Cryptographically Enforced Dynamic Access Control and traceable group data sharing in the Cloud

V.D. Kulkarni[1], Sakshi Singh[2] , Kumari Princee[3] , Jyoti Ochani[4] , Himani Pawar[5].

Abstract: Now a day's people are using their smart phones for various purposes like uploading data, sharing data, use of online services, etc. along with their primary functions. But the problem with smart phones is that they are having limited computational and storage resources. Use of cloud computing in a mobile computing environment solves this problem which also increases the capacity of mobile devices. But the major concern about the use of cloud is the security issue which also becomes the problem in the mobile cloud computing environment. We proposed a light-weighted cryptographic mechanism a proxy re-encryption to solve the data integrity, data security issues in which users have to keep only short secret keys for all cryptographic operations in the mobile cloud without the involvement of any trusted third party. Group information sharing in cloud environments has become a boiling topic in modern decades. With the recognition of cloud computing, the way to reach secure associated economical information sharing in cloud environments is a pressing drawback to be resolved. Additionally, the way to reach each obscurity and traceability is a challenge within the cloud for information sharing. This paper focuses on sanctioning information sharing associated storage for a constant cluster within the cloud with high security and potency in an anonymous manner. By investment, the key agreement and therefore the cluster signature, a piece of unique traceable cluster information sharing theme is projected to support anonymous multiple users publically clouds. On the one hand, cluster members will communicate anonymously regarding the cluster signature, and therefore the real identities of members are traced if necessary.

Keywords:

AES (Advance encryption standard) Algorithm, Keyword Extraction, Group data sharing, ECC (elliptic curve cryptography)

Introduction:

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interests of most researchers because of its low energy consumption and resource sharing characteristics. Cloud computing can not only provide users with apparently limitless computing resources but also provide users with apparently limitless storage resources. Cloud storage is one of the most important services in cloud computing, which enables the interconnection of all types of electronic products. Moreover, various forms of data information can freely flow with respect to the cloud storage service, for instance, social networks, video editing and home networks. However, little attention has been given to group data sharing in the cloud, which refers to the situation in which multiple users want to achieve information sharing in a group manner for cooperative purposes. Group data sharing has many practical applications, such as electronic health networks, wireless body area networks, and electronic literature in libraries. There are two ways to share data in cloud storage. The first is a one-to-many pattern, which refers to the scenario where one client authorizes access to his/her data for many clients. The second is a many-to-many pattern, which refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time. Consider the following real life scenario: in a research group at a scientific research institution, each member wants to share their results and discoveries with their team members. In this case, members on the same team are able to access all of the team's results (e.g., innovative ideas, research results, and experimental data). However, the maintenance and challenges caused by the local storage increase the difficulty and workload of information sharing in the group. Outsourcing data or timeconsuming computational workloads to the cloud solves the problems of maintenance and challenges caused by local storage and reduces the redundancy of data information, which reduces the burden on enterprises, academic institutions or even individuals. However, due to the unreliability of the cloud, the outsourced data are prone to be leaked and tampered with. In many cases, users have only relatively low control in the cloud service and cannot guarantee the security of the stored data. In addition, in some cases, the user would prefer to anonymously achieve data sharing in the cloud.

Related work:

Ateniese et al. [2] proposed a proxy re- encryption scheme to manage distributed file systems that attempt to achieve secure data storage in the semi-trusted party. Based on bilinear maps, the scheme offers improved security guarantees. Although the scheme provides a stronger concept of security compared with [3], it is still vulnerable under collusion attacks and revoked malicious users. In order to overcome the above vulnerabilities, an effective access control for cloud computing was proposed by Yu et al. [1], which attempts to protect the outsourced data from attackers and revoked malicious users. With respect to the key policy attribute-based encryption (KA-ABE) technique, it provides effective access control with fine-grained, scalability and data confidentiality simultaneously. Specifically, each data file is encrypted with a random key chosen by the user. Subsequently, the random key will be encrypted by the KA-ABE. An access structure and secret key maintained by the group manager are distributed to authorized users, which can be used to decrypt the outsourced data. Note that if and only if the attribute of the data satisfies the access structure can the outsourced data be decrypted. However, the scheme is designed only for a general one-to-many communication system, which makes it inapplicable for the many-to-many pattern. On the other hand, a number of studies have been proposed to protect users' privacy [4]. In [5], a traceable privacy preserving communication scheme was proposed for vehicleto- grid networks in smart grids. However, this scheme is only suitable for two entities , thus, it cannot be applied in cloud environments for the purpose of group data sharing. An example of group data sharing in cloud computing was proposed by Liu et al. [6]. In [6], a secure scheme was proposed to support anonymous data sharing in cloud computing. Both anonymity and traceability are well supported by Employing the group signature technique. In addition, efficient user changes are achieved by taking advantage of the dynamic broadcast encryption. However, this scheme suffers from the collusion attack performed by the cloud server and the revoked malicious user. In addition, compared with the broadcast encryption, we believe that the decentralized model is more suitable for data sharing in the cloud. Specifically, in [7], the key management system falls into two categories. The first is key distribution, in which the generation and distribution of the key is completely accomplished by a centralized controller. The second is key agreement, where all the members in the group fairly contribute, negotiate and determine a common conference key together. In the cloud environment, key distribution may be vulnerable since the centralized controller is the bottleneck of the system. Moreover, the large amount of computation and distribution for a common conference key may cause a large burden for the centralized controller. Many researchers have devoted themselves to the design of data sharing schemes in the cloud. But the problems existing in the above research still need to be resolved. In this paper, we focus on constructing an efficient and secure data sharing scheme that can support anonymous and traceable group data sharing in cloud computing. Note that the collusion attack is considered and addressed. Moreover, many- to many group data sharing is supported in the proposed scheme.

System Architecture:

In our system, we share a business document on the group through the cloud in a secured manner. In this system there is two modules one is Business Owner they will upload a document on a cloud with the access key.

The second one is Business client group they will access this document by a key which sanded by Owner in the decrypted format at the time download.

In our system, we share a business document on the group through the cloud in a secured manner. In this system there is two modules one is Business Owner they will upload a document on a cloud with the access key. The second one is Business client group they will access this document by a key which sanded by Owner in the decrypted fomat at the time download.

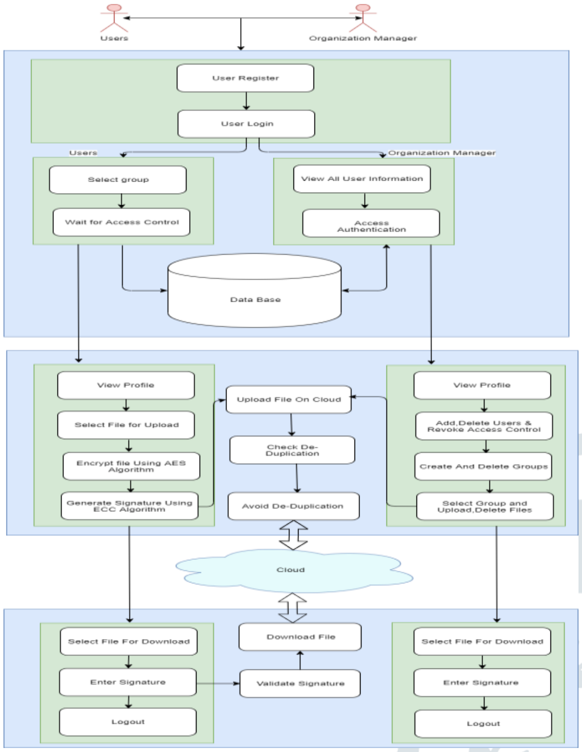

Fig. system overview.

Algorithm:

AES: AES (Advanced Encryption Standard) is a strong symmetric encryption algorithm. A secret key is used for the both encryption and decryption of data. Only someone who has access to the same secret key can decrypt data. AES encryption provides strong protection to your data.

Pseudo code :

```
Key Expansion(byte key[16], word w[44]) {word temp for(i = 0; i < 4; i + +)

w[i] = (key[4*i], key[4*i + 1], key[4*i + 2], key[4*i + 3]);

for(i = 4; i < 44; i + +)

{

 temp = w[i – 1]; if ( i mod 4 = 0) temp = SubWord(RotWord(temp)) ⊕Rcon[i/4];

w[i] = w[i-4] ⊕temp

 }

 }
```

ECC:-(Elliptic Curve Cryptography) In this proposed System we will use ECC (Elliptic Curve Cryptography) algorithm is used to generate a digital signature which is used to identify authorized user.

Conclusion: In this paper we are implementing the secure group data sharing System. We developed the diffident technique to use the system to share secure data on the cloud. It's removing the redundancy of the data and the improving the performance of the system .and we analyze in this system about secured data transition through the cloud and we can store data on a cloud with Owen access control and share this data into a group.

References:

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine- grained data access control in cloud computing," in Proc. Conf. Inf. Commun., 2010, pp. 1–9.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re- encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006.

[3] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," Eurocrypt, vol. 1403, pp. 127– 144, May 1998.

[4] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacypreserving outsourced classification in cloud computing," in Cluster Computing, 2017, doi: 10.1007/s10586-017-0849-9.

[5] H. Wang, B. Qin, Q. Wu, and L. Xu, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2340–2351, Nov. 2015.

[6] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[7] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," J. Commun. Netw., vol. 14, no. 6, pp. 682–691, Dec. 2012.