Cloud Data Security using Key Rotation

Prof. Archana Said[1], Jagruti S. Dambre[2], Tejswini G. Divekar[2], Shital Gharjale[2], Pooja Jadhav[2]

[1]*Assistant Professor,* [1,2]*Department of Computer Engineering*

[1,2]*AISSM'S Institute of Information Technology, Savitribai Phule Pune University, Pune-01*

Abstract ***In previous systems there was lot of burden for computing security tasks such as storage of data and encryption and decryption of data files. Which was more time consuming for processing of data in cloud environment? This is the main drawback of previous or earlier systems. In addition there was no facility 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 solves these earlier security threats, we are using data encryption technique for individual data blocks with key rotation using 128 bit symmetric key. In addition users of particular data can demand for data and do operations on their data such as add, change, and remove etc. very easily. We have use the two standard algorithms AES and SHA1 .The main purpose behind of these two algorithms is data security. Advance Encryption Standard algorithm is used for encryption and decryption of data and for hashing SHA1 is used. we have designed three modules which are TTPA ,CSP and Data Owner . Because of this we are achieving the better result that is strong data security in cloud systems. In our system there is provision of time based access control for providing security to file access if multiple clients are connected via LAN in network that means files access is restricted to authorized users only. The time span is defined by the data owner who is having all the authorities over his data.***

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

I. INTRODUCTION

In cloud systems number of resources such as hardware and software are efficiently provided for computation, storage and use of data. Cloud systems are primarily used for storage of data in the cloud system, because of this burden of controlling data by data owner or authorized users is greatly reduced. It is very advantages to store data in the cloud, by spreading control in rest of network.

Data is securely stored in the cloud, for security of data authentication and encryption operations are done. Access control policies are defined by the owner of data. Integrity checks and data masking are also done for data protection. Cryptography is the system in data is strongly protected when stored in the cloud .The system consists of encryption and decryption operations. While storing data on the cloud plain text is converted into cipher text using shared symmetric key. After encryption data is stored on the cloud. Again when requested data retrieved from the cloud decryption operation is done on data using same symmetric key. Thus, this is symmetric key cryptography.

Efficient key management and authentication of data is done to provide strong protection to data, when data is In transit from user to cloud service provider. In our system these data security threats are reduced. Encryption is done on each and every data blocks and key is rotated each time for individual blocks with 128-bit symmetric key. Users can demand and retrieve requested data users and do manipulations like insertion, updating and deletion etc. from cloud. In proposed system, We have designed three modules which are TTPA (Trusted third party auditor), CSP (cloud service provider) and data owner. We used advanced encryption standard (AES) algorithm which provided very strong security than traditional cryptosystems such as DES where DES had brute force attack and having other inconveniences.

There are multiple users who store and retrieve their data from cloud. Legitimate user demands for data, he has to send requests for data to both TTP and CSP.TTP calculates hash values for data blocks and CSP has stored actual encrypted files. When user is verified by TTP.it sends authorization signals to CSP. User gets hash values from TTP and encrypted file from CSP. User calculates hash values and matches with hash values received from TTP. If it matches user can do decryption using shared symmetric key. In addition , security to files access is provided if two or more users are connected via network in LAN . files are not Accessible to other users other authorized users. Time based access control is imposed for files and it's users which is defined by data owner .data owner has all data permissions and he can do any manipulations on data. TTP is introduced Because of this burden of data owner and CSP is reduced to great extent.

II. RELATED WORK

Dr. Manish Prateek, Prakash G L, and Dr. Inder singh, et al [2] has proposed one system. In which to improve the scope

of software and hardware resources data is outsourced in cloud. To secure these outsourced data is a serious invitation / challenge for data security in cloud computing. In these system there is no any facility provided by DO to authorized user in that facility authorized user can access data in allocated time only which is decided by DO.

Yi-Chang Hsu, Jing-Jang Hwang, Chien-Hsing Wu, Taoyuan, et al [3], has developed one model that is a business model to cloud computing which is based on different encryption and decryption service. In this system CSP (cloud service provider has whole responsibility of task such as encryption and decryption of data, storage of data. So this task produces more overhead on cloud server. The main disadvantages of this system is DO (Data Owner) is fully depend on CSP (cloud service provider).

Deng R H, Junzuo Lai, Jian Weng, Chaowen Guan et al [4], has developed a model. That model is Attribute-Based Encryption with Verifiable Outsourced Decryption for providing security to data in cloud system. In that system model decryption algorithm is based on the user requested attributes for which it requires lot of computational overhead to verify user attributes with encrypted data.

The main drawback of this system is it is less efficient. To overcome or solve this obstacle we have added TTP.TTP is nothing but Trusted Third Party Auditor. It reduces storage as well as computational overhead of the cloud server. Since our system is more efficient than earlier system

III. MOTIVATION

Now days securing data is becoming an important problem. If we store data on cloud there may be chances that it will be lost or it will be used by another person who is not legal or unauthorized. So to secure our stored data on cloud there is need of some mechanism. There are various mechanisms like stenography, cryptography. In stenography our data prevent through images. While transferring data, it hides behind the image. In cryptography encryption and decryption algorithms used to protect data from unauthorized users.

In encryption and decryption there are also two mechanisms. That is symmetric key encryption algorithm and asymmetric key encryption algorithm. In asymmetric key algorithm public key that is known to all used to encrypt data. In symmetric algorithm private key that is known to data owner only used to encrypt data. So to improve performance we have used symmetric key algorithm. Data owner only knows key about his data. Though Data Owner give permission other user to access data he has right to assign limitation on that users. That users can access data within given time only which is decided by Data Owner.

IV. PROPOSED METHODOLOGY

With all the benefits of cloud systems and potential for reducing time, cost, efforts required to develop and use applications. as cloud paradigm is primarily capability for using storage and computing resources which are physically so far. it decreases investments of computing infrastructure in an organizations.

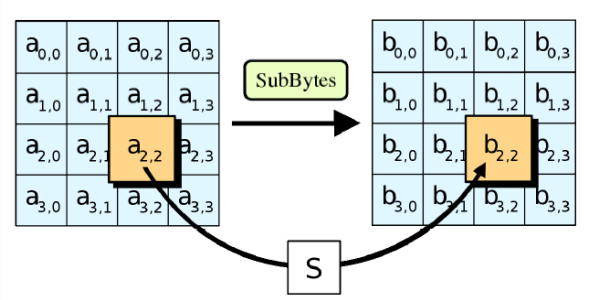
But now a days there are some vulnerabilities and security threats to cloud systems. strong security should be provided to the information and shared resources in the cloud.

For information security we have proposed our system .we use two algorithms to strengthen the data security namely AES(Advanced Encryption Standard) and SHA1(Digital Signature).

AES is symmetric key encryption-decryption algorithm. AES has come over DSA algorithm which had brute force attack. SHA1 is used to get a 160-bit output even message input is of any length. This obtained 160-bits are message digest which is having fix and smaller size than message data, so improves efficiency. The SHA1 provides high security because it is not possible to trace a message from given message digest. Message digest will be unique for each and every message if having very minor alteration among them. So the signature will fail to verify.

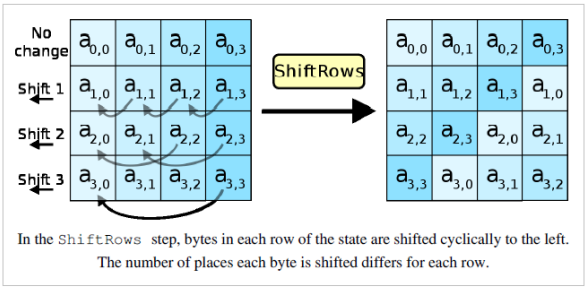
AES Algorithm:

SubBytes: An 8-bit substitution box is used to replace bytes from state matrix with sub Byte .



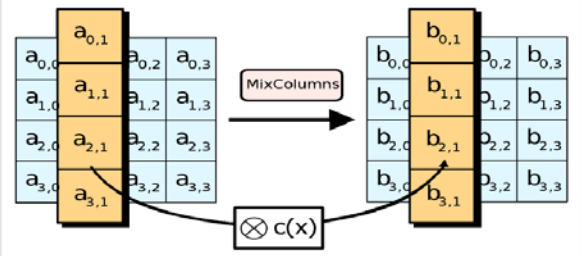
In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

ShiftRows : In this step each row of the state matrix is shifted cyclically to a specified number of steps.



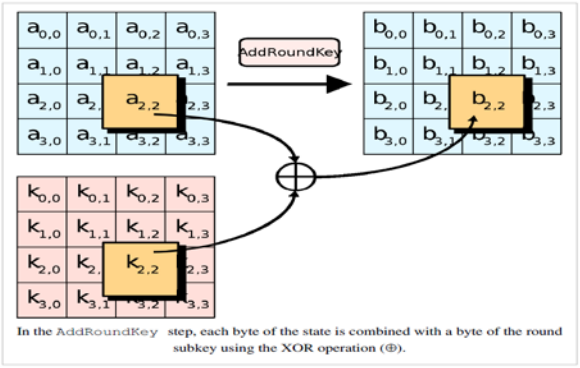
In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

Mix Columns: In the step, columns of the state matrix is multiplied with a known polynomial c(x). multiplication of each column of state and fixed polynomial c(x) is carried out. By using invertible linear transformation four bytes of each Column of the state are combined.



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

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



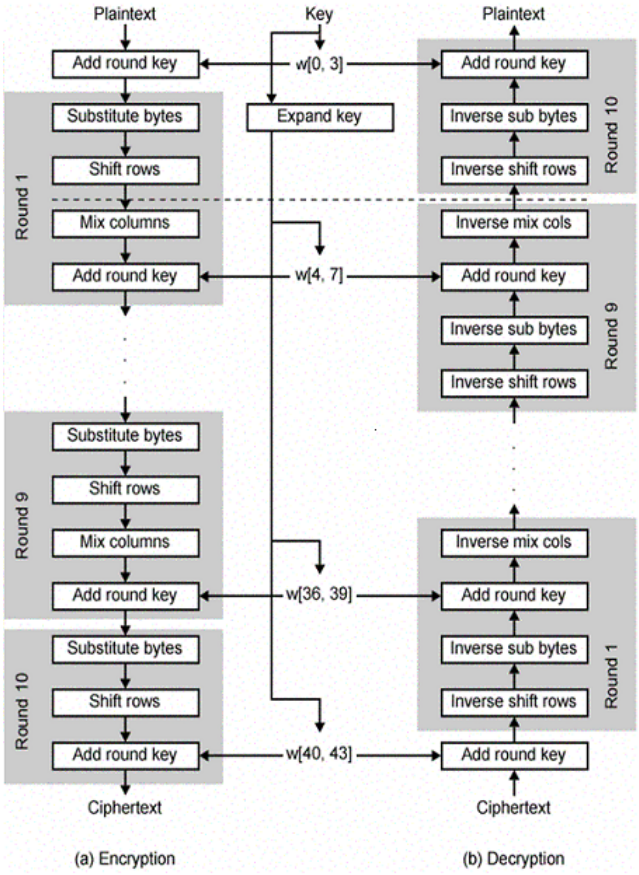
In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).

AES is an iterative symmetric block cipher algorithm:

AES repeats the same predefined steps multiple times.

AES is a symmetric key encryption – decryption algorithm.

AES algorithm is reversible. In this all the steps are same in both encryption and decryption just in reverse order. mix column step is absent in 10th round to make the algorithm reversible. The AES algorithm operates on fixed number of bytes that is 16 bytes at a time and uses 128-bit cipher key, which is easy to implement and explain.



SHA1 Algorithms:

The United States National Security Agency has designed the SHA1 algorithm .SHA1 stands for "Secure Hashing Algorithm".

SHA1 is the most popular and widely used hash function.

SHA1 algorithm used to generate 160-bit output called as message digest which is Condensed representation of a message or data.

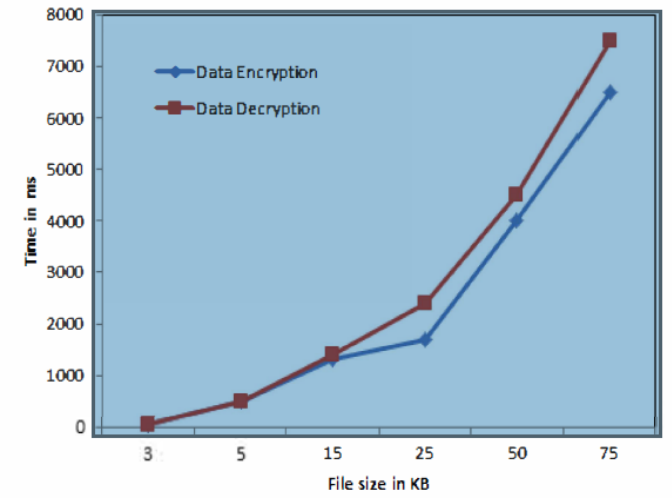
When a message of any length is taken as input, the SHA1 produces a constant size of output even though message input contains any size of input. This Message digest is usually having much small size than the message to improve efficiency. hash algorithm must be same for both the verifier and creator of the digital signature. Which verifies or generates the signature for the message. The SHA1 is highly secure because it is impossible to trace a message from given message digest, Any kind of small change occur to the

message in the transition message digest will be obviously different.

V. SIMULATION/EXPERIMENTAL RESULTS

In proposed system, large number of text files having varying sizes are stored and result is observed. files may contain very large alphanumeric characters. Mapping between alphabetical and numerical values is carried out by using Encoding Map . The 128- bit key is used in size. The key size is kept fix for experimental purpose. The file is divided into size of 128 bit

Blocks. The JAVA language is used for implementing algorithm. The Net Beans IDE and Linux OS are used.



The CA shifter and CA inverter operations are used in both the processes. The two main aspects that is time and accuracy of encryption/decryption process dependent on these two operations. With CA shifter operation key rotated each time for every data block. Thus, new keys are generated for all different data blocks. Number of different files with varying sizes are used for analysis purpose. The CA shifter movements and key remains same. If file with 313 characters 646 movements are done, which is nearly double to the file size. shift operation considers 0.5 character . This concludes that shift operation is performed on each byte and hence the data is disguised at fine level. Again in the CA inverter operation. the complement operation is done 118 times for the file size of 313 characters. in this for every 3 characters complement operation is done and hence the data is secured at coarse level(bytes level). These both operations that is CA shift and complement is done for each and every character. Thus, we concluded that encryption/decryption is happening at finer level(byte level) . the number of movements and complements goes high as file size tends to increase. therefore execution time is directly proportional to the file size. It has observed that encryption operation has taken less time than decryption operation.

VI. CONCLUSION

To secure the outsourced sensitive data in the cloud computing surroundings, we have used an effective advance encryption and decryption algorithm. With data encryption, data owner get the benefits of splitting the file to reduce storage and computational overheads. Also TTPA has introduced to reduce the data owner's and cloud server's burden to retrieve the data from server. There are some access policies are provided to data owner to increase performance of System. With these policies authorized user can access data with certain limitation provided by Data Owner.

VII. FUTURE SCOPE

In future, we can implement dynamic block level operation on encrypted data files. Hence we can do the operations like adding, deleting, updating dynamically which the most important future work is considered.

REFERENCES

[1] Prof. Archana Said, Ms. Shital Gharjale, Ms. Pooja Jadhav, Ms.Jagruti Dambre, Ms.Tejaswini Divekar ," Data Security using key rotations for data security in cloud system" in International Journal Of Scientific Progress And Research dated on Oct 2014.

[2] Dr. Inder Singh , Dr. Manish Prateek and Prakash G L," 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 .

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

[4] Yi-Chang Hsu,Taoyuan ,Jing-Jang Hwang, ,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.

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

[6] Miwen, Rongxinglu, Jing Shenglei, Kuanz hang, 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.