Triple Encryption method for secured cloud data storage

A .Anandhi M.E Assistant Professor, S.Yogeswaran, Dontabhaktuni Saisudharsan

Abstract— **Cloud computing environment contain data relation to user and owner, and these private data must be secured from untrusted persons or malicious users and also revoke these user. Cloud computing environment is not only store user data but also computing users and owner's data and provide the platform and infrastructure for users. This service is accessed from anywhere from world using internet and some network since it uses distributed data resource in open environment. Authentication to right user and data security is major problem in cloud computing environment. In this paper we proposed a generic model triple encryption method which provide security to sensitive data and authenticate the right user in cloud computing environment or model provide clear view of triple encryption and working methodology of the model, Thus using this model we can provide user a secured environment to their data and secure way of transformation of data. Since cloud computing environment does not having proper standard for transmission of data and malicious user cannot be easily revoked. Thus it arise problem in security of owner's data and sensitive data storing cloud environment. Thus we provide a discussion on exiting problems in any systems and disadvantages in the cloud environment.**

Index Terms— **Malicious user, private data, revoke, authentication, data resource.**

I. INTRODUCTION

Cloud computing is a modern and emergent network technology which is used in various domains, applications and business application. Like the traditional client-server model or older mainframe computing, a user connects with a server to perform a task such as storage, computation and etc. User who has permission to access the server can use the server's processing power to run an application, store data, or perform any other computing task instead of using a personal computer every time, the user can now run the application from anywhere in the world, as the server provides the processing power to the application and the server is also connected to a network via the Internet or other connection platforms.

The cloud computing is emergent technology and it is used to store the user's data and used for public and official service so it need more security from malicious user and hackers. The system is used for store the data of any public user, so any one can used it and they may be hackers 'who are trying to hack our data'.

Since it is emergent technology still is has no a standards protocol and it has no proper authentication and it has no trusted storage media .In this paper we proposed a model a triple encryption method which provide security and standard. This paper is a step towards developing secured cloud environment which provider essential security to the data in the cloud environment. Triple encryption method is optimized solution to provide security for data in cloud storage because cloud computing does not have proper standard so, providing security to thus system is difficult and the malicious user can attack the system easily. Thus it is a suggestion for secured cloud data storage and secured data transaction.

II. RELATED WORK

The system tells about Cipher text policy attribute based encryption (CP-ABE)[2] and how to revoke the malicious user (hacker). The cipher text policy attribute based encryption scheme with revocation can be the secure model to archive secured data transfer in cloud computing environment. Here it uses linear secret sharing, binary tree techniques for storage the attributes and in addition each user is assigned with unique identifier, so it easy to revoke the malicious user. The algorithm used in this system is attribute based encryption (AEB). Without using any malicious revocation mechanism then the manager has to rebuild the whole system and so revocation is necessary for the cloud computing environment. It tells us study of feasible revocation operation in CP-AEB scheme and based on the unique identifier revocation technique is proposed which the malicious user are revoke. Efficiency system is increased because user secret key size is increased, so it is better than traditional cipher text encryption. Here the revocation tree is user store the attribute, so the piece of the secret key is used for the decryption of data and computational cost is acceptable.

Effective ways of secure, private and trusted cloud computing [3] presents how to earn customer's good well in cloud computing environment provide security, privacy and reliability while third party process our data. The security challenges deals with the cloud environment are information security policy and infrastructure, security of data from the malicious user, virtualization and grid technology and identity and access management. Privacy challenges deals with the cloud environment are sensitivity of data, applicable law, right to access data and data transfer condition.

***A .Anandhi M.E* assistant professor ,** *department of computer science and engineering , christ college of engineering and technology puducherry, Indai.*
***S.Yogeswaran,** department of computer science and engineering , christ college of engineering and technology , puducherry, Indai.*
***D.Sai sudharsan**, department of computer science and engineering , christ college of engineering and technology , puducherry, Indai.*

ISSN: 2278 – 7798

The cloud service provider[4] have different standards, so in terms trust they also differs according to user, to take care sensitive information, security and privacy issues may raise. To provide security to the data they use cryptographic technology. Here hierarchical identity based encryption system and cipher text attribute based encryption system are combined to solve the above mentioned problem. Here a scheme is proposed by combining the hierarchical identity based encryption system and cipher text attribute based encryption system to achieve high performances, revoke the malicious user and to provide security.

Easier(Encryption-Based Access Control in Social Networks with Efficient Revocation)[5], architecture to support access control and dynamic group member ship by using attributes based encryption. A proxy is used to decryption process to provide security and to provide mechanism for revoke malicious user. Attribute based encryption algorithm is used in system to encryption and decryption this system is used to revoke malicious user. In attribute encryption technique is used to provide secure data storage even in untrusted storage medium.

Cipher text policy attribute based encryption[6] user private key associated with arbitrary attributes to express a string. User only able to decrypt a cipher text with a user attribute pass through cipher text access structure. Here public parameter and master key is used to encrypt and master key a set of attribute is used to generate key and public key and cipher text to decrypt. Here[7] proxy are used to perform re encryption without interference of plain text which include the computational efficiency and improve security .It is used to achieve secured file transaction and data outsourcing. Here the semi trusted proxy is used to perform the encryption operation. This improves the quality of the service, security of data transmission, privacy the data in the storage medium and it prevent the data from untrusted user or malicious user.

The public key cryptography[8] technique for encryption and decryption and the message is first encrypted using key and this key known to receiver side also, they decrypt the message this happens in presence of third party. Then while transferring the data the signature used and for the digital signature obtaining techniques is used. It one user signed the message and that produces the encrypted message and that message is transferred, the receiver receives the message and presumes the sender signature and the general decryption is taken place. This improves the quality of the service. Using this concept we can overcame the problem is transformation courier key and this system allows one to sign the digital documents and transfer it. But there is a security issue in this system and issues are urged user over the message and timing constraints. These issues can be rectified uses some advanced technology and proper terms and condition for users.

To improve the secure transformation data in cloud computing environment the data is re encrypted is carried which increase computational cost but it is acceptable. Here cipher text attribute based encryption method is used to encrypt and decrypt the data and these methods provide better security for data in the system. A controller is used to perform re encryption process, data stored in cloud and public group key directory which is used in encryption process. A manger (trusted authority) is used to take care of group key store and a firewall assigned between cloud storage, manager and users. While concern security the system provides high security data in cloud computing and attribute based provide secure transaction of data using public key and private key. Cipher text encryption algorithm users public key secret key and owner secret key to generate group public key which is used to encrypt the data stored in cloud and another re-encryption key is used to re-encrypt the data once again, while decrypting data it uses data secret key, public partition key, group secret key to decrypt the data . It will reduce the security threads and holes and provide full time security in cloud computing.

We survey papers to prepare our own idea. The above literature survey covers common challenges in cloud environment like security and standard, and disadvantages over the existing system and its related work which gives clear view about the existing problems.

III. PROPOSED SYSTEM

Triple encryption method deals with encrypting the data trice using three admin key and it uses proxy servers, two or more key stores which are separated geographically in different places. This method confuses the hacker or malicious user to attack what system or which server and which server consist of the original data information. While decryption the data, concatenate values of keys are used to decrypt the data, so prediction of keys are not possible. This method is hybrid model of re-encryption method and proxy based security system so it gives the advantage of both re-encryption method and proxy server system.

We can use this method for provide the proper user authentication and authorities for user and data owner. While creating the account the user password is encrypt using three keys and the data store into different data bases. That is two keys are used to encrypt the data twice and stored in data base belong to server along with this stored the key in key store. Then the data of server is once again encrypted with third defined key and stored in proxy server, the keys are used to generate concatenate key value, this key are stored in another key store separately this system are protected and separated using fire walls and trusted manager .While decrypting the data user data id decrypted using concatenate key and verifying using proxy servers then if it is authenticate as right user then it forward to server.

By using this type of triple encryption method it provide both data and user login security by this very complicated type of method. Triple encryption method uses proxy servers and two database where the data is stored in encrypted from and key stores are used to provide keys, therefore it provide backups to data automatically.

Triple encryption method deals with encrypting the data trice using three key and it uses proxy servers, two or more key stores which are separated geographically in different places. This method confuses the hacker or malicious user to attack what system or which server and which server consist of the original data information. While decryption the data, concatenate values of keys are used to decrypt the data, so prediction of keys are not or very less possible. This method is hybrid model of re-encryption method and proxy based security system so it gives the advantage of both re-encryption method and proxy

ISSN: 2278 – 7798

server.

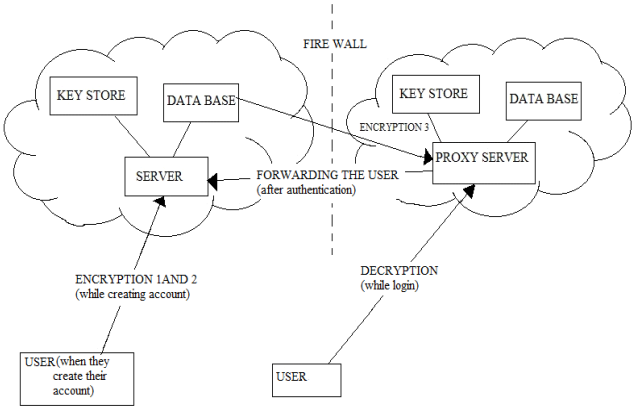
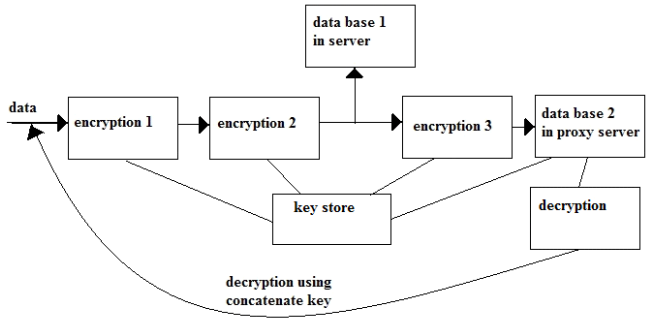


Fig a. SYSTEM ARCHITECTURE



F ig b. WORKING MODEL OF THE SYSTEM

IV. WORK ON CRYPTOGRAPHIC TECHNIQUE

The triple encryption method needs to encrypt the data thrice and decrypt the data only one time, so the cryptographic technique support for this method should be developed. Thus some of existing method does not support, so bilinear transformation is mathematical model which uses two constant, thus one constant is used to define another constant and vice versa. The concept of bilinear transformation is a new idea that suits triple encryption

$$\frac{w-w1}{w2-w3} = \frac{z-z1}{z2-z3}$$

Where w1, w2, w3, z1, z2, z3 are numbers or value used to define the constant. This technique has same basic mathematical limitation such as constant should not be divided by 0 i.e. say w2-w3 not equal to zero, then negative signs must balanced and identical or same value for all constant should not used.

V. CONCLUSION

The paper gives information about related work performed to improve security in cloud environment and to improve standard in cloud environment. Using the gathered information and related work, we prepare our own proposed system. The paper covers common challenges in cloud environment like security and standard, and disadvantages over the system and its related work, which gives clear view about the existing problems. Thus the triple encryption method is optimistic idea for cloud computing environment which can produce a new security method and more security for the data. The future work on this method can produce an efficient and improved security for cloud computing environment.

REFERENCES

[1].Piotr K. Tysowski and M. Anwarul Hasan, Senior Member, Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds ,IEEE 2013

[2].X. Liang, R. Lu, and X. Lin, “Ciphertext Policy Attribute Based Encryption with Efficient Revocation,” Technical Report BBCR, Univ. of Waterloo, 2011.

[3].Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta, Manoj Diwakar ,“Effective Ways of Secure, Private and Trusted Cloud Computing “

[4].G.Wang, Q. Liu, and J. Wu, “Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services,” Proc. 17th ACM Conf. Computer and Comm. Security (CCS ’10), pp. 735-737, 2010.

[5].S.Jahid, P.Mittal, and N.Borisov, “EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation,”Proc. Sixth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’11), pp. 411-415, 2011.

[6].J.Bethencourt, A.Sahai, and B.Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp. 321-334, 2007.

[7].G.Ateniese, K.Fu, M.Green, and S.Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” ACM Trans. Information and System Security,vol. 9, pp. 1-30, Feb. 2006.

[8].R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Comm. ACM, vol. 26, no. 1, pp. 96-99, Jan. 1983.

ISSN: 2278 – 7798