ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
Research Article
www.ijptonline.com

DATA SECURITY WITH MULTIPLE KEY MANAGEMENT IN CLOUD ENVIRONMENT

[1]Anshu Kumar, [2]Dr.N.Srinivasan
Department of MCA (Prof. & Head of Faculty of Computer Science & Application), Sathyabama University, Chennai.
Email:anshu.muz111@gmail.com

Received on 11-02-2016 Accepted on 20-03-2016

Abstract

Cloud computing is rapidly increasing technology and there are no boundary within cloud. Computer are used to store and process the user data can be detected anywhere on the world, depending the volumes that are needed are available in the worldwide computer networks used for cloud computing. Because of the many attractive advantages of cloud computing more users and organization are interested to use the cloud storage for storing their sensitive information. The outsourced data will be stored in remote location in cloud by users and outsourced data can be accessed by fine clients when needed. The main issue in the cloud computing is data security. Storing the data on cloud can be insecure due to use of internet by cloud related services that means minimum control over stored data. One main important worry in cloud computing is how do we snatch all advantage of the cloud while keep security controls on the organization benefits. In existing system FADE technique was used for files deletion from cloud storage when user requested for deletion. Therefore, through our study, FADE fell short on security issues of keys and authentication of joining parties. In existing system there is problem in man in the middle attack between KM and client. To overcome these issues in this paper, we propose Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE), a data security system that gives (a) management of key (b) access control, and (c) file confident deletion. Our main aim is to provide a more good, lightweight decentralized key management technique for cloud computing systems which gives more data security and management of key in cloud.

1. Introduction

Basically cloud computing is internet based technology where the infrastructure, application software and platform are revealed as software and users can entrance it by distributed cloud, as client. Cloud computing is footstep on from

usefulness computing and gives a suitable on demand network entrance to configurable computing shared pool and communication resources. Resources mention to network resources, computing application, software services, platform, computing infrastructure and virtual servers [1][2].

The data and information that is saved on cloud is very important for people with virulent intent. So security is major issue in cloud environment. A substantial calculate of conceivable particular data and secure information is keep away on Pc and the same idea is used currently in cloud for exchange the data. So comprehension the security things that the cloud provider work is very need and important. The primary thing that have to dealt with is effort to start that the supplier of cloud recently has set up. Maintaining the resources with secure management in cloud is the main important and critical issue of cloud computing. Cryptographic is a Main duty of secure management system. Therefore, while elastic capabilities, resources of self configurable, and global computing is given by cloud computing services at minimum price, they also needed for achieving various cryptographic action for the following:

- To give secure data storage that is handled by those services.
- To give secure interaction with cloud for customer with different services.

The above tasks [12] can improve the complication of the KMS (key management system) needed to support process of cryptographic for these above functions because differences in control and ownership of underlying infrastructures on which the resources and KMS are located.

To escape from the security issues in cloud computing we use powerful KMS and security on data in cloud based on DH (Diffie- Hellman) Algorithm. Key exchanging of Diffie Hellman called is called exponential key exchange. It is digital encryption method that uses numbers raised to particular ability to provide keys for decryption on the components basis that are never transmitted directly, creating the code of would-be code breaker overwhelming in mathematically. Our proposed system helps to provide good fault sufferance against Man in the middle attack, data modification and server colluding attacks. We proposed scheme of data security that operates key manager server for cryptographic keys management. The scheme of Shamir's (k, n) threshold [3] is used for keys management that uses k part out of n to reconstruct the keys. Access to data and key is protected by police file that states strategy under which permission is granted to keys. Keys of random symmetric created by client for executing integrity and encryption functions. The public keys are protected by symmetric keys, key managers regenerate the public key. Afterwards all symmetric keys

are deleted in client side. Then encrypted keys and data are uploaded to cloud. For data downloading, client gives policy to cloud storage and download the keys and encrypted data. Key managers decrypt the data and client can access the data.

2. Related Work

Author H. Abu-Libdeh stated [4] the improving popularity of cloud computing is helping organizations to outsource their data into cloud storage. Since it is very costly to switch provider of storage case for using RAIS-such as techniques used by file system and disks, but in cloud computing level minimize the switching provider cost, and better permit outages of provide or failures.

So they suggested RACS, to achieve the disadvantages in existing system. Author G. Ateniese stated [5] that establishing a representation for PDP (provable data possession) that permit a client to verify the data possesses of original data from untrusted server will be serious change in costs of I/O.

So, they suggested two provable secure provable data possession (PDP) schemes that are more better than previous solutions. Author KuiRen Suggested in his concept cloud storage allows user to outsource their data at remote location and enjoy the benefits of high quality on-demand cloud application without the load of local software and hardware management. So to overcome some issues authors used flexible storage probity auditing device, using the distributed erasure code data and homomorphic token.

In searchable encryption scheme David Wagner, Dawn Xiaodong song and Adrian Perrig on 2000[3] suggested a procedure for achieving the searching operation on encrypted data. This procedure has different advantages for provable secure in the procedure that remote server cannot get any details about the plaintext only cipher text. This procedure gives managed searching so that untrusted server not able to fetch anything without user authorization. But this method was not suitable for cloud storage due to the large data amount.

Author Quin Liu et al on 2009 proposed [4] a method, in this method it is not needed to decrypt all cipher text by user, user can only decrypt minimum amount of cipher text. In this method there will be small amounts of data loads on server.

In this method is very useful for providing the data privacy of user with efficiently. The main drawback of this system is only acceptable for singly user scheme only.

3. Proposed Work

3.1 Overview

In our proposed system we suggest a scheme of data security that uses servers of key managers for cryptographic keys management. Shamir's (k, n) scheme of threshold is used for keys management that utilizes k shares out of n to reconstruct key. Hence, cryptographic keys have to stored in well made manner and if any single end of defeat should not influence the data availability. To remove the middle attack by man user can access their data and key is protected by a file policy that states under which polices access is permitted to keys. The DaSCE creates use of both asymmetric and symmetric keys. The integrity and confidentiality services for data are given by symmetric keys which are protected by through the asymmetric keys. Pairs of asymmetric key are created by km's third party. Apart from the key pair, public key is forwarded to client. For secure keys transmission, a secret key is estimated between KM and client by STS protocol.

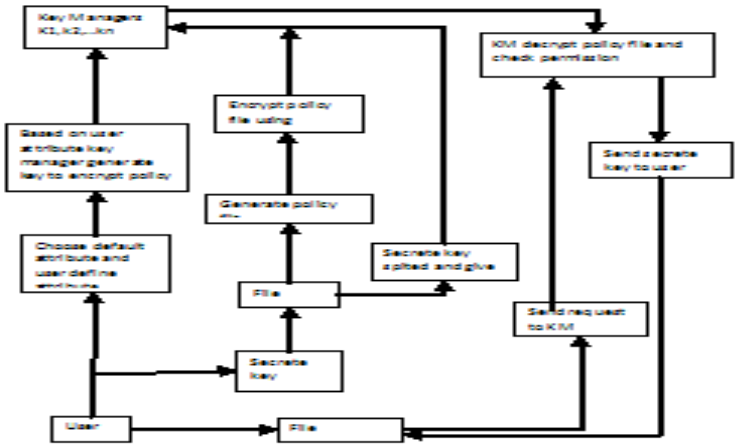

Figure1: Overall Architecture.

3.2 Elgamal Algorithm and Encryption Process

In our proposed system first user must register to become a member of cloud, once they registered user should select some attributes (e.g. email, name, address etc.., and also provide some user defined attributes to encrypt policy file that is created while file uploading process, and this attribute based encryption is achieved by ELGamal algorithm.

3.3 Elgamal Algorithm

ElGamal simplify the algorithm of Die-Hellman key exchange by suggesting a random exponent k. It is substitution for private supporter of receiving entity. Because of the simplification this algorithm can be used for encryption in one way,

without the needs of second party to actively take part. The advantage of the key here is this algorithm can be utilized for electronic messages encryption, which are forwarded by method of public store and forward services.

3.4 Key Manager Process and Share Key Values Securely

Once user uploaded the encryption data, authentication process will be achieved between KM and User for access the data by Diffis-Hellman algorithm. Now user smash up protect key into n sharew (S1,S2,..Sn). i-th share will be encrypts by public key of i-th KM then they forwarded request to Key Manager with suitable attributes. Key-Manager will verify their attributes after the authentication process, then KM will gives decrypted i-th share to user. Now user will collect their secret key and download their file and decrypt by their secret key.

3.5 Securely Process to Revocation And Renewal

In this process user will assign renewal and revocation policies ling, for achieving the policy revocation user send revocation request to KM. Revocation is nothing but user will remove all polices before user set. Revocation of user policy request sent to KM, they delete all user polices. In renewal of policy key manager will permit to renew the user before policy. Once user got approval from KM user will renew the files policy.

4. Result and Discussion

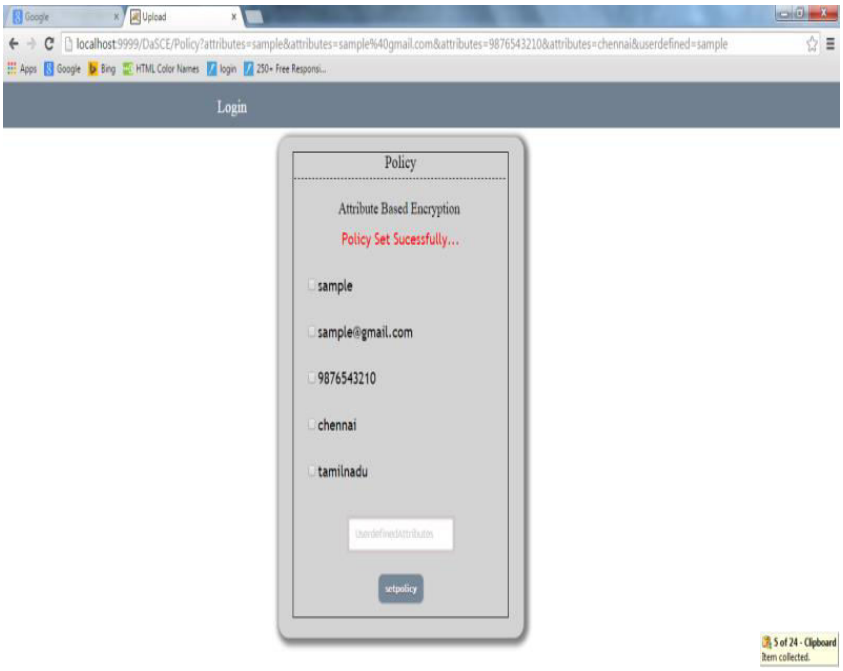

Figure 2: show policy setting based encryption.

The above figure shows the process user policy setting. Once user registration is finished then policy will be set for uploading and accessing a file.

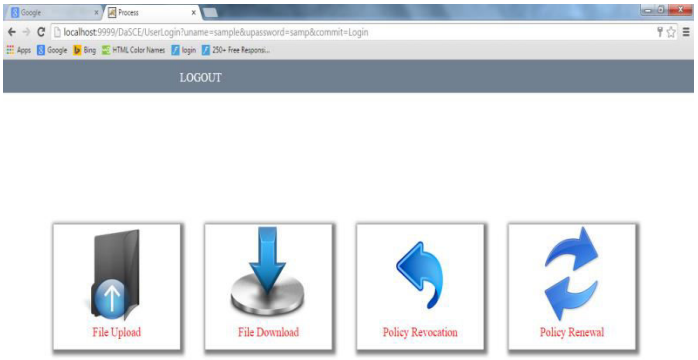

Figure 3: show user login with handle process.

The above figure shows the whole process of this system. This system shows the file uploading , file downloading , and policy renewal process. Once user upload the data then they can download the file by authorized way using key management process.

Table-1: Show proposed techniques are clod start, data sparseness and scalability.

		Time in Sec		
Technique	1	2	3	4
DaSCE and Shamir's	75	80	85	90
Diffi-Hellman algorithm	60	65	70	75
Elgamal algorithm	55	60	65	70
Existing	50	55	60	65

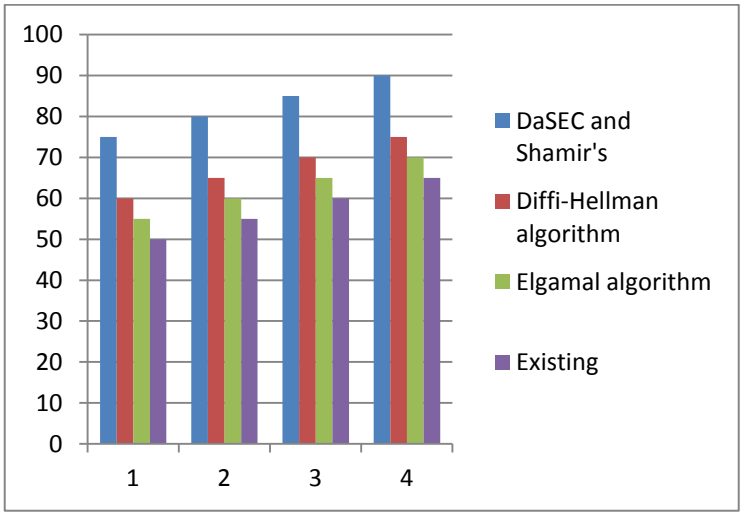

Figure 4: display proposed and existing system technique accuracy result.

Figure (3) display accuracy result between proposed and existing technique, this result show better proposed technique. All process is show accuracy percentage in proposed system.

Table-2: Display proposed and existing efficiency and quality result.

Technique	Efficiency	Quality
Proposed	80	90
Existing	60	70

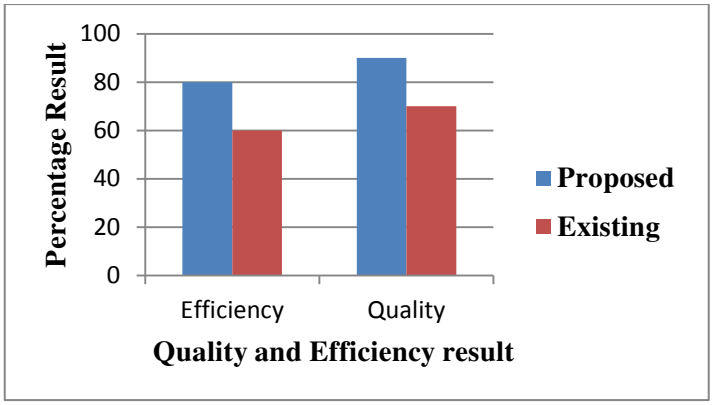

Figure 5: display proposed and existing efficiency and quality result.

This figure (4) shown more security better than existing system compare propose technique and that result is high quality in proposed system.

5. Conclusion and Enhancement

The proposed technique is providing the better enhancement within DaSCE protocol over the storage process of cloud system security which providing the controlling access, deletion of file and key management. The management over key process is accomplishing the (k, n) sharing mechanism over secret threshold. The enhanced policy for encryption of file is generating the cloud storage system for uploading. The inside policy over the file system is authenticating filename, username that being uploaded within the permission for accessing and uploading the user information. The proposed technique policy is generating the encryption key through the key manager by using several attributes.

6. References

1. M. Hogan, F. Liu, A. Sokol, J. Tong, NIST Cloud Computing Standards Roadmap – Version 1.0, Natl. Inst. Stand. Technol. Spec. Publ. 500-291, 83 pages, July 5, 2011.

2. R. Ahuja "SLA Based Scheduler for Cloud storage and Computational Services", International Conference on Computational Science and Applications (ICCSA), pp.258-262, June 2011.

3. A. Shamir, "How to Share a Secret," *Comm. ACM*, Vol. 22, No. 11, Nov. 1979, pp. 612-613.

4. D. X. Song, D. Wagner, and A. P errig, "P ract ical t echniques for searches on encrypted dat a," in SP '00: Proceedings of the 2000 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2000, pp.1- 44.

6. "RACS: a case for cloud storagediversity", byH. Abu-Libdeh, L. Princehouse and H.Weather spoon.

7. Qin Liu, Guojun Wang Jie Wu. " An Efficient privacy Preserving Keyword Search Scheme in Cloud Comput ing" IEEE DOI10.1109/CSE.2009. Internat ional Conference on Computat ional Science and Engineering-2009, pp. 715-720.

8. "Provable datapossession at untrusted stores", by G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson and D. Song.

9. Cong Wang, Ning Cao, Kui Ren, , and Wenjing Lou." Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE transact ion on parallel and distribut ed systems, vol. 23, no. 8, august - 2012, pp-1467-1479.

9. Chandramouli, Ramaswamy, Michaela Iorga, and Santosh Chokhani. Cryptographic Key Management Issues and Challenges in Cloud Services. Springer New York, 2014.

Corresponding Author:

Anshu Kumar*,

Email:*anshu.muz111@gmail.com*