



A Secure Data Sharing in Public Cloud using DES, RC4 and Diffie Hellman Algorithm

Neha Thakur

M.Tech Student

Department Of Computer Engineering

Punjabi University

Patiala, India

Er. Supreet Kaur

Assistant Professor

Department Of Computer Engineering

Punjabi University

Patiala, India

Abstract: *Cloud is not a new technology, but a new delivery method in which services are hosted on third party assets. Due to its distributed architecture, security is one of the prime concern in cloud computing. Cloud computing provides the facility of data storage and access for cloud users, Cloud computing is widely used service model for storage. Outsourcing the data to a third party causes safety issue of sensitive data. Shared sensitive data must be strongly secured from unauthorized access over the clouds so data is protected by restricting the data. We proposed two level security mechanism. In our proposed scheme there is a registration for user to use cloud services. The registration of the user also assures security of the data in cloud. Only authorized users can access the cloud data. Data should be encrypted with the help of symmetric algorithms. Two tier authentication scheme provide the integrity, authenticity to the user. In proposed scheme first encryption is user based and the second is cloud based. After successful authentication user can get the data. Aim of this scheme is to combine the best of symmetric and asymmetric mechanisms to provide effective security model on public clouds.*

Keywords- *Cloud computing, Certificateless encryption, Secure Data Sharing.*

I. INTRODUCTION

Cloud is not a new technology, but a new delivery method in which services are hosted on third party assets. Due to its distributed architecture, security is one of the prime concern in cloud computing. There are various security models proposed and deployed upto now, but none of these is said to be full proof. So there are various research going on to make the cloud environment more efficient and secure. Cloud computing is widely used service model for storage i.e. Storage as a service that enables user to share their data in public cloud . Public cloud storage model should solve the critical issue of data confidentiality that data only accessed by authorized users. Shared sensitive data must be strongly secured from unauthorized access over the clouds. In order to assure confidentiality of sensitive data stored in public clouds, a commonly used approach is to encrypt the data before uploading it to the cloud. Since cloud does not know the keys that we are used to encrypt the data, the confidentiality of data from cloud storage is assured. There are many security methods already existing to provide the security. Security mechanisms are used to provide authentication, confidentiality and integration services in the cloud environment. Main security mechanism comes under any of these two categories: Symmetric key mechanism and Asymmetric key mechanism. Fine grained encryption access control of the data is processed with the symmetric key based method. Symmetric key based mechanisms have various problems as handling uniqueness of keys, which in turn incurs high key management cost. A traditional public key cryptosystem requires a trusted Certificate Authority to issue digital certificates that bind users to their public keys. But this certificate management is very costly and complex [8]. To address certificate management issue new system as Identity Based Public Key cryptosystem (IB-PKC) was introduced but it had a key escrow problem which means the key generation server knows the private keys of a user. So this scheme not safe to assure users privacy. Next the Attribute Based Encryption (ABE) mechanism has been used to encrypting the data content. Attribute Based Encryption provide the flexibility for the user to encrypt every data item based upon their access control policy. But it also had the revocation problem because the private key provided to the existing users has to be updated whenever a user dynamic changes [3]. Al-Riyami and Paterson [9] developed a new mechanism called Certificateless Public Key Cryptography (CL-PKC). Next the Certificate less Proxy Re-Encryption mechanism was introduced for secure data sharing in public cloud. This mechanism is based on CL-PKC to remove the key escrow problem and certificate management issue although uses pairing operation. To address above problem the concept of mediated cryptography has been used which support immediate revocation. Mechanism of mediated cryptography makes a practical and effective use of security mediator (SEM). Security mediator can control security capabilities for every transaction. The user's participation in a transaction will stopped immediately, once the SEM is been notified that a user's public key should be revoked. A notation of security mediated certificateless cryptography is introduced to present a mCL-PKE which depends upon the pairing operations, the computational costs required for pairing are still considerably high [10]. If user applies the basic mCL.PKE scheme to the cloud computing environment or many users access the same data, the cost of encryption becomes high for data owner. In this situation data owner should encrypt the data content with the same encryption key

for multiple times. To remove this difficulty, the basic mCL-PKE scheme with an extension had been introduced. The extended scheme makes the data owner to apply the data encryption key process only once not multiple times like previous scheme which in turns provides some added information to the cloud. So with use of this additional information the authorized users can decrypt their content using the private keys. This scheme is similar to that of the Proxy Re-Encryption (PRE) in which the encryption key is encrypted using the data owner's public key and continue later to decrypt using different private keys. In this extension scheme, cloud does not perform any transformation it simply acts as the storage model. The security models of the existing schemes are insecure against partial decryption attack. So secure mediated CL-PKE without pairings is needed. The idea behind this scheme is that data owner encrypts the data and after encryption process sends the encrypted data to the cloud. Then the cloud partial decrypts the encrypted document and it to the requested users. The user, then fully decrypt the data content using their secret keys. The extremely important thing is that, if more than one user are accepted and they want to get the access to same document then encryption rate will be enormously high for data owner since owner has to encrypt the same document several times for different users using the user's public key in previous mediated Certificateless public key encryption scheme. To overcome this difficulty the extended mCL-PKE system is, data owner encrypts the data only one time and sends the extra information to the cloud for certified users to decrypt the data. But in this proposed system there is no need of extra information for the user to decrypt the encrypted data [8]. Document is decrypted only by secret key given by the owner of the data. After getting the requested data from the cloud user has to decrypt encrypted data by secret key.

II. RELATED WORK

Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y,[3] presented the Attribute-Based Encryption (ABE), which is one effective and promising technique. The technique is used to provide fine-grained access control to data in the Cloud environment. Attribute-Based Encryption is an access control mechanism where a User to encrypt each data item based upon their access control policy. Access to data in the Cloud was provided through Access Control Lists (ACLs) , so this was not scalable and only provided coarse -grained access to data.

Tu S, Niu S, Li H, Xiao-ming Y, Li M [4] proposed a CP-ABE in the context of enterprise applications and also developed a revocation mechanism that allows high adaptability, fine-grained access control and revocation. The assigns users a set of attributes within their secret key and also distributes the secret key to the respective users. If user satisfies the access control policy defined by the data collaborator than he can access the data. The scheme is proven to be semantically secure against chosen cipher text attacks against the CP-ABE model. The scheme is not good in the case of user revocation because the updating of cipher texts after user revocation places heavy computation overhead even if the burden is transferred to the Cloud.

Dan Boneh [5], proposed a identity based cryptography scheme with the use of pairing. This scheme removes the need of certificate authority to manage the certificate. To encrypt a message intended for the entity described with the identity string. Identity based cryptography doesn't solve the revocation difficulty. To manage this problem in identity-based cryptography, short validity periods could be encoded into the identity string. However, this doesn't fit an environment where immediate revocation could be required.

Lei Xu, Xiaoxin Wu and Xinwen Zhang [6], proposed a CL-PRE, a certificateless proxy reencryption scheme for cloud-based data sharing. The Certificateless proxy reencryption scheme eliminates the key escrow problem in traditional identity-based encryption. Their scheme does not require any certificates to authenticate the public keys. This scheme satisfies security requirements for large-scale and flexible information sharing with cloud. Consider a proxy running in public cloud to leverage elastic cloud storage and computing resources. They further propose multi -proxy CL-PRE scheme to deploy intermediate proxies in multiple cloud service providers which further improve the robustness of the system. The performance evaluation shows that their proposed schemes are practical for cloud-based applications.

D. Boneh, X. Ding, and G. Tsudik [7], Presented the concept of mediated cryptography to support immediate revocation. Mediated cryptography removes the revocation problem. The basic idea of the mediated cryptography is to utilize a security mediator (SEM) which can control security capabilities for every transaction. If the security mediator is notified that a user's public key should be revoked, it can stop the user's participation in a transaction

Seung-Hyun Seo and Xiaoyu Ding[8]

proposed a mediated certificateless encryption scheme without pairing operations for securely sharing sensitive data content in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow issue in identity based encryption scheme. Their proposed scheme also solves the certificate revocation problem in public key cryptography system. Existing mediated Certificateless encryption schemes are either inefficient because of the use of expensive pairing operations and also vulnerable against partial decryption attacks. So as to address these security issue, they proposed a mediated Certificateless public key encryption technique without using pairing operations. In their scheme cloud is employed as a secure storage as well as a key generation center. The confidentiality of the data and the keys is preserved with respect to the cloud, because the cloud cannot fully decrypt the data. Further, for multiple users satisfying a similar access control policies, their improved scheme performs only a single encryption of each data and also reduces the overall overhead at the data owner.

III. SYSTEM DESIGN

The proposed scheme is two tier authentication scheme and it is extended from the previous proposal of mCL-PKE. The basic mediated Certificateless public key encryption scheme is based on certificate-less encryption and user is not certified by any authorized entity but in the proposed plan there is registration for user. The registration of the user also assures security of the data in cloud.

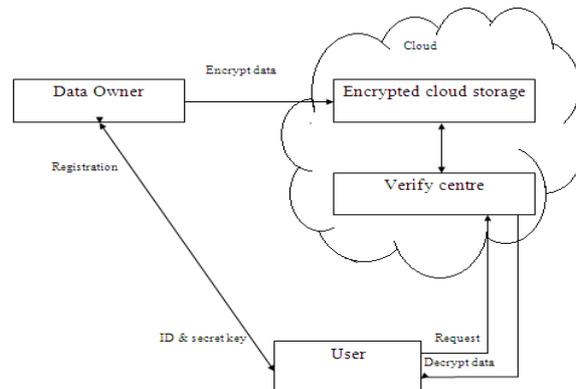


Fig. 1 System Architecture

The Double authentication means two layer encryption which overcomes the computational overhead of the previous scheme. In this approach first of all user needs to get registered to the owner to obtain the secret key to decrypt the encrypted documents. To ensure the confidentiality in public cloud environment, we propose a two level security mechanism in which data is partially encrypted by the data source and partially by the cloud storage. Partial encryption by cloud is to ensure the authorization of the receiver, and then only allow him to access the intended data stored on the cloud storage. For the simulation we will design cloud storage. The authenticated users of the cloud can access their data and they can also send the data to any other client of the cloud. The security will be based on the public private key of the users and the secret key encryption of the data. Figure 2 shows the data flow structure of proposed scheme. First process is cloud setup phase after this setup user must register them to cloud to use cloud services. Third phase is encryption and data uploading phase. In this phase data owner encrypts the data before uploading it to cloud. For two level security data will be two time encrypted . First encryption is user based and second is cloud based. Last phase is data verification and decryption phase after successful verification data should be accessed by the authorized user.

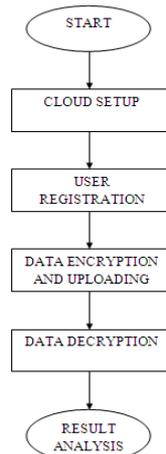


Fig. 2 Data flow structure of proposed scheme

For simulation process we use Cloudsim simulator with eclipse. Our approach mainly focuses on the key escrow problem and revocation problem. The Double authentication means two layer encryption which overcomes the computational overhead of the previous scheme. To provides two level security means two time encryption is done. First encryption is cloud based we use RC4 algorithm to encrypt the key and data content. Second encryption is cloud based where DES algorithm are used. Implement Denial of attack in work in which create two folder of storage. One is based on attack, other is without attack. Storage of attack stored lock file, lock implemented because it is better for security. Other storage stored encrypted file. Many user will use storage folder (this is based on Denial of attack), because users can not read lock file. We also compare the storage space required for encryption process by DES algorithm and Diffie Hellman algorithm. Second comparison is based on time required for encryption process by both algorithms.

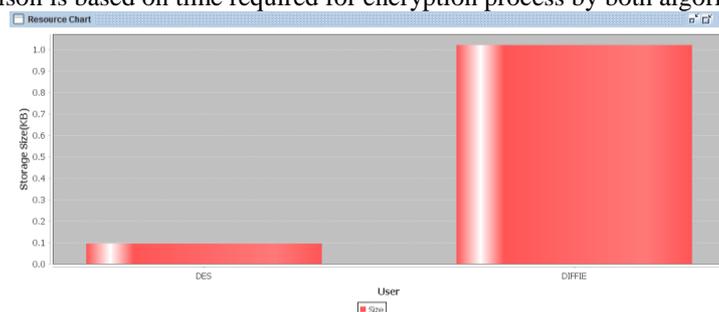


Fig. 3 Comparison of Storage space required for encryption process

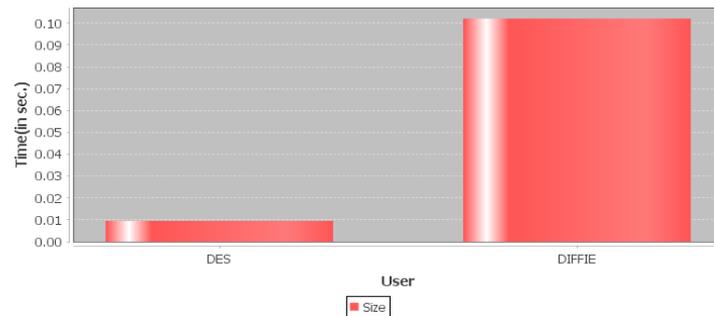


Fig. 4 Comparison of time required for encryption process

Above results shows that DES required less space for encryption storage than Diffie Hellman algorithm. The encryption time graph shows that DES take less time for encryption than the Diffie Hellman. So according to above result DES is better than Diffie Hellman for encryption process.

Table 1 gives the comparison factor for DES and Diffie Hellman algorithms

Table 1 Comparison Table for DES & Diffie Hellman Algorithm

Factors	DES	Diffie Hellman
Date	1972	1976
Block Size	64	Variable
Key Length	56	Variable
Storage Space For Encryption (KB)	0.0849609375	1.0205078125
Time Required For Encryption (Sec.)	0.009	0.102

We compare DES and Diffie Hellman algorithm on the basis of parameters like block size, key length, storage space and time taken for encryption process.

IV. CONCLUSION

In proposed scheme registration of the user offers high security to the cloud data. Symmetric key mechanism is very easy to implement and also offers high speed to the whole process. Comparison result shows that DES is better than Diffie Hellman for encryption process it requires less storage space and time for encryption process The future enhancement of this scheme is that it can also be used for large size of data to provide fast encryption and decryption, so it will be helpful for improving the speed and security of the big size data. It will be much less costlier, less complex and strictly secure security mechanism to deal with cloud security issues.

REFERENCES

- [1] T. Dillon, C. Wu and E. Chang, "Cloud computing: issues and challenges," 24th IEEE International Conference on Advanced Information Networking and Applications, AINA, pp. 27-33, Apr. 2010.
- [2] W. Liu, "Research on cloud computing security problem and strategy," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1216–1219, IEEE, 2012.
- [3] Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y, "Fine-grained data access control systems with user accountability in cloud computing," IEEE second international conference on cloud computing technology and science(CloudCom) 2010, pp 89–96.
- [4] Tu S, Niu S, Li H, Xiao-ming Y, Li M, "Fine-grained access control and revocation for sharing data on clouds," IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.
- [5] Dan Boneh and Matt Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, 32(3):586–615, 2003.
- [6] Lei Xu, Xiaoxin Wu and Xinwen Zhang, "CL-PRE: a Certificateless Proxy Re-Encryption Scheme for Secure Data Sharing with Public Cloud", ASIACCS '12, May 2–4, 2012.
- [7] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, Feb. 2004.
- [8] Seung-Hyun Seo and Xiaoyu Ding, " An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 9, September 2014.
- [9] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in Proc. ASIACRYPT 2003, C.-S. Lai, Ed. Berlin, Germany: Springer, LNCS 2894, pp. 452–473
- [10] C. Yang, F. Wang, and X. Wang, "Efficient mediated certificates public key encryption scheme without pairings," in AINAW, Niagara Falls, ON, May. 2007, pp. 109–112.