European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 08, 2020

Enhancing Data Security In Cloud Using Cryptographic Technique

Shrihari M R [1], Noorain Fathima [2], Pooja P [3], Revathi G [4], Veenalahari M [5]

[1]Assistant Professor, [2345]Student,
[1] Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India
[2]Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India
[3] Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India
[4] Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India
[5] Dept. of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India

[1]shrihari.mr@gmail.com, [2]noorainfathima181198@gmail.com,
[4]revathi301998@gmail.com

Abstract
In these days, storing data over the cloud has become popular. Many organizations and companies have moved to the cloud and they are continuously benefiting from its rising usefulness and convenience. Before the cloud, saving documents or information was simple. All we had to do is save them on our computer or an external hard drive but the information could not be accessible from anywhere which was resolved by cloud storage. Every process has its own pros and cons. Similarly, storing data in the cloud has many pros but is not without cons. Data could still be accessed by cybercriminals using complicated approaches, even though storing data on cloud is safe. That is the reason why every person should be cautious of their own data or information; else their information could be in the hands of data stealers who might disclose the data, if best practices are not applied. In organizations, if employees are not taught or well-informed, data can accessed by attacker. Therefore, this paper discusses about making use of symmetric block cipher technique i.e., AES algorithm in the fog node for the data to be stored oncloud.

Keywords— Advanced Encryption Standard, fog node, symmetric block cipher technique

1. INTRODUCTION

In this humankind, where we reside in, inventions and advancements are continuous change and in terms of technology, more or less all the data is stored on cloud. The numbers of documents being uploaded on cloud are escalating in an exponential pace. Security for the info may be a major problem. So as to beat the matter, Fog Computing methodology was set forth. The prototype which broadens the cloud computing objectives is referred to as Fog computing. Fog basically behaves like an intermediate film between the cloud server and the facts or figures that has to be safely stored. It is not the absolute substitution to cloud; rather it harmonizes with the features of cloud. Fog functions nearer to the data that has to be uploaded and provides computing resources to that particular files or folders. Fog computing overcomes the scalability and reliability factors which are present within the conventional cloud design. Since Fog nodes works at the sting region and it also improves various crucial aspects of securing information like the safeguarding of the data, accuracy, and appropriateness and reduces the latency rate. Also interestingly, because on the whole, bandwidth to cloud is saved, therefore better quality of service (QoS) isachieved.

About FogComputing:

The structural design which makes use of edge devicesto bring out significant quantity of data processing, computation, storage capacity, and quick real time responses/feedback is called fogging. Fog node supports the Internet of Things (IoT) concept, where most of the devices will be connected to each other through which clients can secure theirdata.

Examples:
industrial controllers, wearable health monitoring devices, switches, connected vehicle, electronic gadgets like phones, cameras, computer systems, routers and video surveillance devices.
The fog node is closer to edge devices and has broader distribution of patterns. The device with data processing, capability of holding and securing huge amount of data with networking capabilities is called a fog node. Centralized framework and dispersed decentralized framework is the principal dissimilarity among fog computing and cloudcomputing

Positives and Negatives of Fog Computing Positives:

- As fog is geographically nearer to the data or info that has to be securely stored, it provisions lowlatency.
- Due to multiple interconnected channels the loss of connection isimpossible
- It provides high security and good userexperience

Negatives:

- As we are adding additional layer the system iscomplicated.
- The edge devices cause additionalexpenses.
- It provides limited scalability compared tocloud.

2. Literature review

- The Cloud refers to servers that are accessed over the internet. Cloud provides services like data storage which means the data of the owner is controlled by the third party from which the users can store the data and access the data [1]. Security of that data becomes a threat so the data which is storing in the cloud will be encrypted using blowfish technique and stored so that it will not be visible to the users but plain text based search algorithms cannot be used[1]. The main challenge here is data spill or data breaching. Blowfish encryption techniques have the draw back of that finding the data from file, the whole file has to be decrypted and time taking process.
- For the effective utilization of cloud services there should be a secure communication channel and a secure data exchange. We use RSA algorithm for encrypting together with digital signature for user authentication [2]. RSA goes slows where a huge amount of data have to be encrypted by the same computer and also it requires a third party to verify the readability of public keys and data can also get compromised by middle manattack[2].
- There are severe security challenges in storing the data that has collected from the IoT, cloud, fog. Fog nodes and fog instance which would communicate both physically and virtually with the decentralized cloud data centers and physical sensors [6]. It uses fog computing together with cloud and maintains a decoy system to trap the attacker [6]. In decoy system the attacker will be given duplicate data and he will be confused by the security challenge, drawback is that he can predict the appropriate choice during login and Large working parameters, controversial setting of master keys in the cryptographictechniques.
- As cloud stores a very huge amount of data and is scalable, flexible but the computational time required in retrieving the data from the cloud is high so fog computing reduces the burden on cloud .As per security issue the data will be encrypted in fog and stored [4]. And it provides real time computation. A fog node response quickly as it is very near to edge devices when compared to cloud [4]. Fog is not as scalable as cloud. Creating duplicate data information and setting it beside the original information is highlycomplicated.
- Fog computing is used in health care. It uses IoT sensors or smartphones to trace the health

status of a patient. It is the additional layer of the cloud that extends cloud services, which is closer to edge devices so that time taken to response is less [5]. Fog enables the patients to communicate easily as their record would b maintained at fog and easily retrieved and treat patients [5].

3. Proposed system

A three tier architecture model is been made use in the proposed system. In this model the first level consists of user who uploads or downloads required data which may be structured, semi structured or unstructured, the second level consists of fog node where encryption and decryption of user data takes place, the third level is the cloud where the encrypted data is stored securely.

As shown in Figure 1, initially the user uploads the data to the Fog node this data is the original data which is in the form of plain text, at fog node Advanced Encryption Standard (AES) algorithm is implemented which is a symmetric block cipher technique. The fog node after receiving the user data it encrypts the plain text using AES algorithm with a secret key which is of size of 512 bit. Same secret key is used for both encryption and decryption. After encrypting the data the fog node uploads cipher text to the cloud. The cloud receives the cipher text and stores it. As the data at the cloud is in encrypted form though the attacker retrieves the data he is provided with the cipher text but not the original data. Similarly whenever the user tries to retrieve the data from the cloud the user enters the file name, which is sent to fog, later fog retrieves the required file from the cloud. The cloud sends the file in the encrypted form to the fog where the file is decrypted using the same secret key that was used to encrypt the file. After decryption the original file is sent back to the user.

4. Implementation

The main focus is on the organization's data which is used by large number of users. The security to this data is provided using AES algorithm. The block diagram for an AES algorithm is provided in Figure 2.

AESalgorithm:

In AES both encryption and decryption operations are performed using four steps where the plain text is divided into 16-byte block and it is exhibited in 4x4 matrixes.

The four steps in which the AES operation is performed are:

- **ByteSubstitution:**
  Here, the input which is of 16 bytes is replaced using the lookup table which is known as S-box.

- **ShiftRows:** In this step each and every row of the matrix is shifted towards left cell of a row. The shifting pattern is as bellow:
  - The first row of the matrix isunchanged.
  - The second row will be moved towards left cell by oneposition.
  - The third row will be moved towards left cell by twopositions.
  - The fourth row will be moved towards left cell by threepositions.

The result of this operation is a new 4x4 matrix which consists of same elements but in different position. This result is given as an input to the further process.

Column Mix:

This step makes use of a mathematical technique which transforms the 4 bytes of data in a column to completely new bytes of data. As a result a new matrix will be generated this consists of new 16 bytes

Add Round Key:
This is the last step in AES algorithm, it makes use of the results of previous matrix i.e. the new 16 byte matrix which is then XORed with 512bits of round key. The final XORed value results in the cipher text. In this way AES operates during encryption. Similarly during decryption process AES operates on substitution and permutation network where each step is invertible.

PROJECT MODULE

1. **UserModule:**
The user module enables the user to register and login. While registration the user has to provide all the required information and the given information is validated to check whether the given information is right or not. Once the user is registered he can successfully login using correct user name and password. The user module enables the user to upload the required file to fog node and also can send the file name to fog to retrieve the requiredfile.

2. **Fog Node Module**:
User uploads the file to fog node where these files are encrypted to provide security to the data. The fog node makes use of RSA algorithm with a key size of 512 bit to encrypt the file. After the encryption process the fog node will upload the encrypted file to cloud. Similarly whenever the fog node receives a file name from the user to retrieve it, the fog node will fetch the file from the cloud and decrypts the file using the RSA algorithm. After decryption the original file is sent back to the user. Same secret key is used for both encryption and decryption at Fog node.

3. **CloudModule:**
The cloud receives the encrypted files from the fog node. These files are securely stored in the cloud for further computation. The user can view all the files that are stored in the cloud, the files are in the encrypted form. Whenever user requests for a file the fog requests the cloud to provide the requested file. The cloud sends the requested file which is in the encrypted form to the fog node. The fog node decrypts it and sends it to the user who is requesting for the particular file.

Encrypting File at FogNode:
During encryption process the flow of data across different nodes in the system can be demonstrated as follows, In this project initially the user enters user ID and password to store his data, this will be verified in the user database if it is valid then the user will be authenticated and sends a status message to the user. The user then has to upload his file to fog node .So a file ID will be generated to the file that has to be uploaded. The file ID will be used to fetch the required file from file database and then it is uploaded to the fognode. Asecret key is generated to encrypt the fileinfognode. This secret key isused to encrypt the file. For Encryption AES algorithm is used with a key size of 512 bits. The encrypted file is then stored in the cloud along with the file ID and user ID, then a status message is sent to the user. The dataflow diagram for file encryption as shown Figure 3.

Decrypting File at FogNode:

During decryption, initially the user enters user ID and password to get authenticated .If the user ID and password is valid he will be authenticated status message is sent to the user where he will be authorized to retrieve required data, User enters the file name and sends it to fog where a file ID corresponding filename will be retrieved from the file database. The file ID along with user id will be sent to cloud to fetch required file. At cloud the required file will be searched and then file is sent to fog node. At Fog layer the received file will be decrypted using AES algorithm and same Secret key which was used to encrypt the file. After decryption the decrypted file will be sent to the user .This file now contains data in the form of plain text. In this way security for the data is provided using AES algorithm. The dataflow diagram for file decryption as shown in

Figure 4.

After encrypting the data using AES algorithm, the cipher text has to be stored on any cloud platform. A Cloud Service Provider (CSP), known as DriverHQ is been used to store the data. The entire coding for encryption and decryption of AES Algorithm is done in Java Programming language by making use of packages.

5. Results

Initially the owner has to login, the owner page enables the owner to perform certain operations which is as shown in Figure 6. The owner has to enter the name of the file which has to be uploaded, if the file name already exists then a message called file name already exists will be displayed as shown in Figure 7. If the file is uploaded successfully then a message such as file uploaded successfully will be displayed on the screen as shown in Figure 8. The Owner uploads the file to fog node, the fog node home page as shown in Fig-9. The file uploaded to the cloud is stored in the encrypted form as shown in Figure 10. AS the file is encrypted and then stored the cloud, though if it is been accessed by a wrong person or an attacker, he cannot get the exact data. Because the data is secured by encrypting it using AES algorithm with a key size of 512 bit as shown in Figure 10. The encrypted files can be viewed at cloud where we can see data in encrypted form, the original data is not visible. The person who is viewing the file can see only cipher data.

Performance analysis:

It is carried out to check the time taken for encrypting and decrypting the files at fog node. As shown in Fig-11, it is the performance graph which is plotted for file size in KB against time in ms, it shows the time taken for both encrypting and decrypting the file. Time taken to decrypt a file is more than time taken to encrypt a file.

6. Discussion

This enables to provide good security to the files that are stored and processed at cloud. Previously the security was provided by encrypting the file with a key size of 128 bit or 256 bit. In this project a 512 bit key size is been made use, which is extremely large when compared to 256 bit and 128 bit key size. So it is very difficult for an attacker to identify the exact secret key that is been used to encrypt the file that is stored on cloud. Along with this a fog node is added which reduces the latency and provides quick accessto the user files. This ends up by providing a good user experience. Only fog node without a good encryption technique or a good encryption technique without a fog node may not be a good idea. As both of these concepts are combined here it enables a highly secured transmission between the user and cloud.

AES Algorithm

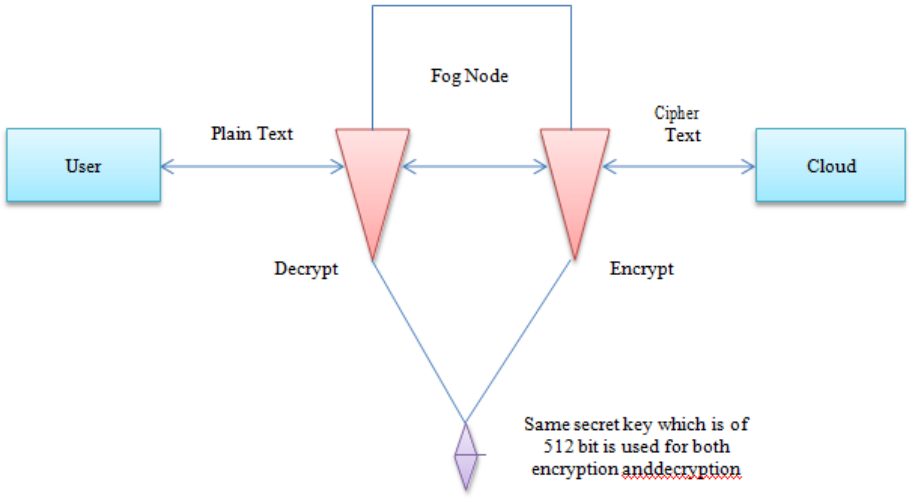


Figure 1. Proposed SystemArchitecture

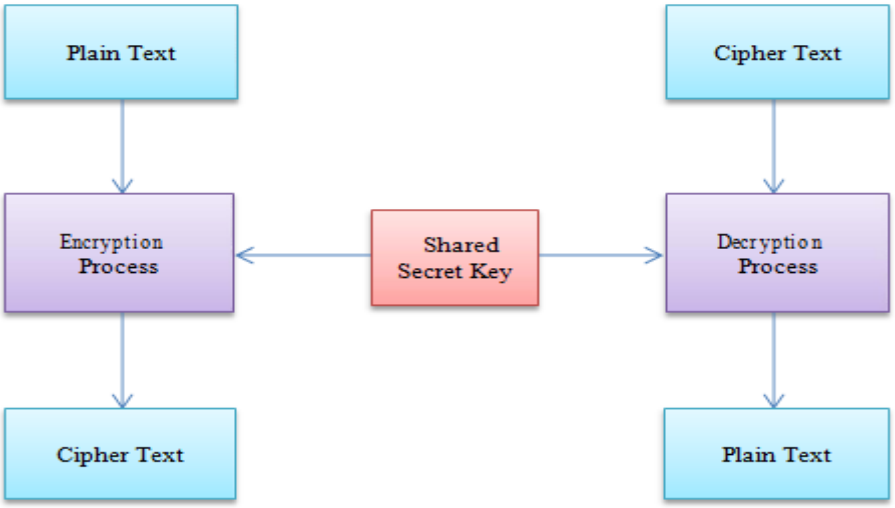


Figure 2. Block diagram for AES algorithm.

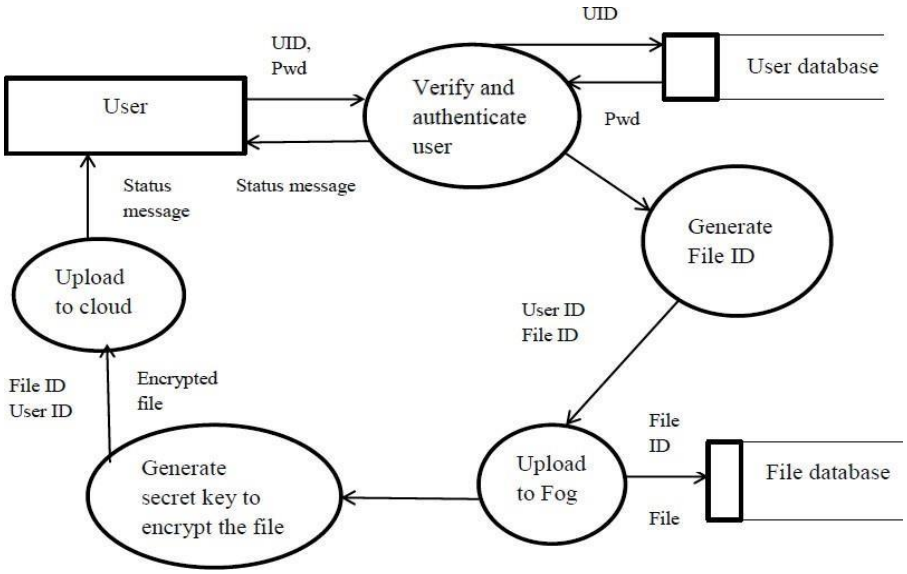


Figure 3. Dataflow Diagram for File Encryption

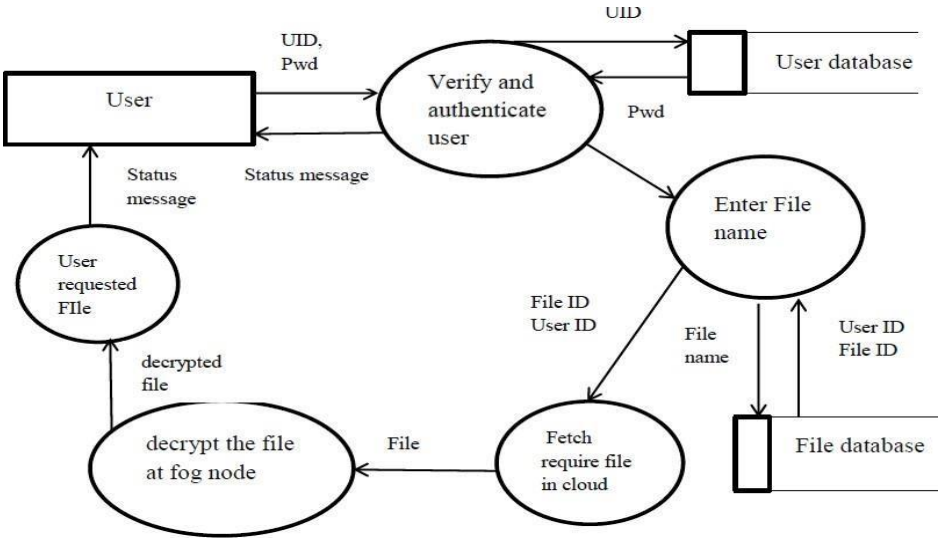


Figure 4. Dataflow Diagram for File Decryption

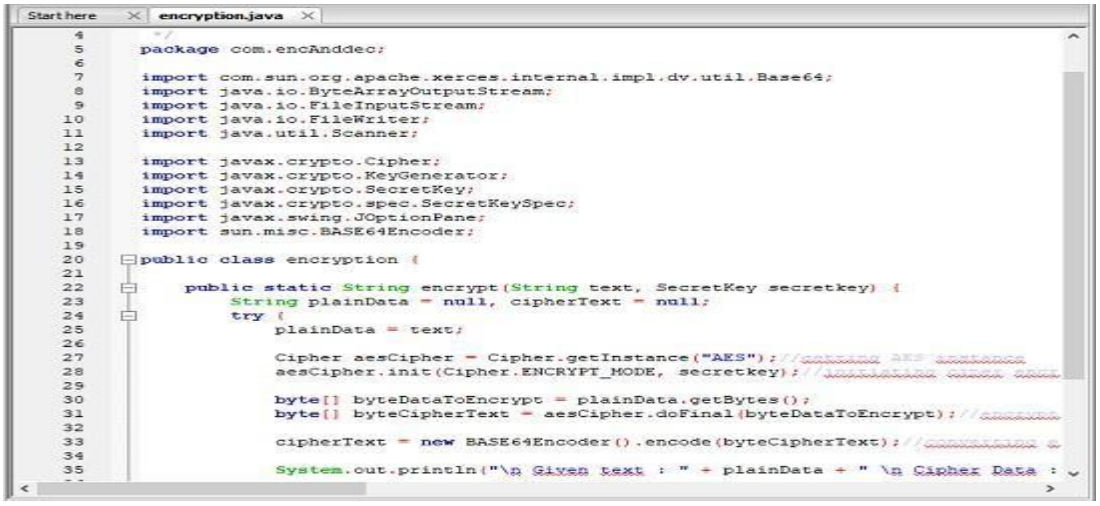


Figure 5.Coding inJava

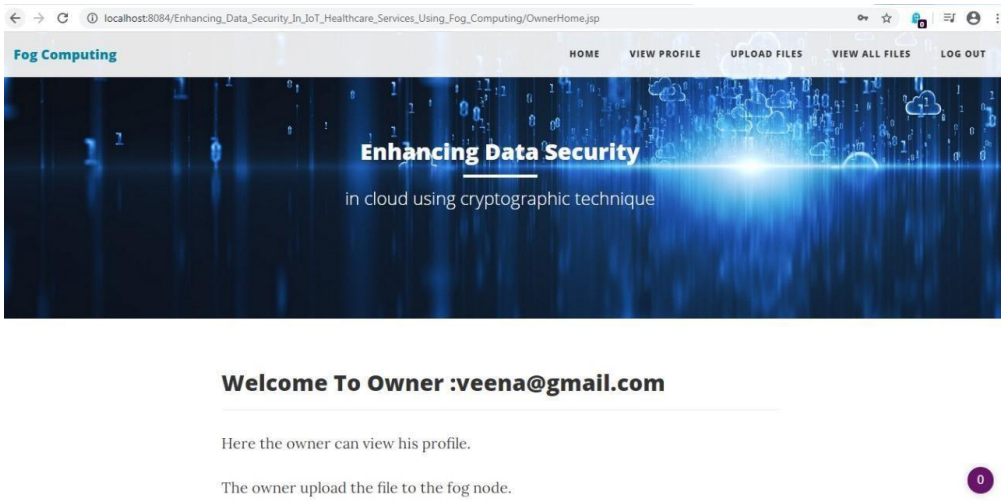
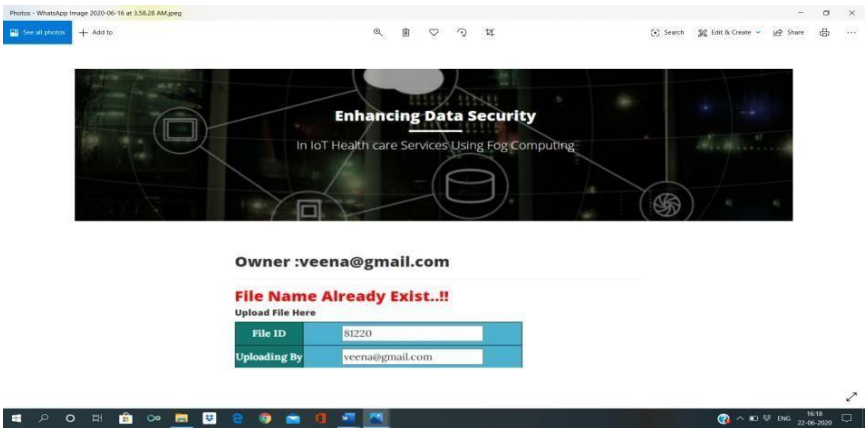


Figure 6. Owner Login Page



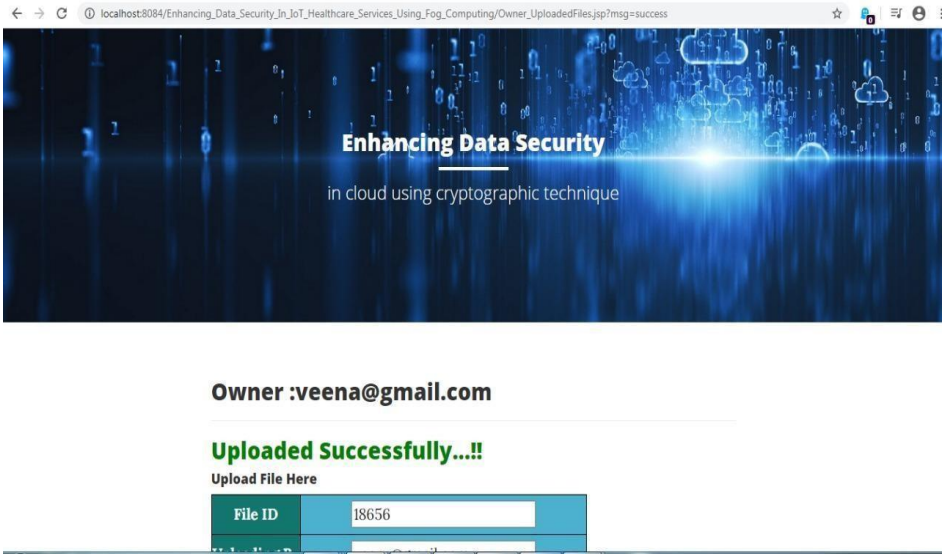


Figure 7. Check whether the file name already Exist

Figure 8. File successfully uploaded to Fog Node by Owner

Figure 9. Fog Home Page

Figure 10. Cipher data of a file after encrypting it with key size of 512 bit at fog node

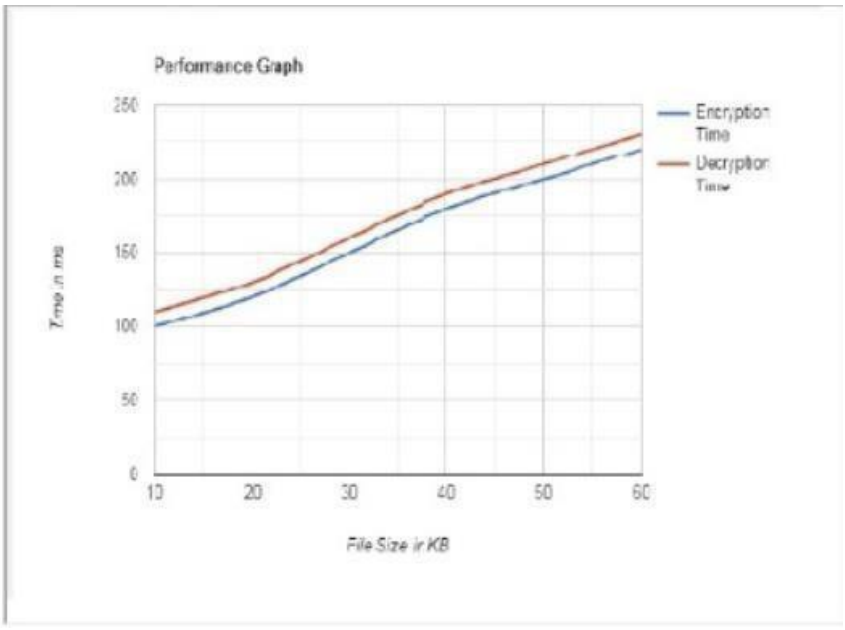


Figure 11. Performance analysis Graph

7. CONCLUSION AND FUTURE ENHANCEMENT

Diverse institutions, companies deal with large amount of information daily which has to be secured and stored somewhere. We can do this by encrypting the information in the fog node and then store it in cloud. This increases high security to the information that is stored in cloud .Also, by introducing fog as a middle layer, it provides quick access to the user's information. Such that high data security is provided along with which the latency rate is been reduced. The confidential data of any organization can be secured with this technique. The precision, consistency and uniformity of facts and figures can be enhanced in future which enables to progress the performance of the cloud and in addition offer good computational efficiency.

REFERENCES

[1] A Venkatesh, Marrynal S Eastaff, "A study of data storage security issues in cloud computing ",International Journal of Scientific Research in Computer Science ,Engineering and InformationTechnology-2018.

[2] Sudhansu Ranjam Lenka, Biswaranjan Nayak, "Enhancing data security in cloud computing using RSA encryption and MD5 algorithm", International Journal of Computer Science Trends andTechnology,June-2014.

[3] Hadeal Abdulaziz Al Hamid, Sk Md Mizanur Rahman, M.Shamim Hossain, Ahmad Almogren, Atif Alamri "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography", Information Science Department ,King SaudUniversity,September-2017.

[4] Sirisha Sanatha , Swathi Amancha,"An enhanced cloud storage method :fogcomputing"-2018.

[5] A George, H Dhanasekaran, J.P Chittiappa,"Internet of things in health care using fog computing",2018 IEEE island systems, applications and technologyconference-2018.

[6] Issac Odun-Ayo ,Olasupo Ajayi,Boladele Akanle,"An overview of data storage in cloud computing", International conference on next generation computing and informationsystems,Dec-2017.

[7] Mayank Kumar Kundalwal, Ashish Singh, Kakali Chatterjee,"A privacy framework in cloud computing for healthcare data", International Conference on Advances in computing, communication control and networking"2018.

[8] Sudhansu Ranjan Lenka, Biswaranjan Nayak, " Enhancing Data Security in Cloud Computing Using RSAEncryption

[9] ",International Journal od Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3 , June-2014.

[10] M.Aathishvar , N.Madhan Kumar , K.Ganesh, "Study on Cloud Computing " International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) Volume 4, Issue 1 (January'2018).

[11] R.Aishwarya, R.Divya Ms D Sangeetha , Dr V.Vaidchi,"Harnessing healthcare data security in cloud", International conference on recent trends in information technology (ICRTIT)-2013.