Implementation of Fog Computing with Three Layers of Privacy

Prof. Madhuri Gurale [1], Sachin Chikhale[2], Adinath Chitalkar[3], Shantanu Satpute[4], Sachin5

[1](Professor, Dr. D. Y. Patil College of Engineering Pune, Akurdi)

[2345](Students, Dr. D. Y. Patil College of Engineering Pune, Akurdi)

Savitribai Phule Pune University

***Abstract*— This paper presents a fog computing approach to overcome the security issues with the semi-trusted cloud service provider. The existing cloud solution is quite weak that can easily be cracked. As most clients stores sensitive data on the cloud, data security is a major concern that needs to be addressed.**

The proposed system can able to keep the data integrity of the stored data on the cloud for the data owner. By dividing the data into blocks and store some part of the data on the fog node and store the remaining data on the cloud in double encrypted form so the semi-trusted member cannot access the original data. It maintains the privacy of the stored data due to double encryption of the data and also the file is stored in two different locations so if CSP tries to access the file then he cannot get the whole data.

***Keywords*— High Level data security, Double Encryption, SHA512, For Computing, AES Encryption, Data Integrity, Cloud Service Provider.**

I. INTRODUCTION

Due to the exponential growth in data, local machines no longer sufficient to meet the user's needs. Cloud provides a more powerful solution, for large data storage. It works on a pay-per-use model, where users have to only pay for the services they are availing of for a given period. It enhances cost saving as workloads can be shifted from one cloud to other cloud platforms., Organizations or institutes put the sensitive information on the cloud, Despite the advantages, security is the most important concern while storing the data. 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.

To overcome the problems or issues of security, a new technique called fog-computing [1][3][4][9] is evolved. It extends the Cloud platform model by providing computing resources on the edges of a network. Some of the benefits of fog computing like enhanced security [1][2], decreased bandwidth, and reduced latency [9] makes it more secure. Fog computing overcomes the scalability and reliability issues that are there in the traditional IoT-cloud architecture. Fog computing is usually a three-level architecture; that enhances data security accuracy, consistency and reduces the latency rate which is an important factor. Some of the main characteristics of for computing that makes it more advanced compared to cloud computing application are shown in below figure 1[9].

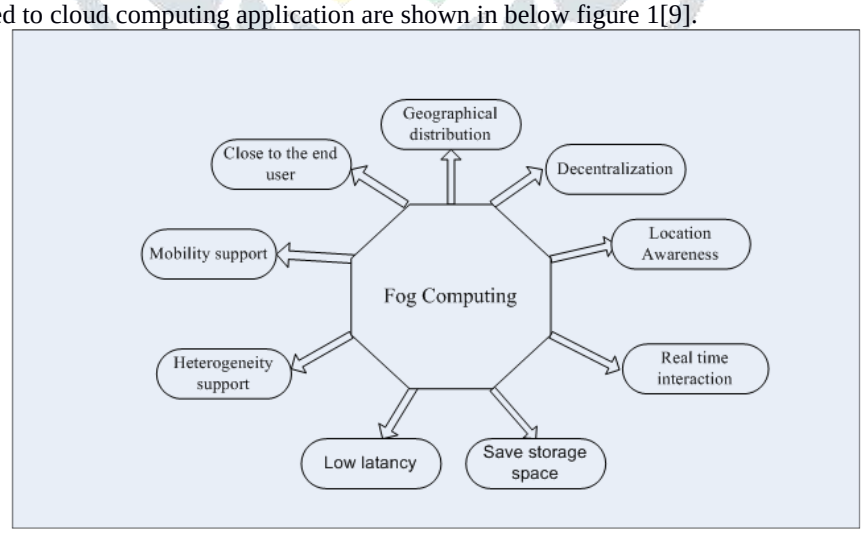

Figure 1: Characteristic of Fog computing

We proposed a solution that uses fog computing to overcome the problem with the semi-trusted cloud service provider. When the user uploads file, it will be uploaded on the fog node, where the encryption of the uploaded file is performed. Then divide the file into blocks and the hash of the data will be computed. And only 5% of data will be stored on the fog device then the remaining 95% of data will be forwarded to the cloud. On the cloud side, we 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. The system provides robust security to personal data and Maintain User data Integrity to the highest levels.

A. Objectives of Proposed System

The objectives of the proposed work are as follows:

- To provides robust security to personal data.
- Maintain User data Integrity to highest levels.
- To protect privacy of user by making data inaccessible to any unauthorized personnel.
- Provide advance security to the data with double encryption technology.

II. LITERATURE SURVEY

There are different types of cryptography techniques used for the privacy and security of the data. Some of the efforts made by the researchers are as follows:
Jonathan Chase et al. [5] 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. [6] 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 the 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 the secure virtual machine is evaluated. In consideration of the privacy of the user's data, the overhead can be tolerated.

Akhilesh Vishwanath et al.[7] introduces AES algorithm in the fog environment. When a user sends data to fog for storing in the cloud, the fog will encrypt the data and send it to the cloud. When the user requests for the data, the encrypted data travels from cloud to fog and fog to end-user and the data will be decrypted at the end-user. In [8] author Ismail Butun highlights the importance and benefits of fog computing for IoT networks. The author tries to provide higher security to these hardware devices.

Sridhar et. al. [9] proposed an intelligent security framework with mutual and double authentication schemes which minimize network cramming. It is effective against quantum attacks and provides better performance by minimizing bandwidth usage. The demerit of this scheme is the authentication provided only to the edge nodes. The intermediate channels are possible to compromise by the various attacks.

Smys S et al.[10] discusses a method to secure the data shared among social networks based on the cloud. Users will encrypt and decrypt data using private and public keys. Then data first send to a proxy server. It will reencrypt data using the AES algorithm. Before sending it to another user it pre-decrypt data. Here group key management is used to provide the public key, private key, and symmetric key to the users and proxy server.

III. PROPOSED SYSTEM

A. System Design

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.

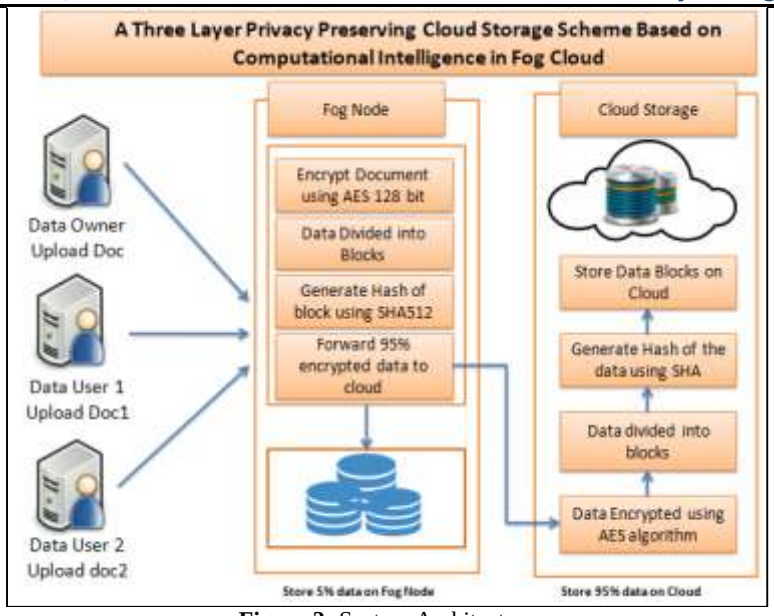

Figure 2: System Architecture

The module wise working of the proposed design is given below:

1. **Proof of Ownership:** Data Owner uploads document, the document will be uploaded on the fog node.
2. **Data Encryption model:** Uploaded file then encrypted using the 16 byte AES key which is entered by the user at the time of Registration.
3. **Data block Generation:** The encrypted file now divided into the blocks. The blocks are of the same size.
4. **Data Block Hash Generation:** The Hash will be computed of the each block. We Maintains the Hash of file data and block of file data as reference and used at the time of downloading. Both the fog and the clouds will follow this step for storing of data.
5. **File merging:** 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.
6. **Serve File to User:** Finally the merged file will be decrypted to achieve the original data and the data will be downloaded on the user browser.

III. ALGORITHMS USED

AES Algorithm

One of the most popular block cipher encryption algorithm is AES (Advanced Encryption Standard) Algorithm. This is used for encryption and decryption of text. AES functions for several time periods by replicating same predefine set of steps.

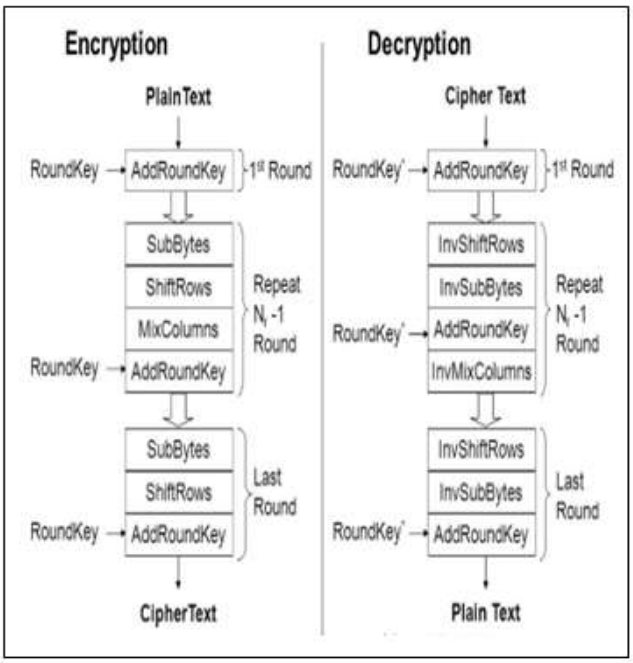

Figure 3: AES Encryption/Decryption

B. SHA 512 Algorithm

The family of cryptographic functions includes SHA (Secure Hash Algorithms) plan for secure data storage.

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

Step 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

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

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

V. EXPERIMENTATION

The systems GUI was designed using java JSP. Core Technologies used were Java, JSP.The overall development was done in the Eclipse Luna and for DB we used MY SQL GUI browser. The database basically used for storing user details like User name, user identity, keyset. The tool used for db functionalities was MYSQL GUI Browser.

A. RESULT EVALUATION

This study makes use of a 16 byte AES algorithm for data encryption. We used the AES algorithm for data encryption which is six times faster than triple DES. The time required for data encryption using AES is less than that of DES. The table shows the encryption and decryption time for both algorithms 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.

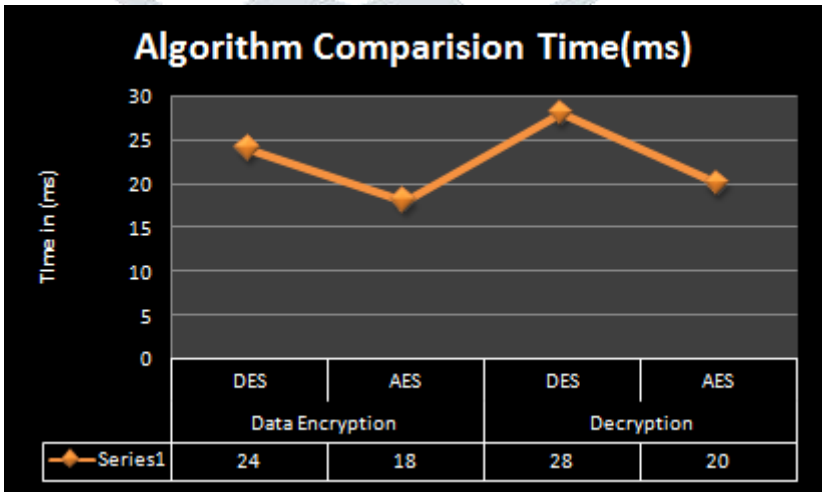

Figure 3: Comparison in terms of Encryption and Decryption

B. PROJECT SCERRENSHOTS

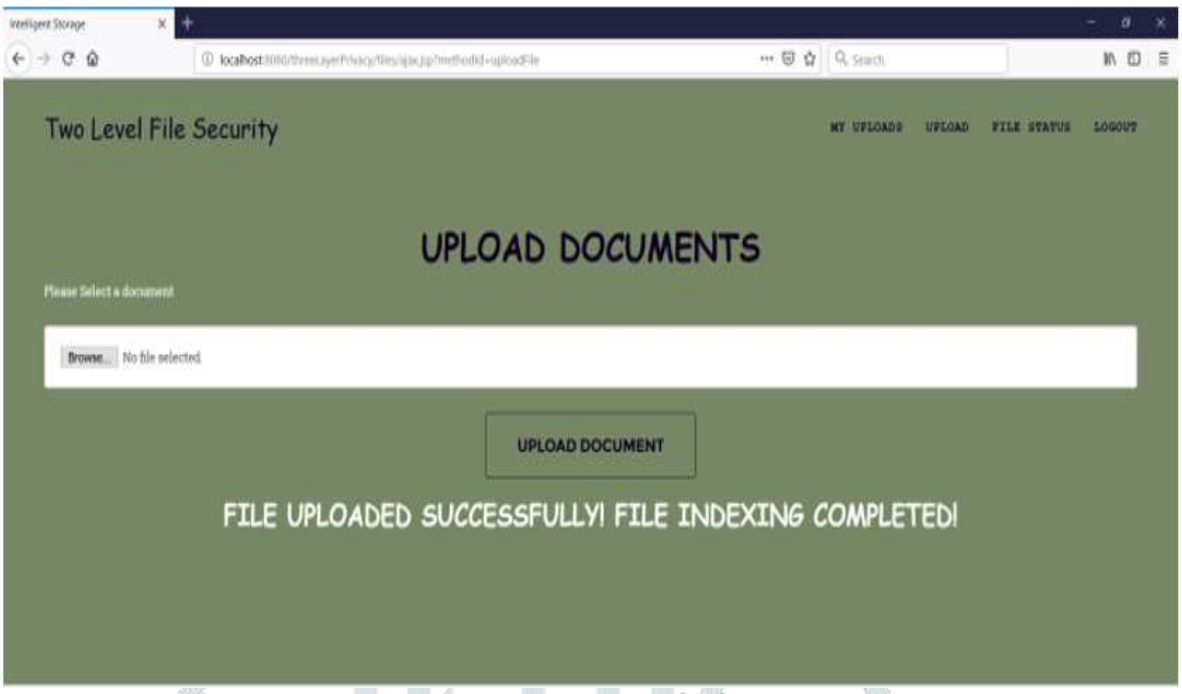

Figure 4: Document Uploading

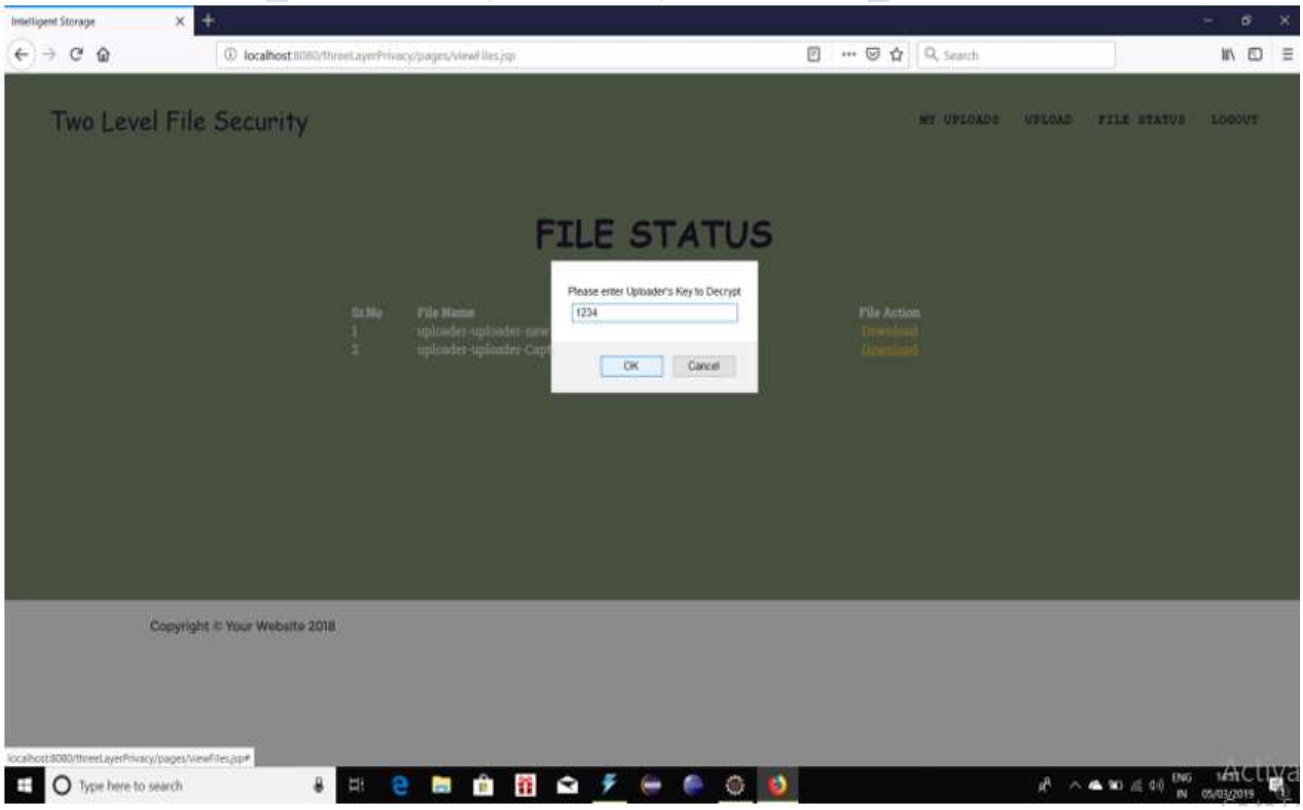

Figure 5: Document Downloading

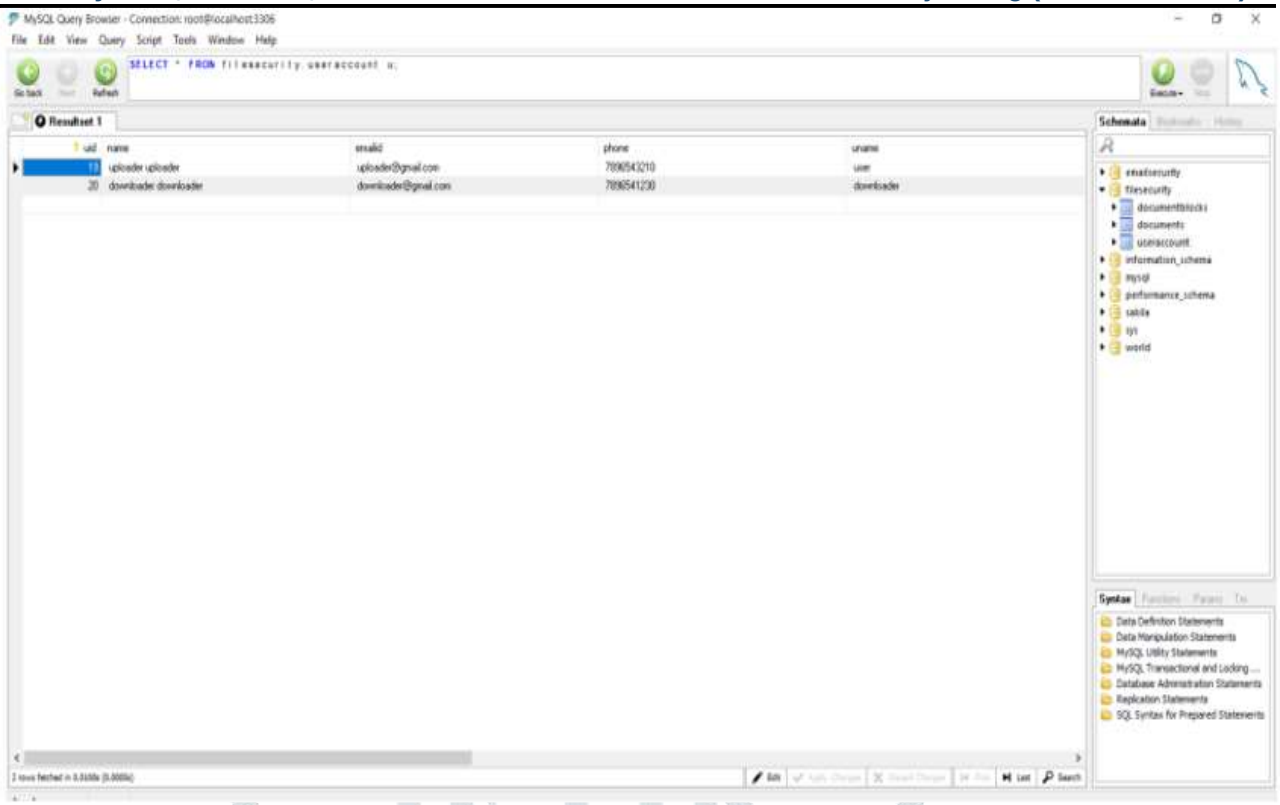

Figure 6: Database Fog Server

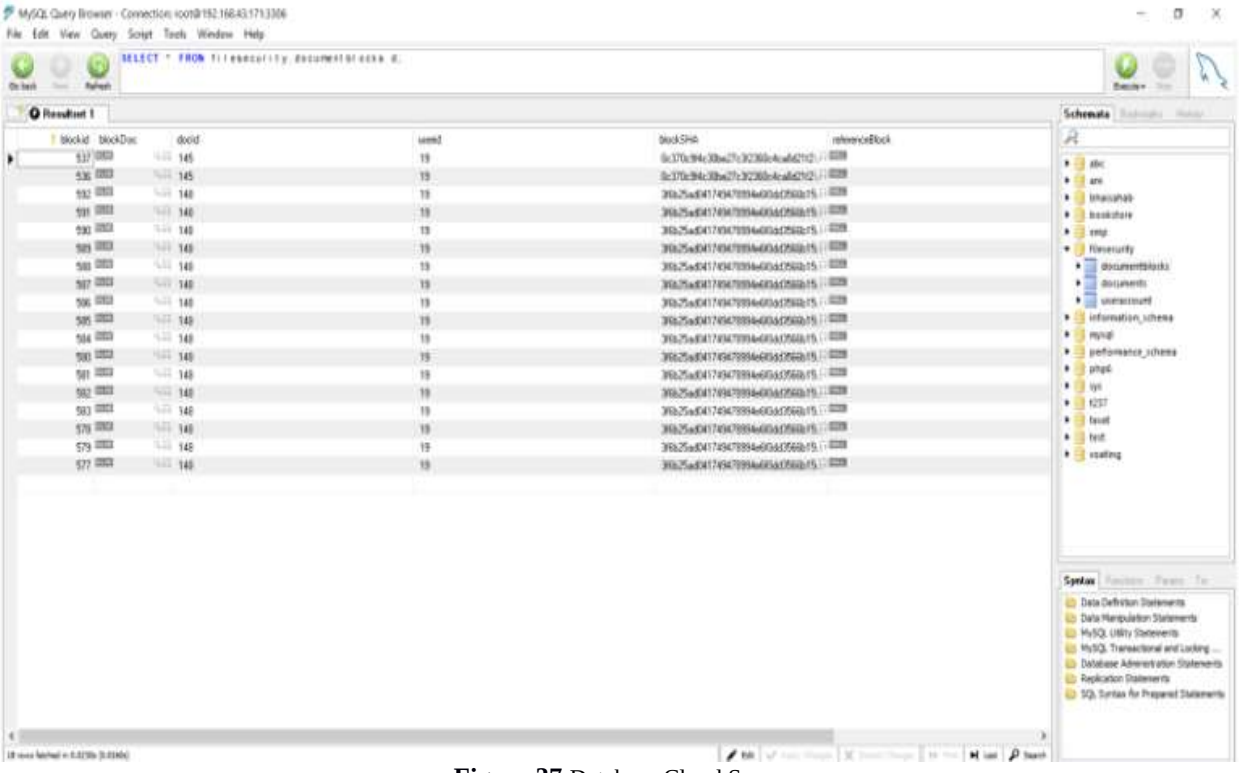

Figure 37 Database Cloud Server

VI. CONCLUSION

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 the data owner uploaded the file to 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] Yumnam Winnie , Umamaheswari E , D M Ajay, ,"ENHANCING DATA SECURITY IN IoT HEALTHCARE SERVICES USING FOG COMPUTING", 2018 IEEE.

[2] 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).

[3] 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).
[4] 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).
[5] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, \Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud comput- ing environments," in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969{2974.
[6] 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.
[7] Akhilesh Vishwanath , Ramya Peruri , Jing (Selena) He ,"Security in Fog Computing through Encryption", I.J. Information Technology and Computer Science, 2016, 5, 28-36.
[8] Ismail Butun, Alparslan Sari , and Patrik Österberg"Hardware Security of Fog End-Devices for the Internet of Thing",www.mdpi.com/journal/sensors,2020.
[9] Sridhar, S., and S. Smys. "Intelligent security framework for iot devices cryptography based end-to-end security architecture." In 2017 International Conference on Inventive Systems and Control (ICISC), pp. 1-5. IEEE, 2017.
[10] Praveena A, Smys S, "Ensuring data security in cloud based social networks", IEEE International conference of Electronics, Communication and Aerospace Technology (ICECA), Vol. 2, pp. 289-295, 2017.