International Innovative Research Journal of Engineering and Technology
ISSN NO: 2456-1983

International Conference on Emerging Innovation in Engineering and Technology
ICEIET-2017

Secure Data Transmission With Multiple Key Management In Cloud Environment

Dr. Santhi Baskaran[1], A. Isaiarasi[2]

[1]Professor, [2]PG Student, Information Technology [1],[2] Pondicherry Engineering College,
[1]santhibaskaran@pec.edu [2]isaiarasi04@gmail.com

Abstract

In cloud computing Off-Site data storage is an application that relieves the customers from focusing on data storage in computing organization. In cloud, outsourcing data to multiple party organizations control leads to serious security concerns. Data leakage can ascend due to attacks caused by unauthorized users. However, security is a huge concern for cloud users. In existing work File Assured Deletion (FADE) technique was used for file removal from cloud storage when user requested for deletion. Therefore, it fell short on serious security concerns of keys and authentication of linking parties. To overcome the problem of man in the middle attack between Key Manager and client, we propose an algorithm to enhance Data Security for Cloud Environment with Semi-Trusted Third Party. This data security system that provides key management, access control and file confident deletion. This delivers security for cloud data storage through a proper key management system with multiple key managers using Shamir's key sharing technique. Also the policy file encryption is done using Elgamal algorithm for secure data transmission.

Keywords— Cloud Computing, Key Management, Data Security, Outsourced data, Policy file encryption

I. INTRODUCTION

Cloud Computing is emerging as tremendous computing paradigm which has been usually used for storing and accessing large amounts of data over the Internet. Data security is one of the major concerns with cloud computing. Even though the encryption and security capability develops at an aggressive estimate, the threat of hackers still looms in the many companies' minds. Cloud computing assets are increased storages, reduced cost, flexibility and manageability.

Cloud takes many different security algorithms such as Elgamal algorithm using Attribute Based Encryption (ABE), Diffie Hellman, RSA and Shamir's key sharing technique to overwhelm the problems among them. Data security act as one of the major challenges and other issues in cloud computing are access controls, key issue. Data being the principal possessions for organization needs must be secured specially, when stored in a public cloud. To avoid proscribed person accessing to cloud data, access control mechanism must be enforced.

Furthermore, data secrecy and data leakage action must be employed so that only authorised person or correct user can access and utilize data. Refraining cloud service providers from utilizing the customer data needs high preventive measures. Encryption techniques provide a key to ensure the confidentiality requirements but attacker can easily hack the cloud storage.

privacy, secrecy and protection. Failure of an key storage ability may lead to the harm of data in the cloud. The security algorithms and Shamir's key sharing technique with multiple key managements for data security in the cloud are used to securely store the data in cloud environment.

II. REALTED WORK

J. Li, X. Huang [2], in their technique developed a monitoring and auditing model that audits the cloud environment for ensuring the new data, data irretrievability, and resilience against disk failures. The methods depend on the users employed role for data confidentiality. Data cannot be protected against service provider fully.

Juels et al [4], presented a technique to secure the cloud data that provides a number of services, such as integrity, freshness, and availability. The authors employed a gate-way application in the enterprise to manage the integrity and freshness checks for the data. The Iris file system is designed to migrate organizations internal file system to the cloud. Moreover, a Merkle tree is used by gateway, which ensures freshness and integrity of data by inserting file blocks, MAC, and file version numbers at different levels of the tree. The gateway application also manages the cryptographic keys for

Minu George [6], incorporates virtualization, on demand deployment, Internet delivery of services and open source software. From another perspective, everything is new

because cloud computing changes tell about invent, develop, deploy, scale, update, maintain and pay for application and the infrastructure on which they run. Because of these benefits of Cloud Computing, it requires an effective and flexible dynamic security scheme to ensure the correctness of users data in the cloud. The users and servers in the cloud can generate secret session key without message exchange and authenticate each other with a simple way using identity-based cryptography. Identity based algorithm being certificate free, well adopted for providing the security to cloud world. Identity based algorithm is less vulnerable to spam and it also enables postdating of messages for future decryption.

A. Yun, C. Shi, and Y. Kim [13] presented the Hash based MAC tree, which is used for providing the aforesaid services. Construction of the MAC tree is done by the Block-wise encryption. The file system on the client side interacts with the file system of the server and outsources the encrypted blocks and these are stored privately. It is produced for confidentiality and integrity services to the outsource data.

S. Kamara and K. Lauter [5], proposed a virtual private cryptographic storage service to provide integrity and confidentiality for the user data within the cloud. This method has three modules for client application. They are data processor, data verifier, and token generator. The Master key is generated by Client application for subsequent operations. The data processor encrypts the file to be uploaded with keys generated from master key and uploads to cloud. Using a token generator it generates a token for downloading a file in the cloud. Once the data is downloaded in cloud, integrity of data is done by the data verifier checks. ABE (Attribute Based Encryption) is used for encryption [6]. Here the key resides on the client side and single point failure is present.

Zarandioon, S., Yao [10], developed user-centric privacy preserving cryptographic access control protocol called Key To Cloud (K2C) that enables end-users to securely store, share, and manage their sensitive data in an untrusted cloud storage anonymously [9]. K2C is scalable and supports the lazy revocation. It can be easily implemented on top of existing cloud services and APIs. The main advantage of the AB-HKU scheme is that it supports efficient delegation and revocation of privileges for hierarchies without requiring complex cryptographic data structures. But it does not improve the efficiency of K2C, and access control protocol by using proxy re-encryption to off-load key distribution task to the cloud.

Shuhua Wu [3], proposed two smart card based, password authentication, key exchange protocols that have achieves two factor authentication fully which become completely insecure once one factor is broken.

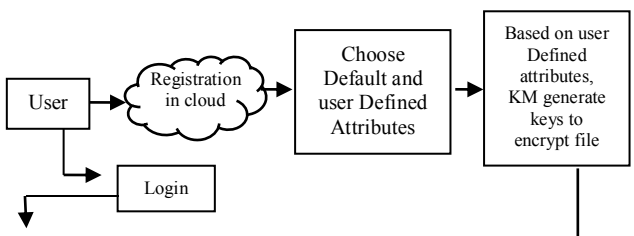
The FADE [6] protocol provides privacy, integrity, access control and assured deletion of outsourced data. The FADE uses both symmetric and asymmetric algorithms for security purpose. The FADE have file upload and download modules. The analysis of FADE identified the intruder (man- in-the middle attack) between client and key managers. An Intruder can intercept the user keys and policy, then send the modified policy to key managers. If users didn't receive the appropriate key from key manager may lead to the loss of data.

III. PROPOSED WORK

In proposed work a data security that uses key manager servers for the management of cryptographic key is erected. Shamir's (k,n) sharing threshold technique is used for the management of keys that uses k shares out of n to restructure the key.

Therefore, cryptographic keys are kept in a robust manner and a single point of failure will not affect the accessibility of data. To escape man-in-the-middle attack user can access their key and data is ensured through a policy file that states policies under which access is granted to the keys. The Data Security in Cloud Atmosphere makes use of both symmetric and asymmetric keys. The confidentiality and integrity services for data are provided through symmetric keys that are secured by using asymmetric keys.

Asymmetric key pairs are generated by third party Key Manager (KM). Out of the key pair, only public key is transmitted to the client. For secure transmission of keys, a secret key is established between client and KM through ELGAMEL algorithm.
In this system, the user has to register and become a participant in the cloud, Once they registered in cloud user has to choose Default attributes and also give user defined attributes to encrypt their policy file which is created by user while file uploading process. All attributes are encrypted by the elgammal algorithm. After completing the policy setting process, the authentication process will be achieved between user and key manager using Diffie-Hellman (DH) Algorithm. After that, the user will encrypt their file using secret key which is provided by KM in the cloud, based on user attributes provided in the policy file and uploaded in cloud. Now cloud Key manager split up the secret key into n shares (s1, s2,…..sn) and passes to multiple key mangers (k1,k2,…kn)



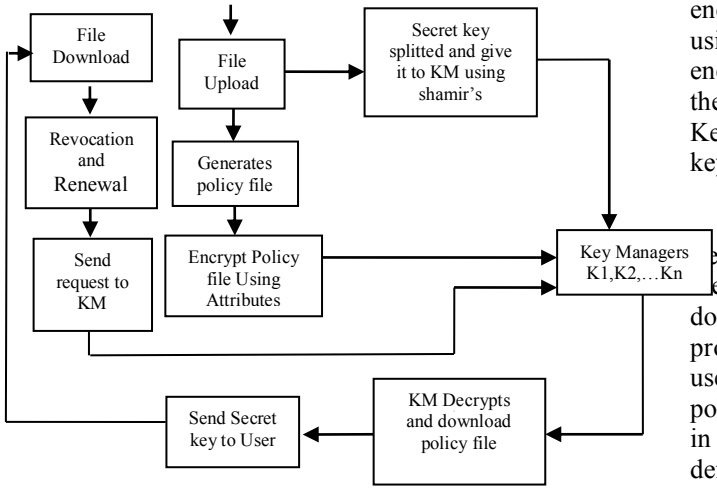


Figure 1.1: Overall System Architecture

After that key managers encrypt the spilt key and send the public key to the registered user in the cloud. If users need to download their files in the cloud, then they will send requests to the key manager with suitable attributes. The Key-Manager will check their attributes in the policy file for authentication. Key-Manager will provide decrypted i-th key share of the user. After that users will collect their secret key and securely download their files from the cloud.

The proposed modules are:

- Cataloguing of Users & Policy Setting
- File Upload & Key exchange
- KM Process and Decrypting File to Download
- Policy Revocation and Renewal

A. Cataloguing of Users & Policy Setting

First the user has to register to become a participant in the cloud. In the proposed model, once user registered to cloud, the user has to choose some attributes to create a policy. There are two types of attributes used. One is default attributes and another is user defined attributes. In Default attributes, the user has to choose some attributes like name, email, address, etc. using Attribute Based Elgamal algorithm.

Elgamal algorithm

Using this algorithm, attribute keys are generated and is a public-key cryptosystem technique. Elgamal algorithm is used for encrypting and decrypting the file in the cloud environment by the users. In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm. This method, using attributes generate a secret key, which is used for policy file encryption security.

B. File Upload & Key exchange

After registration, the user has to login into the cloud using username and password. Using authentication process, key manager creates a secret key for the file encryption. The secret key is created by the key manager using Diffie Hellman Key Exchange Algorithm. The encrypted file uploaded into the cloud. Key managers split the secret key and send the key to multiple key managers. Key managers create a public and private key for that own key.

The key splitting process is done by using Shamir's technique. All key managers transmit the public key to the users for the purpose of the decryption during download process. Simultaneously during the file upload process, policy file is generated. The policy file contains username, filename which is uploaded by the user. This policy file is also encrypted using a secret key and stored in the cloud. The secret key is generated by the user defined attributes.

Diffie - Hellman

This algorithm is used for authentication between client and key management. It is a method for constructing a shared secret numeric key over an open network with potential eavesdroppers.

Shamir's Technique and Goal

This technique is used for divide the secrets into multiple parts and stored in multiple key managers and then reconstruct the keys for security purposes. Shamir's Secret Sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is splitted into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

The main aim of shamir's technique is to share the secret s among n participants P1, P2,P3, ..., Pn such that at least k participants are required to rebuilt the secret s.

C. KM Process and File Decryption

If users need to download their text files or images, then they will send a request to Key-Manager with proper attributes. The Key-Manager will check their attributes for authentication process and provide decrypted share for the user. After getting the key from KM, users will receive their secret key and download their file and decrypt their secret key using RSA algorithm.

D. Secure Revocation and Renewal process

In this process user will allocate renewal and revocation policies, for achieving the policy revocation and user send revocation request to KM. Revocation is defined as user will confiscate all polices before user set. Revocation of user policy request is sent to Key Manager, to delete all user polices. In renewal process key manager will allow to use renew the policy. Once user got authorization from KM, user will renew the policy file.

IV. EXPRIMENTAL RESULTS

In this section, proposed Data Security in Cloud Environment is evaluated in terms of File Upload/Download Time Calculation with Multiple Managers. Subsequently, the file sizes used for evaluation were 0.3KB, 1KB, 10KB, 50KB, 100KB, 500KB and 1MB. Ten key managers were used for splitting the users keys for secure authentication. The experimental scheme is implemented by JAVA language on a Apache Tomcat Windows using XAMPP Server with Intel Core 2 Processor 2.0 GHz.

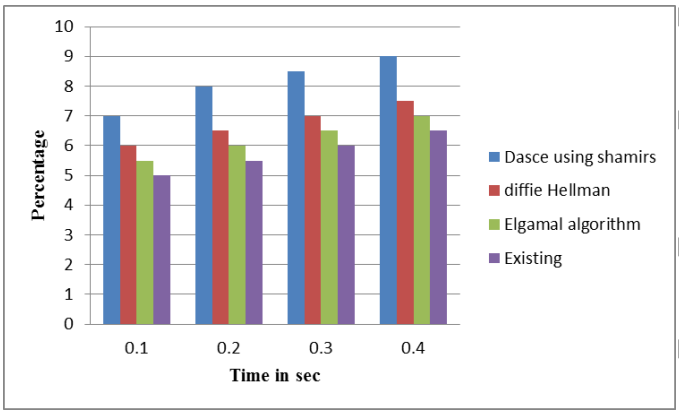


Figure 1.2: Proposed and Existing results

The above mentioned figure1.2 shows more security than the existing system when compared to the proposed technique**.**

V. CONCLUSION

In cloud computing Data Security in Cloud Environment (DaSCE) protocol is a cloud storage security system that provides key management, access control, and file assured deletion. Assured deletion was based on policies accompanying with the data file uploaded to cloud. On revocation of policies, access keys were removed by the Key Manager that results in halting the access to user data. Therefore, the files were logically deleted from the cloud. The key management was accomplished using shamir's (*k, n*) secret sharing mechanism. The analysis highlighted some problems in key management of FADE. DaSCE improved key management and authentication processes. In future, the DaSCE approach can be extended to secure group shared data and secure data forwarding.

REFERENCES

[1] Mazhar Ali,Saif U. R. Malik, Samee U. Khan (2015), "DaSCE: Data Security for Cloud Environment with Semi Trusted Third Party," *IEEE Transactions on Cloud Computing, , Vol. 77, No. 4, pp. 541-580.*

[2] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang (2014), "Securely Outsourcing attribute-based encryption with check ability," *IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 8, pp. 2201–2210.*

[3] D. Thilakanathan, S. Chen, S. Nepal and R. A. Calvo (2014),"Secure data sharing in the cloud,"" Security, Privacy and Trust in Cloud Systems, chapter, Part 1, pp. 45-72, 2014

[4] Juels and A. Opera (2013), New approaches to security and availability or cloud data, *Communications of the ACM, Vol.56,No.2, 2013,pp.64-73.*

[5] Minu George, Dr. C.Suresh Gnanadhas, Saranya.K (2013), A Survey on Attribute Based Encryption Scheme in Cloud Computing, *International Journal of Advanced Research in Computer and Communication Engineering,Vol. 2,pp.25-43.*

[6] Ashish Kumar(2012), "World of Cloud Computing & Security," International Journal of Cloud Computing and Services Science (IJ-CLOSER)Vol.1, No.2, pp. 53~58.

[7] Y.Tang, P.P.Lee, J.C.S.Lui, and R.Perlman (2012), "Secure Overlay Cloud Storage with Access Control and Assured Deletion," *IEEE Transactions on Dependable and Secure Computing, Vol.9, No.6, Nov. 2012, pp.903-916.*

[8] Shuhua Wu and Yuefei Zhu (2011), "Improved Two-Factor Authenticated Key Exchange Protocol," *International Arab Journal of Information Technology, Vol. 8, pp.66-79.*

[9] Zarandioon S, Yao D D, & Ganapathy V (2011) "K2C: Cryptographic cloud storage with lazy revocation and anonymous access." *International Conference on Security and Privacy in Communication Systems, vol.2* pp. 59-76, Springer Berlin Heidelberg.

[10] C. Caching and M. Schunter," A clo9ud you can trust," *IEEE Spectrum, Vol. 48, No. 12, 2011, pp.28-51.*

[11] S.Kamara and K. Lauter (2010), "Cryptographic cloud storage" Financial Cryptography and Data Security, *Springer Berlin Heidelberg, pp.136-149.*

[12] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Ktaz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoics and M. Zaharia (2010), "A View of Cloud Computing, " *Communications of the ACM, Vol.53, No.4, pp.50-58.*

[13] Yun, C. Shi, and Y. Kim (2009), "On protecting integrity and confidentiality of cryptographic file system for outscored storage," *Proceedings of 2009 ACM workshop on cloud computing security CCSA'09, vol.2,pp. 67-76.*

[14] G. Ateniese, M. Steiner, and G. Tsudik (2000),"New multi-party authentication services and key agreement protocols," *IEEE J. Sel. Areas Cmmun, vol. 18, no. 4, pp. 628–639.*

[15] W.Diffie,P.C.V.OorschotandM.J.Wiener(1992),"Aut hentication and authenticated key exchanges," Designs, Codes

Authors Biography

Dr.Santhi Baskaran

She received her B.E. degree in CSE from Madras University, M.Tech. degree in CSE from University of Pondicherry and

Ph.D degree in CSE from Pondicherry University. She is working as Professor in the Department of Information Technology, Pondicherry Engineering College. She is a Life member of ISTE.

A. Isaiarasi is currently pursuing as a PG Student, in the Department of Information Technology from Pondicherry Engineering College (PEC), Pillaichavadi, Pondicherry.