Secret Sharing and Splitting Based Data Security In Cloud Computing

Rohit Gautam, Ritwik Kumar, Anup Pillay, Anurag Raj

Rohit Gautam, Information Technology, SKNSITS, Maharashtra, India
Ritwik Kumar, Information Technology, SKNSITS, Maharashtra, India
Anup Pillay, Information Technology, SKNSITS, Maharashtra, India
Anurag Raj, Information Technology, SKNSITS, Maharashtra, India

ABSTRACT

Cloud computing provide low cost storage and computational space. Confidentiality, integrity and access control are the main challenges in cloud. In cloud computing, there are three types of services PaaS, IaaS and SaaS. Data security is a major obstacle in the way of cloud computing ,people are still fearing to exploit the cloud computing.To place these issues related to cloud computing. In our Project, we are performing in IaaS i.e. Infrastructure as a service. IaaS is take the servers on rent instead of buying them directly and pay for the use. We can't trust on cloud service provider because CSP can attack the system and he/she has got all the access rights, for this user might not be comfortable handling over their data to third party. Here to deal with these challenges we use threshold cryptography method. We transfer the data in encrypted format to CSP with the help of keys ,by using threshold cryptography three times encryption is provided and upload on cloud. Data confidentiality and access control are two basic security requirements for outsourced data in cloud computing .Sometime, when we emphasize more on security of data, we forget about performance of systems (DO, CSP, users). In which each keys are divided into group which is used to decrypt the data by user from CSP and there is capability list to control the access. Data confidentiality is achieved and amount of keys are reduced. By implementing these techniques of control access, message digest technique, encryption thrice, we can overcome all problems of security.

Keyword : - *Access Control , Capability List , Integrity, and Confidentiality.*

1. INTRODUCTION

Data confidentiality and access management are 2 basic security needs for outsourced data in cloud computing. Sometime, once we emphasize additional on security of data, we have a tendency to ignore performance of systems (DO, CSP, users). As an example, to secure data, we have a tendency to someday use too several keys. We all know that keys are confidential, therefore there's have to be compelled to secure and maintain these keys that are further work. These further works have an effect on the performance of the system. So, it's fascinating to scale back no of keys. So, there's want a scheme that has not solely data security however additionally maintain the performance. Several schemes are prompt to full fill these needs. The scheme proposed in [13] is the group-key scheme. In group-key scheme, there is a single key corresponding to each group of users for decryption process and all users of the group know that key. Here, number of keys is reduced but there is a problem of collusion attack of CSP and a user because a single malicious user can leak whole data of the group to CSP. We know that CSP is not trusted party. It can use data owners data for its commercial benefits. The scheme proposed in [4] tried to achieve data confidentiality and access control. In this scheme, data are encrypted by symmetric keys and symmetric keys are known only to data owner and corresponding data users. The encrypted data are stored at CSP. CSP can't see data stored at it as data are encrypted. Data are further encrypted by one time secrete session-key shared between CSP and user by the modified Diffie-Hellman protocol to protect data from outsiders during the transmission between CSP and user. This scheme no doubt provides whole data security but there is associated a key corresponding to each user and users may be large in number in some applications. So, number of keys may increase. Hence, increases the maintenance and security concerns of keys. Communication model of the proposed scheme somehow matches with it [4] but proposed scheme is more secure and reduces number of keys. The proposed scheme is useful for those applications where works are done in team and group such as in software industries. You may think proposed scheme has limited applications but it is not as such. It is applicable all where you can group users on some basis and can apply threshold cryptography technique. For example and university have vice-chancellor, hods, teachers, clerklier-staff and students. Each one has different level of access right.

1.1 PROJECT SCOPE

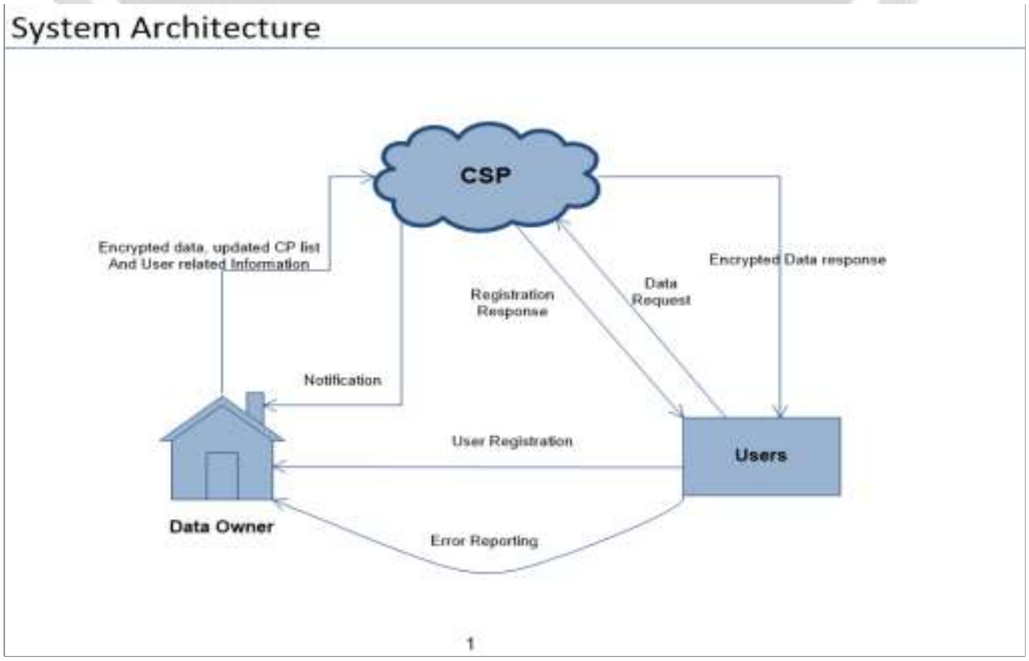
The objective of the system, firsts is to remove all data storage threats for ensuring the confidentiality, integrity and access control of the data. Also our system uses threshold cryptography in which data owner divides users in groups and gives single key to each user group for decryption of data and, each user in the group shares parts of the key. Also we use capability list to control the access. This scheme not only provides the strong data confidentiality but also reduces the number of keys.

1.2 MOTIVATION

The goal of the semantic Web is to endow the current Web with metadata, i.e., to evolve it into a Web of Data. Currently, there is an increasing popularity of semantic-web ontology, chiefly in the context of Linked Open Data, and they focus on a variety of domains, such as government, life sciences, geographic, media, or publications. Semantic web ontology build on the so-called semantic-web technologies, i.e., RDF, RDFS, and OWL ontology languages for modelling structure and data, and the SPARQL query language to query them. For the sake of brevity, we refer to semantic-web ontology's as anthologies. Ideally, anthologies are shared data models that are developed with the consensus of one or more communities; unfortunately, reaching an agreement in a community is not a trivial task. Furthermore, new anthologies try to reuse existing anthologies as much as possible since it is considered a good practice; unfortunately, it is usual that existing anthologies cannot be completely reused, but require to be adapted. Due to these facts, there exists a variety of heterogeneous anthologies to publish data on the Web, and there is a need to integrate them.

2. SYSTEM DESIGN

This low level diagram is basically the architecture diagram, which include Data Owner, CSP, and Users. Here it shows the data flow of the encrypted data. Here first of all the admin register itself in data owner and encrypt the data and sends to the cloud. And the cloud further sends the data to the users.



Char 1

High Level Diagram

The second diagram shows the sub functions performed by the Data Owner, CSP and Users.

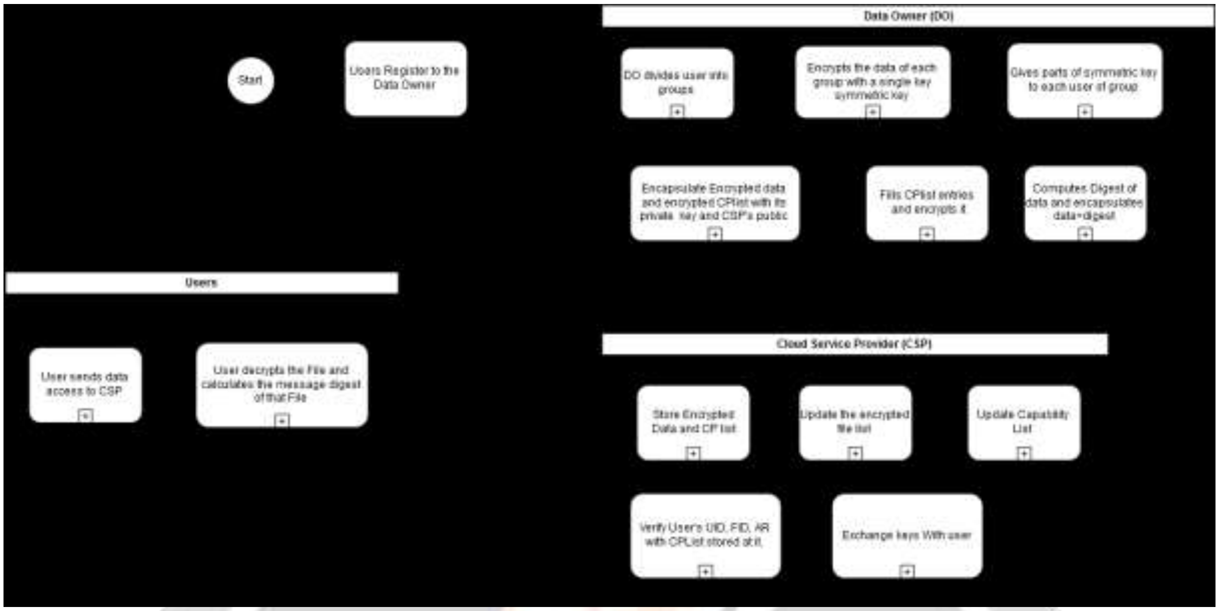

Start
Users Register to the Data Owner
Data Owner (DO)
DO divides user into groups
Encrypts the data of each group with a single key symmetric key
Gives parts of symmetric key to each user of group
Encapsulate Encrypted data and encrypted CPlist with its private key and CSP's public
Fills CPlist entries and encrypts it
Computes Digest of data and encapsulates data+digest
Users
User sends data access to CSP
User decrypts the File and calculates the message digest of that File
Cloud Service Provider (CSP)
Store Encrypted Data and CP list
Update the encrypted file list
Update Capability List
Verify User's UID, FID, AR with CPList stored at it.
Exchange keys With user

Fig -1: **Low Level Diagram**

2.1 SOFTWARE REQUIREMENTS

1. Operating System: Windows XP/Vista/7/8 and Linux
2. Application Server: Tomcat 7.X
3. Languages Used: HTML, JavaScript, JSP
4. Scripts: JavaScript.
5. Database: MySQL
6. Database Connectivity: JDBC

2.2 HARDWARE REQUIREMENTS

1. Processor - Pentium III
2. Speed - 2.1 GHz
3. RAM - 1 GB (min)
4. Hard Disk - 40 GB
5. Key Board - Standard Windows Keyboard
6. Mouse - Two or Three Button Mouse
7. Monitor - SVGA

SKNSITS,

3. MODULES

3.1 DATA OWNER

(a) Group creation (b) Encrypt Data (c) Define CP list (d) Upload Data (e) Exchange keys

(a) Group creation: Data owner will divide users into groups on some parameter (for ex consider on project basis). (b)Encrypt Data: In this module Data owner will encrypt data with a single symmetric key (Kt) for each group. One key for one group will be generated. (c)Define CP list: In this module DO (Data owner) will define the access rights for each member of corresponding group. All information such as user id, file id, access rights will be stored in CP list (d) Upload Data: In this module encrypted bundle (data +digest +cp list) is uploaded from data owner to the cloud. (Data is outsourced to cloud) (d)Exchange keys: In this module data owner will share/exchange keys with CSP (Cloud Service Provider) and User using modified Diffie-Hellman algorithm.

3.2 CLOUD DERVICE PROVIDER

(a) Save Data (b) Update Lists (c) Send data
(a)Save data In this module CSP will receive data/bundle from data owner and decrypt the bundle using Do public key. The data received from DO is saved on cloud.
(b)Update Lists In this module CSP separate out the bundle by decrypting the outer encryption
And will update various lists such as file lists, cp lists etc.
(c)Send data in this module CSP will accept requests from users and will provide requested data (encrypted data) to Corresponding user.

3.3 USER

(a) User Registration (b) Login (c) File access request (d) Read/Write intended files (e) Download (f) Decrypt the file
(a)User Registration In this module new user register the information in order to use the cloud for accessing files Uploaded by DO (Data Owner). SKNSITS, Department of Information Technology, 2015-16 7 Secret Sharing and splitting based data security in cloud computing (b)Login In this module user can login by using his/her username and password. (c)File Access Request In this module each user can request for accessing the file and requirements to the cloud service provider. (d)Read/Write intended files In this module each user can read or write the files assigned to the group. Read or write privileges are be defined by data owner in Capability list (e)Download In this module each user can download encrypted data/ file from cloud service provider. (f)Decrypt the file In this module user will request other members for their partial keys and then after achieving a desired threshold, he/she can decrypt the file successfully.

4. CONCLUSIONS

Thus we presented a new approach which provides security for data outsourced at CSP. 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, DO stores its data at CSP in encrypted form and, keys are known only to DO 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 (because in threshold cryptography, there is a single key corresponding to each group) have reduced in the proposed scheme SKNSITS.

5. 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 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 ConferenceWorkshops (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, 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 finegrained access control of encrypted data, Association for Computing Machinery, in Proc. of CCS, 2006

[8] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc. of IEEE INFOCOM 2010, 2010

[9] H. Zhong, and H. Zhen, An Efficient Authenticated Group Key Agreement Protocol," Security Technology, 2007 41st Annual IEEE International Carnahan Conference on, vol., no., pp.250-254, 8-11 Oct. 2007.

[10] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy," O'Reilly Media, Sep. 2009.

[11] A. T. Velte, T. J. Velte, and R. Elsenpeter, Cloud computing a practical approach," Tata McGraw-Hill Edition, 2010, ISBN-13:978- 0-07-068351-8. SKNSITS, Department