Data Security Using Key Rotations In Cloud System

Prof. Archana Said (Asst. Prof.), Jagruti S. Dambre, Tejswini G. Divekar, Shital Gharjale, Pooja Jadhav
Department of Computer Engineering
AISSM'S Institute of Information Technology, Savitribai Phule Pune University, Pune-01

Abstract - In existing systems there was lot of overheads for computing security tasks like data storage and encryption and decryption of data files. Which was more time consuming for processing of data in cloud environment. This is the main disadvantage of these system. In addition there was no provision for controlling the data by data owner. Again for verification of attributes with their own data is also having more computational and storage overheads. We proposed a system which addresses these previous security threats, We design data encryption technique for individual data blocks with key rotation using 256 bit symmetric key. In addition data users can request and do operations on their data like insert, update, delete etc. very efficiently. We are using the two main algorithms Advanced Encryption Standard (AES) and hashing algorithm (SHA1) .These two algorithms are used for data security.AES algorithm is used for the data encryption/decryption and SHA1 is used for hashing. we are designing three separate modules that are Trusted Third Party Auditor ,Cloud Service Provider and Data Owner . By using these three modules, we are achieving the phenomenon result that is secure data retrieval in cloud systems using Key Rotation. In our system there is provision for securing the file access if two clients are connected in LAN network that means files are not sharable among the multiple clients and the authorized user having access for those files for particular time span only which is allocated to him or her.

Keywords: data storage; encryption and decryption of data; data owner; verification of attributes;third party auditor; cloud service provider,AES algorithm, SHA1 Algorithm .

I. INTRODUCTION

In cloud computing environment vast number of resources like hardware and software are provided by cloud for efficiently managing the data. By storing the our data in the cloud system, The control of data will be decreased by cloud environment for data owner. There is very advantages for securing data in the cloud, by maintaining control in rest of network. This greatly reduces control of data for data owner or user.

For securing data in the cloud, access control policies are imposed, authentication and encryption of data is done, integrity verification and masking of data are all data protection techniques used. Cryptography is the data protection machanism for data security in cloud . This includes encryption and decryption algorithms. In symmetric cryptography, before outsourcing data to cloud server plain text is encrypted into cipher text using secret key and later user decrypt using same shared secret key. In this user encrypts the data with their private secret key and uploads to the cloud. And after downloading data, data is decrypted using same secret key. Thus, using symmetric key cryptography.

Authentication of data is a secure way to protect the data using key management ,when data is passed from user to cloud server. In our proposed system to address these data security threats, we encrypt sensitive individusal data blocks using key rotation with 256 bit symmetric key. In addition, users can request for data and do manipulations on there data like insert, update and delete etc from cloud .In this system, we are designing three separate modules viz Trusted third party auditor(TTP),cloud service provider(CSP) and data owner. We used Advanced encryption algorithm(AES) for encryption of data.

When authorized user request data , he sends request to both TTP and CSP.TTP is responsible for calculating hash values for data blocks and CSP is responsible for storage of encrypted files. When user downloads files from CSP and gets hash values from TTP he decrypts the data blocks using same secret key.

In our system there is provision for securing the files access if two clients are connected in LAN network that means files are not sharable among the multiple clients. The authorized user can have access for files for particular time span only which is allocated to him or her by the data owner.

II. SYSTEM MODEL

In our proposed system there is one cloud server, Data owner, Trusted Auditor, and Authorized user. The following steps shows the flow of overall system.

1. Data owner sends the encrypted data and key to the Third Party Which is Trusted Auditor (TA).

2. Then TA calculates the hash value of encrypted file and sends encrypted file, BST(Block Status Table) to the cloud server.
3. Authorized user sends data request to the TTPA and Cloud server.
4. TTPA verifies the user whether he is authorized or not then send verified signal to the cloud server.
5. After verifying user TTPA sends the hash value of that encrypted file to the requested authorized user.
6. Cloud server sends the encrypted file and BST of that file to the requested authorized user.
7. After receiving BST and encrypted file from cloud server, authorized user calculates hash value of it.
8. After that it matches this hash value with TTP's hash value. If both are equal then authorized user will get decryption key to decrypt data or file.

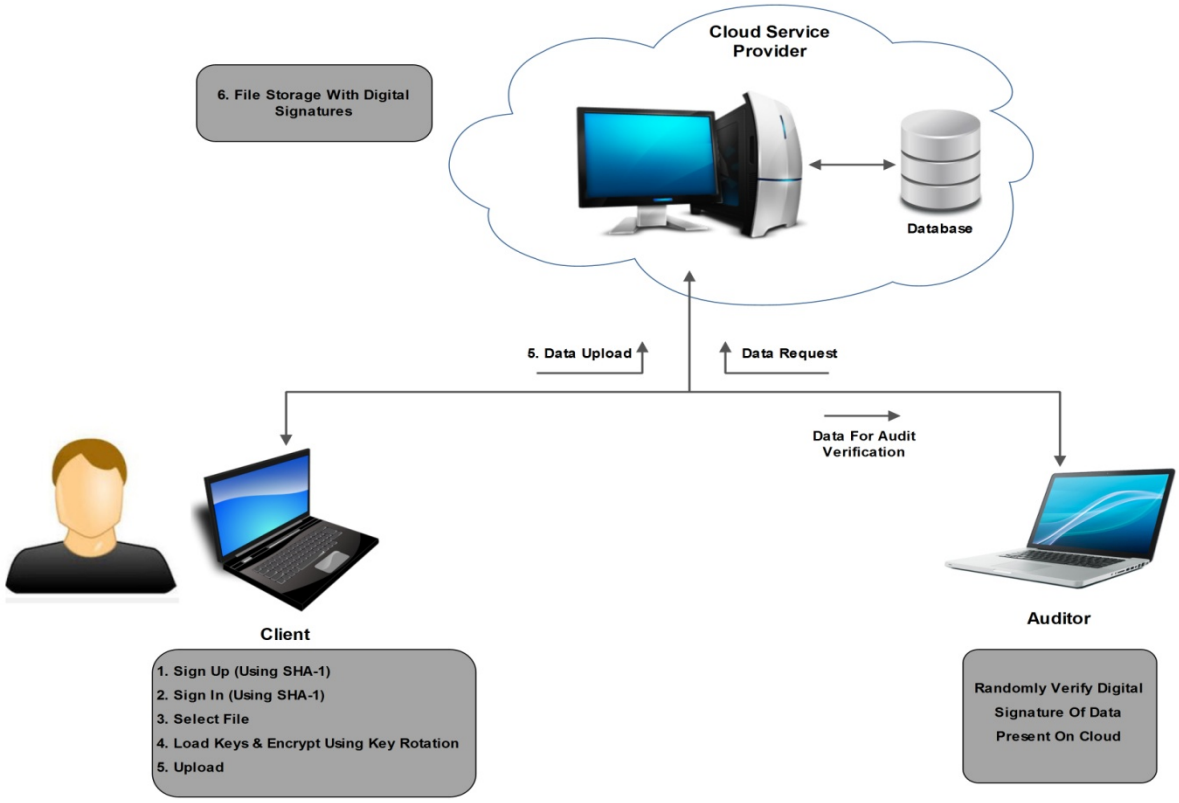


Fig: Overall System Model The above figure shows the overall system model.

In above figure client may be either Data Owner or Authorized user. If user wants to upload some data on cloud then he or she will be Data Owner of that File.

And If user wants to retrieve or download data from cloud server then that user will be authorized user.

III. PREVIOUS WORK

Prakash G L, Dr. Manish Prateek and Dr. Inder singh, et al[2], has proposed outsourcing data in cloud computing to generate incremental scope of hardware and software resources. To protect outsourced data is a major challenge in cloud computing for data security. In these method there is no provision for that the Authorized user can retrieve the data in given time period which is allocated by Data owner.

Jing-Jang Hwang, Yi-Chang Hsu,Taoyuan,Chien-Hsing Wu et al [3], has proposed A business model for cloud computing based on separate encryption and decryption service. In this system cloud service provider is responsible for all the tasks related to data encryption /decryption and storage. Which requires lot of computational overhead for process of data in cloud server. The main drawback of this system is data owner is dependent on cloud service provider. And in this data owner is completely dependent on cloud service provider.

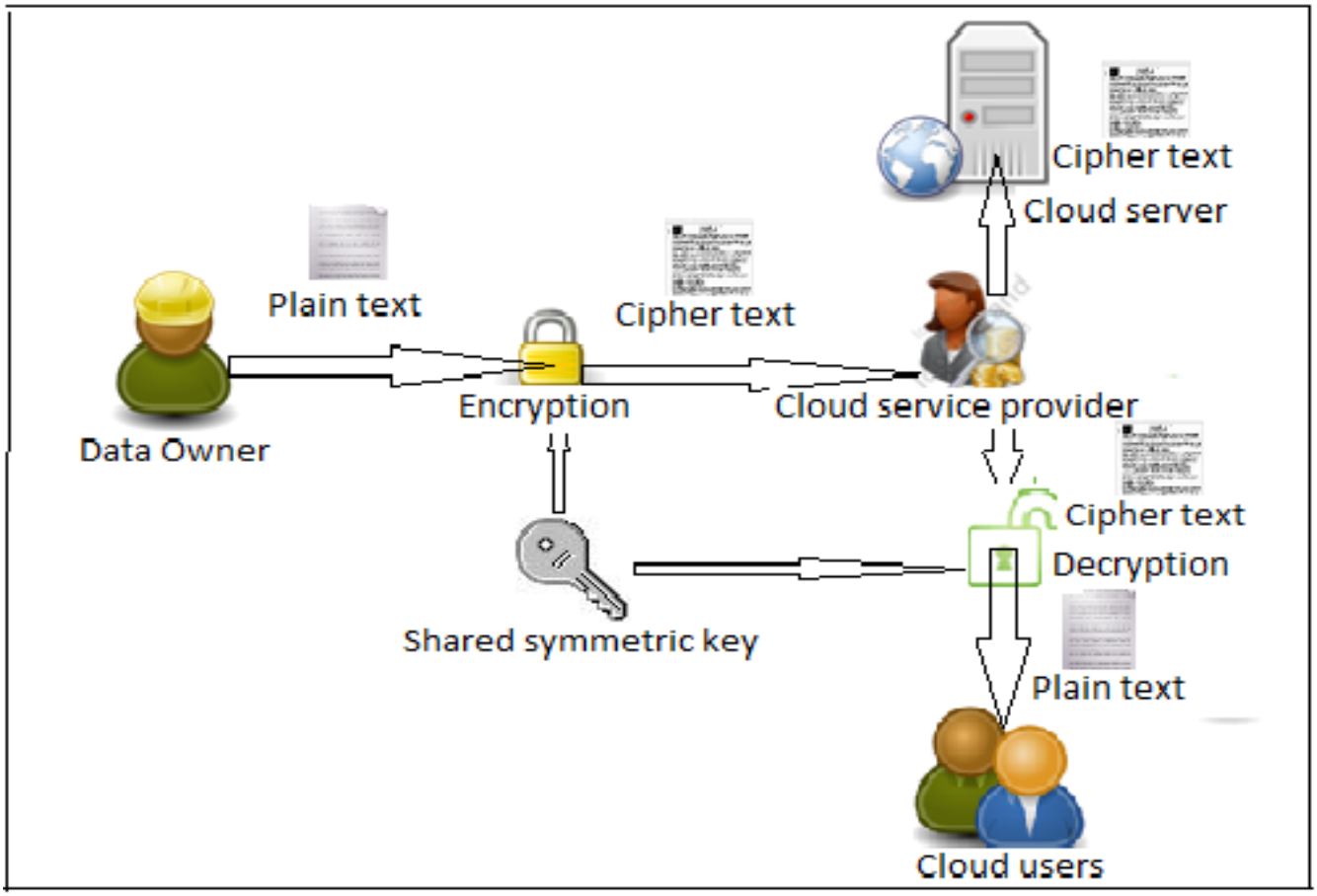


Fig: Block Diagram of Data Encryption and decryption in cloud system.

Junzuo Lai, Deng R H, Chaowen Guan, Jian Weng et al [4] , has propose a model Attribute-Based Encryption With Verifiable Outsourced Decryption to provide data security in cloud system . They have design decryption algorithm which is based on the user requested attributes. Which requires lot of computational overhead for verification of user attributes with the encrypted data. The main disadvantage of this system is that it has less efficiency. To overcome this problem we are adding Trusted Third Party Auditor .That reduces storage, computational overhead of the cloud server. So our system is more efficient.

IV. PROPOSED METHODOLOGY

Key Character(KC): In this step, the subkey is added with the each state. For each round, from the main key subkey is derived using Rijndael's keys schedule. subkey size is same as state. The subkey is added by
combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

Array Inversion (Al): The Array Inversion process is done for high degree of security.Inversion of cicular array is done based on processing of adjacent key characters . if the addition of ASCII values of these key characters is even then circular array is inverted.
Let CA is circular array, block character is ci and Xi be the key character, then Inverted CA is

$$IA=\sim IA \text{ iff } Xi+Xi-1\%2=0$$

Array Shifter (AS): In this , the circular Array is shifted/rotated. shifting of circular array is based on the addition of two key characters. If the result is a factor of 5 then shift circular array by 2 else it is shifted by summation mod 5.

$$AS= CA >>>(2 |(Xi+Xj)\%5)$$

Where Xi and Xj are key characters,ci is the block character, CA is circular array and AS is resultant shifted array.

Encryption Module(EM): Encryption Module is computational unit which converts block character into

cipher character. Encryption Module comprises above three components (Key Character, Array Inverter and Array Shifter) CE be the cipher engine as below

EM= KC U Al U AS

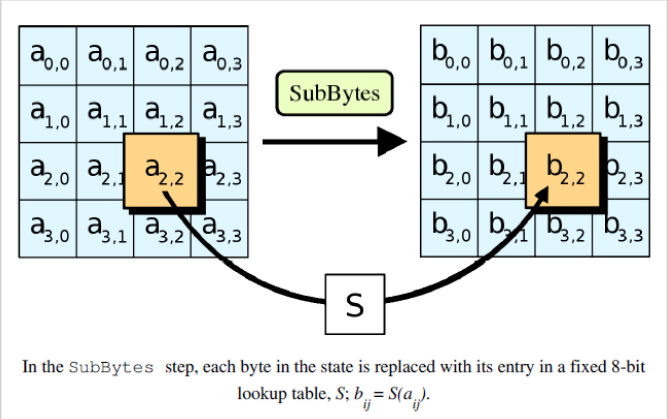
Decryption Module(DM): The Decryption Module comprises same components as Encryption Module but in reverse order as below

DM= AS U Al U KC.

We are using AES and SHA1 Algorithms to provide security in cloud system.

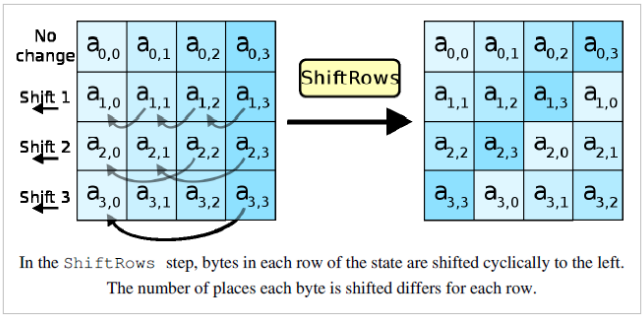
AES ALGORITHM:

SubBytes: Each byte in the *state* matrix is replaced with a SubByte using an 8-bit substitution box



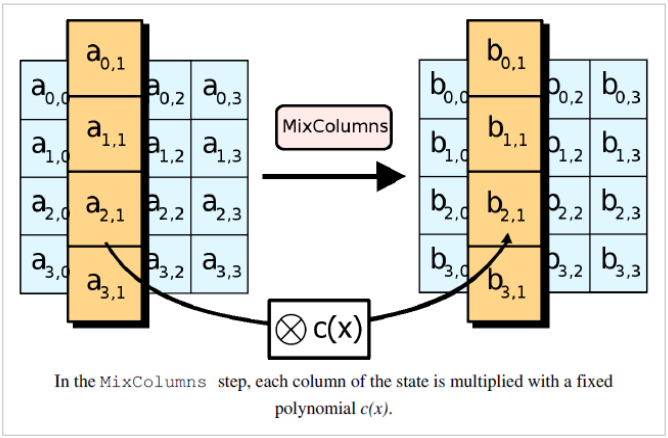
In the `SubBytes` step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

ShiftRows : It is transposition step where each row of the state is shifted cyclically a certain number of steps.



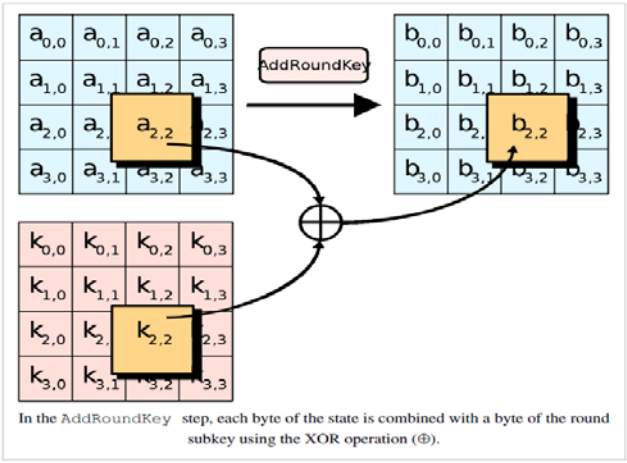
In the `ShiftRows` step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

Mix Columns: In the Mix Columns step, each column of the each state is multiplied with a fixed polynomial c(x). During this operation, each column is multiplied by the known matrix which is fixed c(x). invertible linear transformation is used for combining four bytes of each Column of the state.



In the `MixColumns` step, each column of the state is multiplied with a fixed polynomial $c(x)$.

AddRoundKey : In this step, the subkey is added with each state. In each round, from the main key subkey is derived using Rijndael's keys schedule. size of subkey remains same as the state . using bitwise XOR The subkey is added by combining each byte of the state with the corresponding byte of the subkey.



In the `AddRoundKey` step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).

SHA1 Algorithm-

The SHA1 is "Secure Hashing Algorithm". It is designed by the United States National Security Agency. SHA1 is currently the most widely used SHA hash function.

The SHA1 encryption algorithm is a Secure Hash Algorithm (SHA1). SHA1 algorithm used to generate the Condensed representation of a message or data called as a message digest. The SHA1 is a Digital Signature Algorithm (DSA) which is specified in the Digital Signature Standard (DSS).

When a message of any length is taken as input, the SHA1 produces a 160-bit output. This output called as a message digest. This digest can then be input to the Digital Signature

Algorithm (DSA), which generates or verifies the signature for the message. Message digest is usually much smaller in size than the message ,thus efficiency is improved . The same hash algorithm must be used by both the verifier and creator of the digital signature. The SHA1 is very secure because it is impossible to find a message according to given message digest, or to having the same message digest for two different messages . Any minor alteration to a message in transition will result in different message digest, and the signature will not get verified as a result signature will fail to verify. SHA1 is improvement over the SHA ,which has been added the circular left shift operation.SHA1 algorithm improvement over the security provided by SHA standard. The SHA1 is based on similar principles as that of the MD4 message digest algorithm.

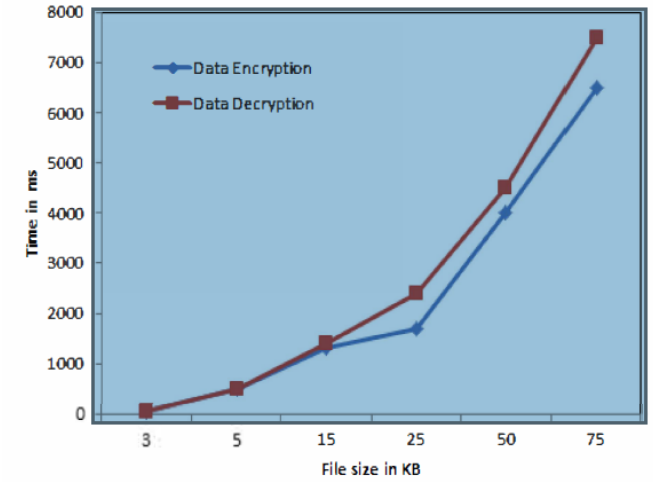
SHA1 Features:

- By using SHA1 message digest for a given message or data block is obtained.
- Bit string is taken as input which can be either message or data file.
- Any number of bits can be taken in the message .
- For compactness Message is represented in hex format if number of bits is multiple of 8.
- Message padding is done for making the total length of a padded message a multiple of 512.
- When computing the message digest SHA1 processes the blocks of 512 bits sequentially.
- The SHA1 algorithm then processes padded message as 512-bit blocks.

V. SIMULATION/EXPERIMENTAL RESULTS

The result is observed on the storage of text files having various size. data or text file contains alphanumeric characters. The Encoding Map is obtained to have mapping values for alphabets and numericals. The key used which is 256 bits in size. The key size is fixed for experimental purpose. The file is splitted into blocks of 256 characters that is 4096 bits in size. Algorithm implemented using JAVA language.The NetBeans IDE and Linux OS are used. The key operations in both processes are CA shifter and CA inverter. The time and accuracy encryption/decryption process is directly depends on these two operations.

Along with CA shifter the key rotation is done for every data block. This ensures that, Different key is generated for multiple data blocks. The analysis is done on different files and number of movements used for shifting CA and key remains same for the file with size 313 characters the number of movements done is 646, which is almost double the file size. every shift operation considers 0.5 character i.e. half the character which is 8 bits. This implies that shift operation is performed on each byte and hence the data is distingushed at byte level(fine level). The second parameter is the CA inverter operation.118 times the complement operation is done for the file size of 313 characters . This implies that for every 3 characters complement operation is performed and hence the data is disguised at coarse level(bytes level). As CA shift and complement operation is done for every character. It has more impact on the process of encryption/decryption and thus we concluded that encryption is happening at finer level(byte level) .As file size increases the number of movements and complements are high and hence the time of execution is directly proportional to size of file. It is observed that encryption is taking less time than decryption process.



VI. CONCLUSION

Our study of experiment conveys that we protect data strongly in cloud environment by using key rotation. Advanced Encryption Standard (AES) is used for encryption /decryption which provides high security to the data. The Storage and computational overheads are reduced with data encryption algorithm when data owner splits the file into blocks of fixed size. The Auditor(trusted third party)verifies the authorized user for accessing the data from cloud environment, this reduces the work of data owner .Highest data privacy is provided , when TTP and cloud service provider works parallel. We evaluate the performance of data encryption / decryption algorithm. It Increases the storage effectiveness and efficiency of the cloud environment. In

provision the Authorized user can retrieve the data in given time period which is allocated by owner of data, thus only data owner is having all access rights and highest priority . data owner has rights to restrict the access to another authorized users and he can do any operations on data like update, delete and insert.

VII. FUTURE SCOPES

In future , dynamic block level operations can be evaluated on encrypted data files. So we can also do the operations on data like insert , delete and update etc. dynamic block level operations which is the most important future work considerd .we can also use this system in military forces.

REFERENCES

[1] Prakash G L, Dr. Manish Prateek and Dr. Inder singh," Data Encryption and decryption algorithms using key rotations for data security in cloud system" in international journal of engineering and computer science dated on april 2014 .

[2] Prakash G L, Dr. Manish Prateek and Dr. Inder singh," Data Encryption and decryption algorithms using key rotations for data security in cloud system" 978-1-4799-3140-8/14/$31.00 ©2014 IEEE

[3] Jing-Jang Hwang, Yi-Chang Hsu,Taoyuan,Chien-Hsing Wu, "A business model for cloud computing based on separate encryption and decryption service",in international conference on information science and applications(ICISA),pages 1-7,2011.

[4] Junzuo Lai, Deng R H, Chaowen Guan, Jian Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption" , in IEEE Transactions on Information Forensics and Security, vol. 8(8), pages 1343-1354, 2013.

[5] Miwen, Rongxinglu, Kuanz hang, Jing Shenglei, Xiaohuiliang and Xueminshen," PaRQ:A Privacy-Preserving Range Query Scheme Over Encrypted Metering Data for Smart Grid", in IEEE International Journal of Computer Networks, pages 178-191,2013.