSTEM

A. System Architecture

Any client/small organization that processes data in the cloud is subjected to an inbuilt level of risk as the outsourced services bypass the "physical, logical and personnel controls" of the user. While storing the data on the cloud, one might want to ensure if the data is correctly stored and can be retrieved later. so there is a need to provide such assurance to a client. The proposed system gives the guarantee of the security of sensitive data stored by use of fog computing. The system can protect the privacy of the user by making the file inaccessible to any unauthorized personnel. Figure 1 shows the architecture of the proposed system followed by the system working.

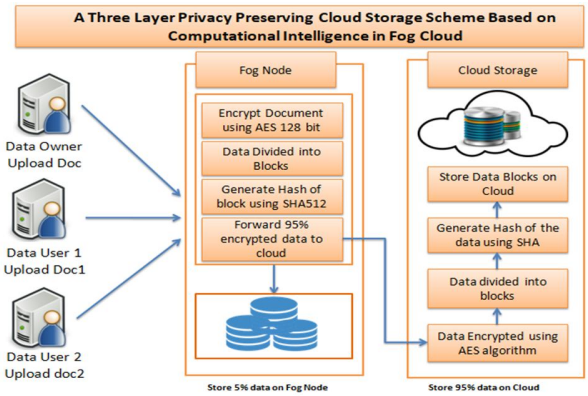

Figure 1: System Architecture

Data Owner uploads document, the document will be uploaded on the fog node. Uploaded file then encrypted using the 16 byte AES key which is entered by the user at the time of Registration. Data block Generation: The encrypted file now divided into the blocks. The blocks are of the same size. The Hash will be computed of each block. We Maintain the Hash of file data and block of file data as a reference and used at the time of downloading. Both the fog and the clouds will follow this step for storing data. While data owner wants to access the data then firstly the fog will access the stored data in decrypted from the Cloud and then merge all the blocks to generate one file. Finally, the merged file will be decrypted to achieve the original data and the data will be downloaded on the user browser.

B. System Flowchart

The overall flow of the proposed system is as shown in below figure.

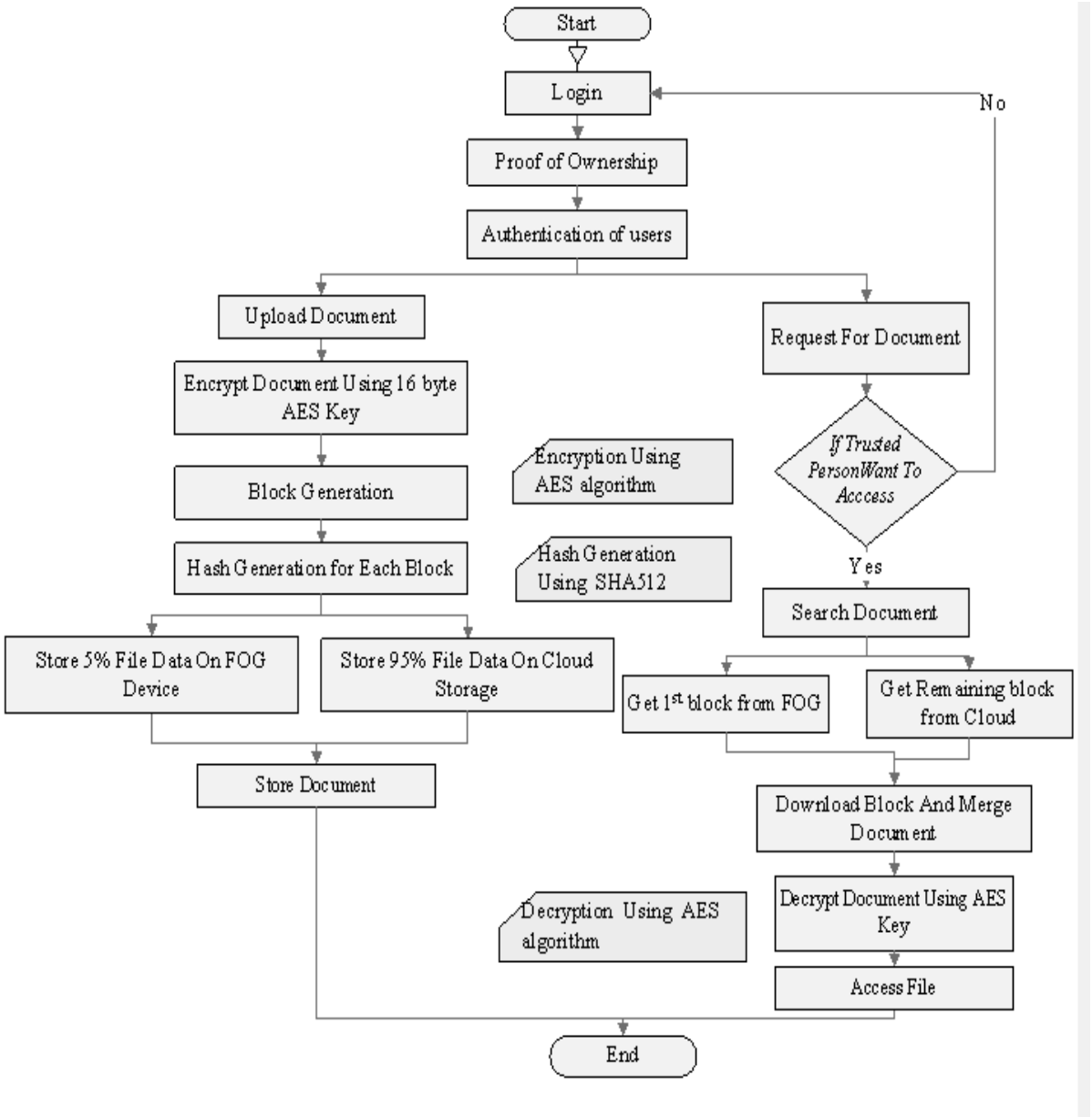

Figure: 2 System Flow

IV. ALGORITHMS USED

A. AES Algorithm

1) Encryption

a) You take the following AES steps of encryption for a 128-bit block:

*i)*Get the set of round keys from the cipher key.

*ii)*Initialize the state array with the block data (plaintext).

*iii)*Add the initial round key to the starting state array.

*iv)*Carry out nine rounds of state manipulation.

*v)*Execute the tenth and final round of state manipulation.

*vi)*Copy the final state array out as the encrypted data (cipher text).

b) Every round of the encryption procedure need a series of steps to change the state array.

These steps involve four types of operations as follows:

*i)*Sub-Bytes
*ii)*Shift-Rows
*iii)*Mix-Columns
*iv)*Xor-Round Key

2) Decryption

a) It involves reverse all the steps taken in encryption using inverse functions

*i)*InvSub-Bytes
*ii)*InvShift-Rows
*iii)*InvMix-Columns

b) Operation In Decryption Is

*i)*Perform initial decryption round:

1. Xor-Round Key
2. InvShift-Rows
3. InvSub-Bytes

*ii)*Perform nine full decryption rounds:

c) Xor-Round Key

*i)*InvMix-Columns
*ii)*InvShift-Rows
*iii)*InvSub-Bytes

1. Perform final Xor-Round Key

B. SHA 512 Algorithm

1) Append Padding Bits and Length Value: This step makes the input message an exact multiple of 1024 bits:

2) Initialize Hash Buffer with Initialization Vector: Before we can process the first message block, we need to initialize the hash buffer with IV, the Initialization Vector

3) Process Each 1024-bit (128 words) Message Block Mi: Each message block is taken through 80 rounds of processing.

4) Finally: After all the N message blocks have been processed, the content of the hash buffer is the message digest.

V. EXPERIMENTAL RESULT

This study makes use of fog computing to overcome the problem with the semi-trusted cloud service provider. A user first will upload the file and file will be uploaded on the fog node, here the fog node performs the encryption of the uploaded file and then divides the file into blocks and hash of the data will be computed. When data owner wants to access the data then firstly the fog will access the stored data in decrypted from the Cloud and then merge all the blocks and by decrypting the file we can get the original data. Firstly user has to login to the system with user ID and password given at the time of registration. User can upload the file; the file will be uploaded on the fog node with indexing. At the time of file uploading one part is stored on the cloud server and rest of all stored on cloud server. User can download the document by decrypting the key entered at the time of registration. If the file or document is present on the fog node then it fetch from the cloud node and merged it.

We used AES algorithm for data encryption which is six time faster than triple DES. The time required for data encryption using AES is less than that of DES. Table shows the the encryption and decryption time for both algorithm in milliseconds.

Table I: Algorithm Comparison

Algorithm Comparision		
Sr.No	**Algorithm**	**Encrryption Time(ms)**
Data Encryption	DES	24
	AES	18
Decryption	DES	28
	AES	20

The plot for algorithm comparison is shown in below table.

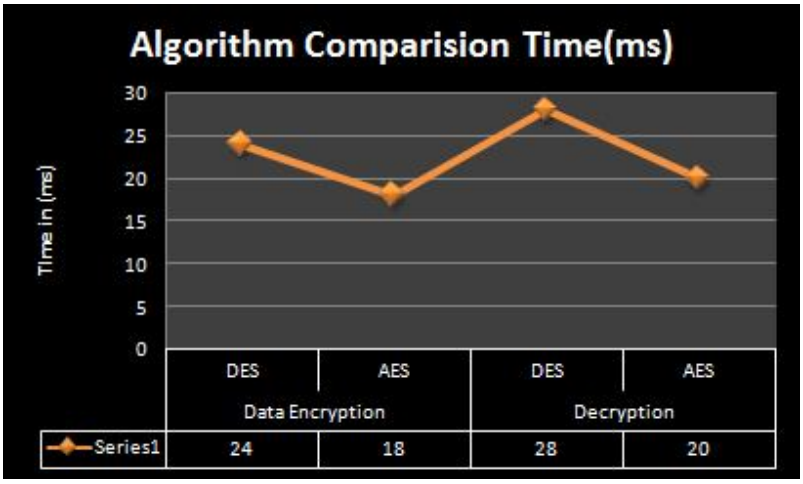

Figure 3: Comparison in terms of Encryption and Decryption

Table II: Algorithm Comparison

The time required for block generation using SHA algorithm is less than that of ECC (Elliptic-curve cryptography) and MD5 (Message Digest) algorithm. The table II gives the time required for each of algorithm in millisecond.

Algorithm Comparision		
Sr.No.	Algorithm	Signature Generation Time(ms)
1	ECC	24
2	MD5	20
3	SHA	15

The graphical representation of the above table which shows that SHA is much more efficient for using has generation is given below

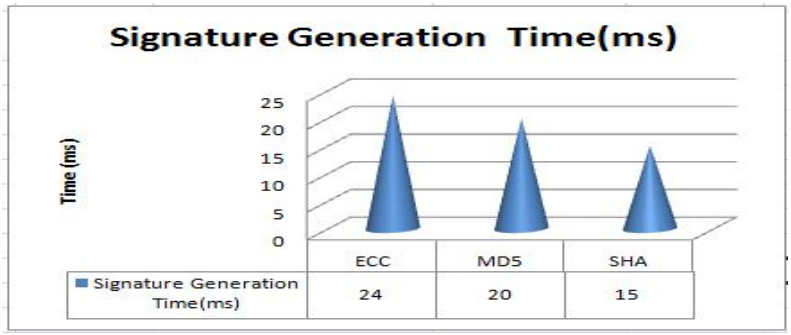

Figure 4: Plot for Signature Generation

VI. CONCLUSION

Existing privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively oppose attack from the inside of the cloud server. Again with the continuous and exponential increase of the number of users and the size of their data. So it is difficult to maintain the integrity of data on the cloud.

We propose a system that provides double security i.e. by using double encryption than the existing system. By analysing the security we can substantiate that our planned proposal is probably protected by encrypting the file twice i.e. one at the time when data owner uploaded the file to the fog node the fog node performs the encryption of the uploaded file and when we forward the data to the cloud on the cloud we again going to perform encryption of the data to make it more secure. Here we used an AES 128 bit for the encryption of the file.

REFERENCES

[1] P. Mell and T. Grance, \The NIST definition of cloud computing," Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50{50, 2009.
[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, \A survey of mobile cloudcom- putin: Architecture, applications, and approaches," Wireless Commun.Mobile Comput., vol. 13, no. 18, pp. 1587{1611, 2013.
[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, \Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments," in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969{2974.
[4] H. Li, W. Sun, F. Li, and B. Wang, \Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397{1409, 2014.
[5] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, \Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130{143.
[6] Q. Hou, Y. Wu, W. Zheng, and G. Yang, \A method on protection of user data privacy in cloud storage platform," J. Comput. Res. Develop., vol. 48, no. 7, pp. 1146{1154, 2011. Department.
[7] Cong Wang, Qian Wang, and Kui Ren,Wenjing Lou,"Privacy-Preserving Public Auditing for Data StorageSecurity in Cloud Computing",2010 IEEE.
[8] Arwa Alrawais ; Abdulrahman Alhothaily ; Chunqiang Hu ; Xiuzhen Cheng ,"Fog Computing for the Internet of Things: Security and Privacy Issues", IEEE Internet Computing (Volume: 21 , Issue: 2 , Mar.-Apr. 2017).
[9] Kanghyo Lee ; Donghyun Kim ; Dongsoo Ha ; Ubaidullah Rajput ; Heekuck Oh ,"On security and privacy issues of fog computing supported Internet of Things environment" ,: 2015 6th International Conference on the Network of the Future (NOF).
[10] Abduljaleel Al-Hasnawi ; Ihab Mohammed ; Ahmed Al-Gburi ,"Performance Evaluation of the Policy Enforcement Fog Module for Protecting Privacy of IoT Data", 2018 IEEE International Conference on Electro/Information Technology (EIT).
[11] Praveen Kumarl, Nabeel Zaidi2 and Tanupriya Choudhur,"Fog Computing: Common Security Issues and Proposed Countermeasures",th International Conference on System Modeling & Advancement in Research Trends, 25th_27'h November, 2016.
[12] S.Rathna1, V.Shanmugavalli2,"A THREE-LAYER PRIVACY PRESERVING CLOUD STORAGE BASED ON COMPUTATIONAL INTELLIGENCE IN FOG COMPUTING",IRJAET 2018.
[13] G. Kulkarni, R.Waghmare, R. Palwe, V.Waykule, H. Bankar, and K. Koli, “Cloud storage architecture,” in Proc. 7th Int. Conf. Telecommun. Syst., Serv., Appl., 2012, pp. 76–81.