An improved Signature Schema for user Authentication and Privacy of Shared Data for Dynamic Groups in Cloud

Suri Nilima[1], G. Sivalakshmi[2]
Final M.Sc Student[1], Lecturer[2]
[1, 2] M. Sc Computer Science, Chaitanya Women's PG College, Old Gajuwaka, Visakhapatnam Andhra Pradesh

Abstract:

Now a days cloud computing provides more attractive features like scalability, low cost, flexibility and easy start for the beginners. By implementing cloud architecture it provides more security of shared data and information in the cloud. The sharing of data throughout group members to preserves data and also provides privacy from untrusted users. By providing privacy from untrusted users, it will also grants access of data from the cloud to group members. Before giving access permission of each group member, the group key manager will perform the authentication process of each group member. After completion of authentication process the group manager will generate secret key for all group members and send to all group members. Each group member will get secret key and perform the encryption process. After completion of encryption process the group member will stored the cipher format data into cloud. If any group member wants that particular file it will check access permission of group members and give the permission for download the file. In this paper we are implementing the Prime order Acknowledgment protocol for user's verification process and also get same secret key of all users. After completion of authentication and key generation process it will encrypt the shared data by using byte shuffle encryption algorithm. By implementing those concepts we can provide scalability and also provide more flexibility of shared data in cloud.

Keywords: *Signature, Authentication, Cryptography, Dynamic Groups, Cloud Computing.*

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics.

In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans.

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse

of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner, where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management. Several security schemes for data sharing on un trusted servers have been proposed. In these approaches, data owners store the encrypted data files in un trusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. Proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single- owner manner hinders the adoption of their scheme into the case, where any user is granted to store and share data. To solve the challenges presented above, we propose Mona, a secure multi-owner data sharing scheme for dynamic groups in the cloud.

Cloud Computing is recognized as an alternative to traditional Information Technology (IT) due to its intrinsic resource-sharing and low-maintenance characteristics. In this cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud computing users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures, and one of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypting data files, and then uploads the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. Many privacy techniques for data sharing on remote storage machines have been recommended. In these models, the data owners store the encrypted data on untreated remote storage. After that they will share the respective decryption keys with the authorized users. This prevent the cloud service providers and intruders to access the encrypted data, as they don't have the decrypting keys. However the new data owner registration in the above said models reveals the identity of the new data owner to the others in the group. The new data owner has to take permission from other data owners in the group before generating a decrypting key. The proposed system identified the problems during multi owner data sharing and proposed an efficient protocols and cryptographic techniques for solving drawbacks in the traditional approach. In this it proposed an efficient and novel secure key protocol for group key generation and using these key data owners can encrypt the all files. Suppose new user register into group the user need not to contact the data owner during the downloading of files and data can be encrypted with AES before uploading the data in to the cloud.

II. RELATED WORK

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers. However, security concerns become the main

constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. A cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key. However, the file-block keys need to be updated and distributed for a user revocation, therefore, the system had a heavy key distribution overhead. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users. The techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents. However, the single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others. However, the scheme will easily suffer from the collusion attack by the revoked user and the cloud.

Security is one of the main element in online computing, but only security is not enough. Users can only use inline computing if they are confident enough that there data is safe. Without the assurance of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. We can take an example that any member can mislead his other team member by sharing false files or malicious files. For this we use a property called traceability, which enables the group manager to reveal the real identity of a user. As we know sharing data only by manager in a single owned manner is not flexible so we use multi-owner manner. In our project ,we mainly concerned that the secret key is not generated again and again whenever there is a revocation, We are using a revocation list which the names of the revoked members.It is helpful in a way that whenever a relocked member try to log in or uploading files ,he is not able to do these works. This is helpful in user identity proof. Now we deal with data security, only authorized member can view or upload data and there is group signature key which distributed only to the existing members of the group, it is a combination of private key of member and group key of group and private key is generated each time whenever a new member is added to group. Using group signature key ,a member is able to upload or view a uploaded file. data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

CLOUD computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following Challenging issues. An essential driver of poor site configuration is that the web designers' understanding of how a site ought to be organized can be respectably not quite the same as those of the clients. Such contrasts bring about situations where clients can't without much of a stretch find the coveted data in a site. This issue is hard to dodge on the grounds that when making a site, web engineers might not have a reasonable understanding of clients' inclination and can just compose pages focused around their own particular judgments. Be that as it may, the measure of site viability ought to be the fulfilment of the clients instead of that of the engineers. Subsequently, Webpages ought to be composed in a manner that by and large matches the client's model of how pages ought to be sorted out. Past studies on site has concentrated on a mixture of issues, for example, comprehension web structures, discovering applicable pages of a given page, mining educational structure of a news site, and concentrating layout from pages. Our work, then again, is nearly identified with the writing that inspects how to enhance site safety through the utilization of client route information. Different works have attempted to address this inquiry and they can be for the most part characterized into two classifications: to encourage a specific client by rapidly reconstituting pages focused around his profile and traversal ways,

regularly alluded as personalization, and to alter the site structure to facilitate the route for all clients, frequently alluded as change.

III. PROPOSED SYSTEM

Proposed a scheme that provides a secure way for key distribution without secure communication channels. In which the user can securely obtain their private keys from the group manager without any certificate authority due to the verification for the public key of user. This scheme can achieve fine grained access control. This scheme uses the prime order acknowledgment protocol for user verification process and key generation. This scheme support dynamic group efficiency in which private key will not be recomputed and update at the new user joining or user revocation. In this paper we proposed a scheme that provides the anti-collision data sharing in multiuser cloud. Firstly the user registration user can register in the system in which user provides the information about him and complete the registration process system provides the user id and password to access the cloud. This information should be managed by the group manager. The uploading user uploads a data into the cloud. Before upload data into cloud each group member will encrypt the data and stored into cloud. So that only the authorized group member should be download file and decrypt it. Before performing those operations each group member will be authorized by group manager and also give the access policy for uploading, download the file. By performing the authorization and key generation process we are using prime order acknowledgment protocol. The implementation process of prime order acknowledgment protocol is as follows.

Group Member Registration Phase:

In this phase each group member will register into cloud service by providing personal information. After completion of registration process the system will provide user id and password for each group member to access the cloud servers. Those user ids and passwords will provide the accessing cloud and also provide data access from the cloud. Before accessing the data from the cloud each group member will be identified group manager and also getting secret key. By performing verification process we are implementing prime order acknowledgment protocol.

User verification and Group key Generation Phase:

In this module each group member will verified by group manager and also generates group key. By performing verification process each group member will use id and password for accessing cloud. Using id and password each group member also contact with group manager. By performing verification and key generation we are using prime order acknowledgment protocol. The verification and key generation process of prime order acknowledgement protocol is as follows.

i) Verification Process:

1. The group manager will generate public key (p) for all group members and send that public key to all group members.

2. The group member will retrieve public key and choose private key (k), base value g.

3. The generation of base values can be done by using following formula.

```
For(int i=2;i<p;i++)
 {
  If(gcd(i,p)==1)
   {
    g=i;
   }
 }
```

4. After generating g value the group member will calculate public key by using following formula.

Public key= g^k mod p

5. Each user also generate secret key by using following formula.

```
for(int i=2;i<p;i++)
{
   If(gcd (i,p-1)==1)
     {
       sk=i;
     }
}
```

6. After generating secret key the group member will choose Random Nonce (Rn) and calculate the Sa value by using following formula.

```
c= (id.hascode) mod 20000;
val=k-sk;
c1=val-c;
k1=inverse (sk, p-1);
v=c1 * k1;
 if(v<0)
   {
     Do
       {
         Sa=v+p;
       }while(v<p);
     }
  return (v % p);
```

7. After completion of Sa value each group member again calculate another public key by using following formula.

```
Int temp=1;
For(int i=1;i<sk;i++)
  {
     temp=(temp* Sa) mod p
   }
  P1=temp;
```

8. Take that public key(p1) and send the public key, Rn , Sa and public key P1 to group manager.

9. The group manager will retrieve those values and generate the individual private key(pk) of each user.

10. After generating the group key manager will generate public key Rb of individual users by using following code.

```
int temp=1;
For(int i=1;i<Rn;i++)
 {
    temp=(temp* pk) mod p
}
Rbi=temp;
```

11. The group manager will send those public keys to individual user.

12.The group members will retrieve that public and generate Ca, ack by using following code.

```
int temp=1;
For (int i=1;i<Rn;i++)
 {
    temp=(temp* sk) mod p
}
Ca=temp;
String ka = ""+ power (Rbi, sa,p);
  int ka1 = ka.hashCode();
 String con = cb +""+ Ca;
 int ack = ka1 + Integer.parseInt(con);
```

13. After generating ack and Ca values each group member will send those values to group manager.

14. The group manager will retrieve Ca and Ack from group members and verify by using following code.

```
String kb= “”+power(P1,pk,p);
 String kb1=kb.hashcode ();
 String cn=Rbi+””+ Ca;
  Int ack1= kb1+Integer.parseInt (cn);
  If(ack==ack1)
  {
     Status=”Authenticated User”;
  }
  Else { Status=”Not Authenticated User”; }
```

15. After completion of verification process the group key manager will generate keys for individual by using following code.

```
int temp=1;
for (int i=1; i<=pk; i++)
 temp= (temp*Ca) %p;
keyi= temp;
```

By calculating individual secret key of each group member, using those key_i the group key manager will generate group key for all users.

ii) Group key Generation:

The group key manger will take all key_i and generate one signal group key. The generation of group key is as follows.

groupkey= key_1 ® key2 ® ……® key_n

After generating group key the group key manager will generate secret point for individual users by using given code.

```
x1=groupkey/public key;
y1=groupkey/public key;
```

Take the (x1, y1) point and send that point all group members.

Encryption and Decryption Process:

In this module group members will encrypt and decrypt the shared data. Before sharing the data or information we should encrypt and stored into cloud server. After storing data into cloud server we can retrieve and decrypt the data. For the completion of decryption process we should get original data. Before performing the encryption and decryption process each group member will retrieve the secret points from the group manager. By using that secret point each group member will generate group key. The generation of group key is as follows.

```
groupkey= x1*p+y1;
```

After getting group key the group member will choose the upload file and encrypt that file. By performing the encryption process we can use the rijendeal algorithm. After completion of encryption process that file will be stored into cloud server. If any other group member wants to particular file will be retrieve and perform the decryption process of rijendeal algorithm. By performing decryption process it will get original file without loss of information. By implementing those concepts we can improve the scalability, feasibility and low cost for building the cloud computing.

IV. CONCLUSIONS

In this paper we are design an efficient secure anti collusion schema for provide security of sharing data. In our schema we are implementing mainly three concepts are group member's verification process, group key generation process, encryption and decryption of shared data. Before sharing the information between the group members each member will be verified by the group manager. After completion of verification process the group key manager will generate secret points for each group member. Using those secret points each group member will generate secret key. Each group member using that group key or secret key encrypts the data and stored into cloud server. The cloud server contains all information within format of cipher and if any group member wants the particular file retrieves. After retrieve that file the group member will decrypt and get original file. By implementing those concepts we can provide more security of shared data and low cost.

REFERENCES

[1] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[2] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[3] Varun and Vamsee Mohan.B," An Efficient Secure Multi Owner Data Sharing for Dynamic Groups in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 730-734

[4] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[5] Zhongma Zhu and Rui Jiang, "A secure anti-collusion data sharing scheme for dynamic groups in the cloud", IEEE Transactions on parallel and distributed systems, vol.27, no.1, January 2016

[6] Yong CHENG, Jun MA and Zhi-ying "Efficient revocation in cipertext-policy attribute-based encryption based cryptographic cloud storage" Zhejiang University and Springer-Verlag Berlin 2011

[7] Zhongma Zhu and Rui Jiang," A Secure Anti- Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems DOI:10.1109/TPDS.2015.2388446.

[8] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[9] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions On Parallel and Distributed Systems, Vol.24, No. 6, June 2013.

[10] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc.Int'lConf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.