



Cloud Computing Based Data Security by Using Threshold Cryptography

Jyoti J. Ghule, Jyoti R. Khebade, Sonali A. Landage, Prof. D.N.Wavhal

Department of Computer Engineering, JCEI's Jaihind College of Engineering, Kuran, India

ABSTRACT: Now a day's cloud computing is very popular in large and small scale organization as it will stored large amount of data and provide low cost service. Hence it was create daily new challenges to provide secure authorization, integrity and access control. Some approaches are ensuring about security but there are also some lack in these approaches and issues due to collusion attack, heavy computation. To resolve this issue we proposed a scheme its threshold cryptography in which data owner can divide users in group and provide single key with the using key each user in group can access the data. In these studies, we use capability list to control the access. In this scheme not only provide data security but also provide reduce number of keys.

KEYWORDS: Cloud computing, Outsourced data, Access control, Malicious outsiders, Authentication, Threshold cryptography, Capability list.

I. INTRODUCTION

Now a day's cloud computing is fast growing and data storage system as it provide storage system in very low cost .Cloud computing provides services according to three fundamental service models: Infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Storage as a service is basically a platform as a service. The five characteristics of cloud computing are: on-demand service, self service, location independent, rapid elasticity and measured scale service. The feature of cloud computing is unique. Most of the organization and institute utilized of this characteristics of the cloud computing and take benefit to gain profit [1]. Hence, industries are shifting their businesses towards cloud computing. Cloud computing uses increased day by day, however, Data security is main concern in cloud computing. Peoples are worried for stored data at cloud server. Some people believe that cloud is unsafe place and once you send your data to the cloud, you lose complete control over it [8] [9].data owner can be stored data on external server thus sometime it may be unsecured. So, confidentiality, integrity and access of data become more vulnerable. Service provides will be provide an external server that is why data owner can't trust on them as they can use data for their benefits and can spoil businesses of data owner [4]. Data users may be harmful thus data owner cannot trust on them. Data confidentiality may violet through collusion attack of malicious users and service providers. Many schemes are given to ensure these security requirements but they are suffering from collusion attack of malicious users and. To address these issues we propose a scheme. In this scheme, there are basically three entities: Data Owner, Cloud Service Provider and Users. Users are divided in location, projects and department each user use key for encryption and decrypted data. Each user in the group shares parts the key. Data will be decrypted when among the users are available on cloud server. Our proposed system focus on provide security as well as reduce the number keys. With the capability list can achieve fine-grained data access control [6]. It is basically row-based decomposition of access matrix. Authorized data which is provide by owner and operation are mentioned in capability list. It is better suit than Access Control List [5] [10] [16] because ACL specifies users and their permitted operation for each data and file. It's not suitable when two users access same type of data. In this paper, these system has been used as the Diffie-Hellman algorithm to create one time access session-key between cloud service provider and user to keep secure the data from outsiders.

II. LITERATURE REVIEW

In cloud computing mostly two important security requirements are keep data secure and efficient access control for data. Some time we focus on data security we not concentrate on system performance access control and have to focus on Data owner, Cloud Service Provider, Users. Like sometime we use among the keys for secure data. All keys are



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

confidential so need to be keep secure and maintain these keys which are additional work. These additional works affect the performance of the system. Hence it is needed to reduce these keys so our system help for reducing keys with provide data security as well as increased the performance of the system. Many schemes are suggested to meet these requirements. In [13] author define the group-key scheme. In this scheme, there is single key for the one user group for decryption process and this single key used by each user in group. These scheme help for the reduce key but simultaneously it will be cause for collusion attack as many cloud service providers can attack and there is a user a single malicious user can access the hole data of group and leak whole data of the group to Cloud Service Providers. As we know that Cloud Service Provider is not trusted party. Cloud Service Providers can access Data owner's data for the commercial benefit. In the [14] Proposed scheme can define data security and data access. In this scheme data encrypted by symmetric key and this symmetric key are only known to the Data owner and corresponding Data users. Data owner can encrypted data same will be uploaded on cloud server. Cloud Service Provider can't see data stored at it as data are encrypted. Data are further encrypted by one time session key which is secret shared with the Cloud Service Provider and User by the modified Diffie-Hellman protocol to protect data from outsiders during the transmission between Cloud Service Provider and User. This proposed system provide security undoubtedly but the description key has been available with each user so among of the users included in some applications, hence number of keys may increase. Hence, increases the maintenance and security Concerns of keys Communication model of the proposed scheme some how matches with it [4] but proposed scheme is more secure and reduces number of keys. Our system useful for those application where data will be used in large amount where work done in team ex: software industries. You may think proposed scheme has limited applications but it is not as such. Threshold cryptography can use when group of users access data. Such as software and hardware industries, medicals, institutes, banks and large fields. There is provide hierarchy of access which is reliable and useful. For Example, university has Hods, teachers, clerk, counselor and students. Each one has different level of access right.

III. IMPLEMENTATION DETAILS

We suppose that our model is composed of three entities: Cloud Service Provider, Data Owner and many Users associated with Data owner. Initially, all Users are registered at data owner. During registration users send their credentials to Data owner. We assume that user's credentials are sent securely to Data owner. Data owner then divides users in groups and provides encryption keys, tokens, algorithm (MD5) and other necessary things for secure communication to user groups in response of registration. A user can get data from Cloud Service Provider in a confidential manner after successful authentication of him self at Cloud Service Provider. We assume that Cloud Service Provider has a large capacity and computational power. We also assume that no one can breach the security of Cloud Service Provider. Further we assume that the algorithm which is used to generate the secrete keys for encryption is secure at data owner. Data owner has storage capacity to store some files and data and he can execute programs also at Cloud service provider to manage his files and data. We are using modified Diffie- Hellman and public key cryptography to secure communication between Cloud service provider and User. Modified Diffie-Hellman protocol is used to create one time session-key between Cloud service provider and User. Fig.1 illustrates the secure communication between entities in the proposed scheme.

We present a complete model for secure communication between different entities and secure access to data. There are four algorithms in the proposed scheme. Algorithm 1 describes secure communication of data between Data owner and Cloud service provider moreover this algorithm insures data confidentiality and authentication of Data owner and Cloud service provider. Algorithm 2 describes procedures which Data owner and Cloud service provider apply after a new file creation in respect. Algorithm 3 describes about secure communication of data between Cloud service provider and User. In this algorithm user's authorization is also checked. Algorithm 4 describes the threshold cryptography technique for decryption of a user's file. Algorithm 4 is applied at user side where number of keys is reduced (one key corresponding to one group) and no threat of collusion attack as in group-key Scheme.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

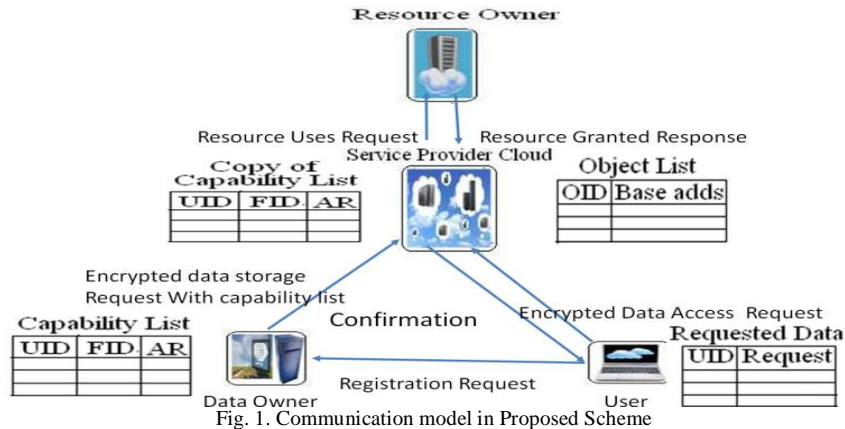


Fig. 1. Communication model in Proposed Scheme

IV. ALGORITHMS

A. Algorithm 1: Procedure to be followed by Cloud service provider after getting encrypted file and capability list from Data owner.

Step 1: Cloud service provider stores encrypted data and capability list which are received from Data owner.

$$\text{Array} \leftarrow \text{Rece}(\text{Ek}_{\text{PuCSP}}(\text{Ek}_{\text{PrDO}}(\text{EK}_{\text{KT}}(\text{Fi})) \parallel (\text{CPList})))$$

$$\text{CPList} \parallel \text{EK}_{\text{KT}}(\text{Fi}) \leftarrow \text{Dk}_{\text{PrCSP}}(\text{Dk}_{\text{PuDO}}((\text{Array})))$$

Step 2: Cloud service provider updates the encrypted file list.

$$\text{Encrypted File List} \leftarrow \text{Encrypted file list (FID, Base Adds.)}$$

Step 3: Cloud service provider updates capability list

$$\text{CPList} \leftarrow \text{CPList (UID, FID, AR)}$$

Algorithm 1 describes the process what Cloud service provider do after getting encrypted data and capability list from the Data owner. Cloud service provider decrypts the message using its own private key and the public key of Data owner and stores the encrypted data and Capability List in its storage. Cloud service provider then updates the encrypted file list and capability list. Since, Data are encrypted using Symmetric key (KT) which is known only to Data owner and respected User group, Cloud service provider can't see data even though user's credential comes through it.

B. Algorithm 2: Procedure to be followed after a new File Creation

Step 1: Data owner updates capability list.

$$\text{CPList} \leftarrow \text{Add.}(\text{CPList}, (\text{UID}, \text{FID}, \text{AR}))$$

Step 2: Now, Data owner encrypts the CPList, Encrypted File, symmetric key and sends these to the Cloud service provider.

$$\text{Send}(\text{Ek}_{\text{PuCSP}}(\text{Ek}_{\text{PrDO}}(\text{CPList}, \text{Ek}_{\text{KT}}(\text{Fi}), \text{Ek}_{\text{PrDO}}(\text{Ek}_{\text{PuUSR}}(\text{K}_s, \text{N}+1, \text{TimeStamp}))))))$$

Step 3: Cloud service provider updates its copy of the capability list, encrypted file list and sends symmetric key to indented User group.

$$\text{Send}(\text{Ek}_{\text{PuUSR}}(\text{Ek}_{\text{PrDO}}(\text{Ek}_{\text{PuUSR}}(\text{K}_T, \text{N}+1, \text{TimeStamp}))))$$

Step 4: Now, the user can send actual access request for te file directly to the cloud service provider. Users of the user group then decrypt the message and get their own parts of the symmetric key (KT). To avoid man-in-middle and replay



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

attack we use once and timestamp in each message. After getting the details, user can request to cloud service provider for data.

C. Algorithm 3: Algorithm for secure data exchange between CSP and User by using Modified Diffie-Hellman key exchange.

Step 1: User sends data access request to Cloud service provider.
Send(UID, FID, AR))

Step 2: Cloud service provider matches UID, FID, AR with CP List stored at it.
If(match)
Go to step (3)
else
Go to step (6)

Step 3: Cloud service provider initiates D-H exchange with that User and shares one time shared session key(KS)

Step 4: Cloud service provider encrypts the encrypted File with shared session key and sends it to User
Send($E_{k_{KS}}(E_{k_{KT}}(Fi))$)

Step 5: User decrypts the File and calculates the message digest of that File
If
Calculated digest matches with stored digest then File is original
else
File is modified and user sends "Error Notification" to Data owner.
Step 6: Cloud service provider sends 'invalid request' message to User.

D. Algorithm 4: Algorithm for Decryption of a File for User 1

Step 1: User 1 receives encrypted file.
 $M \leftarrow \text{Rece}(E_{k_{kt}}(Fi))$

Step 2: Initially, all bits of PKS Vector is zero. Here, PKS vector indicates parts of the key. User 1 will update this PKS vector with the components he has $PKS = PKS \text{ OR } A_1$.

Step 3: User 1 forwards M and PKS to i^{th} user of the group. Who will decrypt it and update the PKS Vector.
 $M = D_{k_{KT1}}(M)$
 $PKS = PKS \text{ OR } A_i$
The i^{th} user then forwards M and PKS to next user in the group. The next user performs same operations as i^{th} user did. This process is continued.

Step 4: if($PKS = 11111\dots\dots\dots$ up to d bits)
Go to step (5)
else
Go to step (3)

Step 5: Forward M to the user 1
User 1 then decrypts message (M) and get file

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

$$F_i = D_{k_{T2}}(M)$$

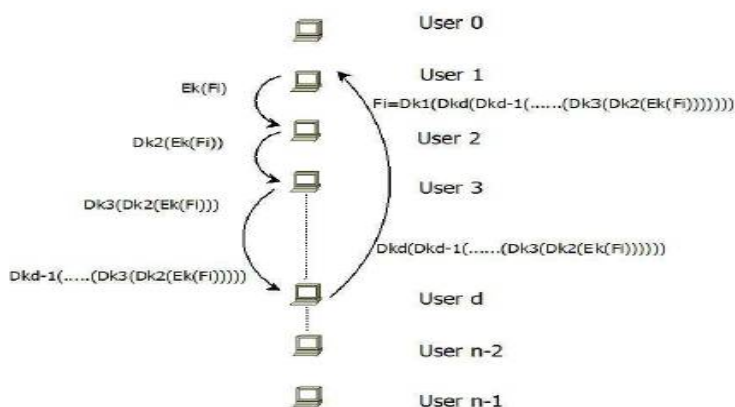


Fig.2. Process of Description

V. EXPERIMENTAL RESULT

We have developed project to prevent the unauthorized access of file stored on the cloud storage. To upload the file on cloud storage user need to login to the system and enter the cloud id for which he is going to registered.



Fig.3. User Login to Cloud Server

The second image shows the options available to the data user when he login to the cloud server. The data owner can view the access rights details and can see the capability list of cloud user.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

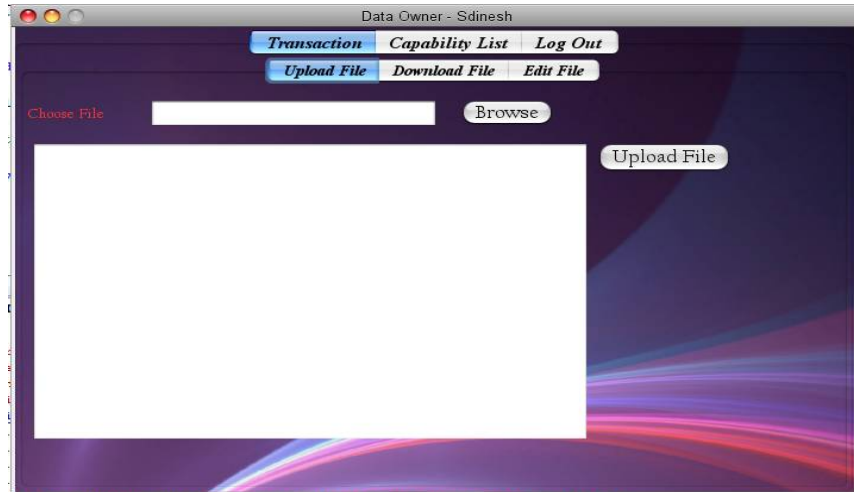


Fig.4. Process Of Description

When user request for particular file then cloud data owner can decide is to approve the rights or not. If owner deny the access rights then user can not able to download the file.



Fig.5. Admin providing access rights to user

VI.CONCLUSION

In this paper, we presented a new approach which provides security for data outsourced at cloud service provider. Some approaches are given to secure outsourced data but they are suffering from having large number of keys and collusion attack. By employing the threshold cryptography at the user side, we protect outsourced data from collusion attack. Since, Data owner stores its data at cloud service provider in encrypted form and, keys are known only to data owner and respected users group, data confidentiality is ensured. To ensure fine-grained access control of outsourced Data, the scheme has used capability list. Public key cryptography and MD5 ensure the entity authentication and data integrity respectively. Public key cryptography and D-H exchange protected the data from outsiders in our approach. No of keys



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

(because in threshold cryptography, there is a single key corresponding to each group) have reduced in the proposed scheme.

VII.FUTURE SCOPE

We have discussed the approach for security of authentication but threshold cryptography divide secret and store in different server. That means server is trusted entities but some authorized user itself changes the key structure that is stored as part of secret on server then next time some authorized user uses that secret to part reconstructed .but that key cannot be formed because one or more part of secret are not original secret that are involved to reconstruct key. We can enhance this work for identification and detection of cheater among share holder that holds the part of secret.

ACKNOWLEDGMENT

We express my sincere thanks to my project guide **Prof. D. N Wavhal** who always being with presence & constant, constructive criticism to made project successful. We would also like to thank all the staff of **Computer Engineering Department** for their valuable guidance, suggestion and support through the project work, who has given co-operation for the project with personal attention. We again take it as great privilege to express our heartfelt thanks to our Principal and Head of Department for their valuable suggestion for developing project at every state. Above all we express my deepest gratitude to all of them for their kind-hearted support which helped me a lot during project development. At the last. We are thankful to our friends, colleagues for the inspirational help provided to me through a project work.

REFERENCES

- [1] J. Do, Y. Song, and N. Park, "Attribute Based Proxy Re-encryption for Data Confidentiality in Cloud Computing environments," Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First 206 ACIS/JNU International Conference on, vol., no., pp.248-251, 23-25 May 2011.
- [2] A. Shamir, "How to share a secret," Communications of the ACM, v.22 n.11, p.612-613, Nov. 1979. [Online]. Available :<http://portal.acm.org/citation.cfm?id=359168.359176>.
- [3] N. Bennani, E. Damiani, and S. Cimato, "Toward Cloud-Based Key Management for Outsourced Databases," Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual, vol., no., pp.232-236, 19-23 July 2010.
- [4] S. Sanka, C. Hota, and M. Rajarajan, "Secure data access in cloud computing," Internet Multimedia Services architecture and application (IMSAA), 2010 IEEE 4th International Conference on, vol., no., pp.1-6, 15-17 Dec. 2010.
- [5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005.
- [6] C. Hota, S. Sanka, M. Rajarajan, and S. Nair, "Capability-Based Cryptographic Data Access Control in Cloud Computing," Int. J. Advanced Networking and Applications Volume: 01 Issue: 01 Page: (2011).
- [7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Association Computing Machinery, in Proc. of CCS'06, 2006.

BIOGRAPHY

Ms. Jyoti Ghule is BE, Student at Computer Department., Jaihind College of Engineering, Kuran, Maharashtra, India

Ms. Jyoti Khegade is BE, Student at Computer Department.,Jaihind College of Engineering, Kuran, Maharashtra, India

Ms. Sonali Landge is BE, Student at Computer Department., Jaihind College of Engineering, Kuran, Maharashtra, India

Prof. D. N. Wavhal Assistant Professor at, Computer Department. Jaihind College of Engineering, Kuran, Maharashtra, India