ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

A Reliable Cloud Data Sharing Scheme Ensuring Security for Frequent Change of Membership

Kanchan Govinda Vaidya[1], P. Jyotheeswari[2]

[1]M.Tech Student, Dept. of CSE., SVCET (Autonomous), Chittoor, JNTUA, A.P, India

[2]Associate Professor, Dept. of CSE., SVCET (Autonomous), Chittoor, JNTUA, A.P, India

ABSTRACT: The basic service provided by the Cloud is Data Storage. Cloud computing offers efficient, well-organized and cost-effective solutions for sharing resources between cloud users. However, it is a difficult task for sharing data in multi-owner manner where group manager and all group members can store and modify data while preserving data and identity privacy from an untrusted cloud server, due to the frequent change of the membership. Therefore, a reliable cloud data sharing scheme ensuring security for frequent change of membership have been proposed which involves the integration of group signature and dynamic broadcast encryption techniques. In the meantime, the storage overhead and encryption computation cost are not affected with the number of revoked users. We introduce multiple read and write on the content of data stored and allow data owner to create set of Access Control Policy based on ABAC which helps from different malicious attack.

KEYWORDS: Cloud computing, multi-owner manner, group signature, dynamic broadcast encryption, access control policy

I. INTRODUCTION

Cloud computing based solutions are becoming popular and adopted widely due to its low-maintenance, resource-sharing management and cost-effective characteristics. Cloud users can be benefitted from high-quality services, access resources like hardware and systems software on remote datacenters, and save significant upfront investments on their native infrastructures thus decreasing the cost for system administration and improving maximum possible resource utilization just by transferring the local data into cloud servers and with its powerful datacenters. The fundamental service provided by Cloud is data storage. Data stored in Cloud may be highly sensitive and confidential, such as medical records, business plan and social networks. It may cause a significant risk to the privacy and security of those stored files. Therefore security and privacy have always been very important concerns in cloud computing, specially, when the cloud servers maintained by cloud providers are not trustworthy.

A basic solution provided by existing system to ensure data privacy and security is encrypting the data files, and uploading the encrypted data files into the cloud server. Designing a reliable and efficient cloud data sharing scheme ensuring security and preserving privacy for dynamic groups in the cloud is not straightforward task because of the following three challenging reasons.

1. Identity privacy: The first major problem for the wide deployment of cloud computing is Identity Privacy. User privacy should be maintained properly so that the actual identities of the user cannot be disclosed easily to the various kinds of intruders and cloud service providers (CSPs). Therefore, Cloud users may be unwilling to connect in cloud based computing systems without the assurance of identity privacy. Also, unconditional user identity privacy may result in the abuse of privacy. For this reason, traceability is highly desirable for the group manager to disclose the real identity of such mendacious user.

2. No multiple-owner manner: Multiple-owner manner refers to any member in a group should be able to fully enjoy the data storing and sharing services and can be benefitted from the services provided by the Cloud. In single-owner manner, only the group manager is able to store and modify data in the Cloud. Unlike single-owner manner,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

each user in the group in multiple-owner manner is able to both read and modify his/her part of data. Therefore it is highly advisable to have multiple-owner manner.

3. Groups are dynamic in practice: Lastly, the participation of new staff and revocation of current employee makes the group dynamic in nature. The frequent alterations of membership make efficient and secure data sharing in Cloud extremely complicated and hard due to the following two primary reasons: First, new granted users are not allowed to learn the content of data files stored before their participation by the anonymous system, because it is not possible for new granted users to directly contact with anonymous data owners and obtain the corresponding decryption keys. Second, to reduce the complexity of key management it is desirable to obtain an efficient membership revocation mechanism without modifying or updating the secret keys of the remaining users.

There are several security schemes that have been proposed up-to-date for efficient and secure data sharing on untrusted servers like Plutus[5], SiRiUS[6] and Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage[7] . In all of these approaches, the encrypted data files are stored in untrusted storage and distribute the corresponding decryption keys only to authorized users by the data owners. Thus, storage server and unauthorized users have no knowledge of the decryption keys to learn the content of the data files. Also security schemes based on ciphertext-policy attribute-based encryption (CP-ABE) and key policy attribute-based encryption (KP-ABE) technique have been proposed. But, the issues of user revocation and multiple-owner manner have not been addressed in these schemes respectively.

Our Contribution: A reliable cloud data sharing scheme ensuring security for frequent change of membership have been proposed to solve the challenges presented over. The main advantages of this scheme include:

1. Data owner create set of access control policy along with data read, created and modified which helps from different malicious attack.
2. It offers multiple read and writes on the content of data stored in the cloud and assured any member in a group to secretly make use of the cloud resource as it provides the secure and privacy-preserving access control features to users. Also, when disputes occur between users, Traceability can be easily achieved as the real identities of data owners can be disclosed by the group manager.
3. Authentications of user who store and modify the data in the cloud are based on captcha and text level.
4. Frequent change of membership can be handled easily. Also, new granted users can directly decrypt data files uploaded without contacting with data owners before their participation. Novel revocation list is used to achieve the user revocation without updating the secret keys of the remaining users. Also with the number of revoked user, the computation overhead of encryption and size remains constant.

II. RELATED WORK

Kamara et al. [3] describes several architectures that integrates new and non-standard cryptographic primitives for constructing a cloud storage service securely on top of public cloud infrastructure where the service provider is not fully trusted by the customer. Generally, cloud infrastructures are categorized as private or public. Customer is responsible for managing the infrastructure and resides on- premise in a private cloud. Whereas in a public cloud, cloud service provider is responsible for managing the infrastructure is resides off-premise. It provides scalable and dynamic storage just by transferring their data to the cloud as customers can save the costs of building and maintaining a private storage infrastructure. Although using cloud storages have many benefits it introduces significant risk regarding security, privacy and integrity of data as the data stored in files may be business plan, medical record and social networks.

Yu et al. [4] offered a scalable and fine-grained data access control scheme by defining and enforcing access polices based on data attributes and KP-ABE technique which helps in achieving of user access privilege confidentiality and user secret key accountability. The combination of attribute-based encryption (ABE), proxy re-encryption and lazy re-encryption helps in acquiring and allowing the data owner to assign the computation tasks include in fine-grained data access control to untrusted server without revealing the essential contents of data. Data files are encrypted using random key by data owner. Using primitive of cryptography like key policy attribute-based encryption (KP-ABE), the random key is further encrypted with a set of attributes. Then the authorized users are assigned an access structure and corresponding secret key by the group manager. Thus, only the user with data file attributes that satisfy the access structure can decrypt a ciphertext. User revocation can also be achieved as the group manager assigns tasks of data file

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

re-encryption and user secret key update to cloud servers. Unfortunately, the multiple-owner manner is not supported as only group manager are responsible for modifying the data file shared.

A cryptographic storage system, named Plutus proposed by Kallahalla et al. [5] utilizes a cryptographic primitive that allows the sharing of files securely and protects files without having much trust on the file servers. The key characteristic of Plutus is all the files are divided into filegroups and filegroups are encrypted with a unique file-block key. All the process of key management and cryptographic operations are carried out by clients and all key distribution is handled in decentralized manner. Thus, the filegroups can be shared easily among others by providing the corresponding lockbox key by the data owner. File-block keys are encrypted using lockbox key and Plutus pre-computes the encryption of lockbox key only after the modification of the data. Although the encryption and decryption cost can be spread across different users and never involve the server, it is not flexible for large-scale file sharing system as it lead us to heavy key distribution overhead. Also considering the viewpoint of user revocation, the file-block key needs to be updated and distributed repeatedly.

Goh et al. [6] proposed a scheme called SiRiUS, a secure file system which uses hash tree constructions and offers its own read-write cryptographic access control for file level sharing, assumes the network storage is not trustworthy and improves the security of a networked file system without making any alteration to the network server. Files that are stored on the untrusted server can be described in two folds: file metadata and file data. The file metadata holds the information of access control comprising sequences of encrypted key blocks. All the sequences of encrypted key blocks are encrypted under the public key of authorized users. Therefore as the number of authorized users grows the size of file metadata also linearly increases. As the file metadata needs to be updated, it is not flexible for large-scale file sharing. Thus, user revocation is difficult to achieve with this method. The NNL construction [11], the extensions version to SiRiUS includes large scale group sharing used for efficient key revocation construction. But, it is still not flexible for dynamic group as the private key of each user needs to be recomputed when new user joins the group in NNL system. On the other hand, as the file sharing scale increase, the computation overhead of encryption also increases linearly.

To add the access control to the secure file system and distributed storage, Ateniese et al. [7] used a method named proxy re-encryptions. Blocks of content are encrypted with unique and symmetric content keys by the data owner. The resulting encrypted content keys are further encrypted under a master public key. Additionally, to grant a user's public key, the appropriate content keys from the master public key is directly re-encrypt using proxy cryptography which helps in maintaining the access control and improvement of security. To supervise access to encrypted content stored on distributed untrusted replicas, this scheme makes use of centralized access control server. The main benefits of this scheme are that they are unidirectional and only a limited amount of trust is placed in the proxy. However, a collusion attack can occur between any revoked malicious user and untrusted server allowing them to find out the decryption keys of all the encrypted blocks of content.

Secure provenance scheme proposed by Lu et al. [8] records ownerships and process history of data object. This scheme is based on the bilinear pairing techniques which rely upon group signatures and ciphertext-policy attribute-based encryption (CP-ABE) techniques. The basic feature of this scheme is to offer the anonymous authentication for user accessing the files, information confidentiality on sensitive documents stored in cloud and tracking the provenance on disputed documents for revealing the identity. Mainly, the system consists of a single attribute. After the registration, each user in this scheme obtains two keys: a group signature key and an attribute key. Using attribute-base encryption (ABE) any user can encrypt a data file. For decryption of the encrypted data, an attribute keys is used by other in the group. To accomplish privacy preserving and traceability features, the user signs encrypted data with group signature key. Unfortunately, the demerit of this scheme is that user revocation is not supported.

In [13] Dan Boneh, construct a short group signature scheme with length under 200 bytes where the signatures are nearly the standard RSA signature size with the same level of security. Group signature security of this proposed scheme is based on the Strong Diffie-Hellman (SDH) assumption and a new assumption in bilinear groups called the Decision Linear assumption. This system stands on a new Zero-Knowledge Proof of Knowledge (ZKPK) of the solution to an SDH problem where ZKPK is converted to a group signature via the Fiat-Shamir heuristic [14].

In [14] Fiat et al. proposed schemes that offers efficient solutions in terms of both transmission length and storage at the user's end. It introduces new theoretical measures for the qualitative and quantitative assessment of encryption schemes designed for broadcasting secure transmissions to an arbitrary set of recipients while minimizing key management related transmissions. The broadcast encryption scheme transmits message securely to all members of the privileged subset. The new parameter added in this scheme represents the number of users that have to collude so as to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

break the scheme. The scheme is considered broken if a user that does not belong to the privileged class can read the transmission. It also consider another scheme parameter called *random-resiliency* that refers to the predictable number of users, selected uniformly at random, that have to collide so as to break the scheme.

III. SOFTWARE SYSTEM ARCHITECTURE

The Software System Architecture presented in Fig. 1 consists of three important units namely: Cloud, Group Manager and Group Members. Cloud is managed by Cloud Service Provider (CSPs) and offers required storage service. As the CSPs are not reachable by cloud user, Cloud user basically presume that Cloud is not fully trustworthy. Cloud may attempt to gain the knowledge of the identity and content of stored data of user and assume will not modify or delete data. The set of authorized user who can store data in the cloud server and share data with others in the groups are Group Members. User need to register first. Once the group members are register, Group manager distributes key to authorized user for login the system. Group Manager is responsible for key distribution, system parameters generation, user registration and revocation, and disclosing the identity when argument occurs between owners. Group member can read and modify the file stored in the Cloud server. Group manager have the authority to revoke the user. Once revocation is performed to user, the revoked user cannot access the file from the cloud.

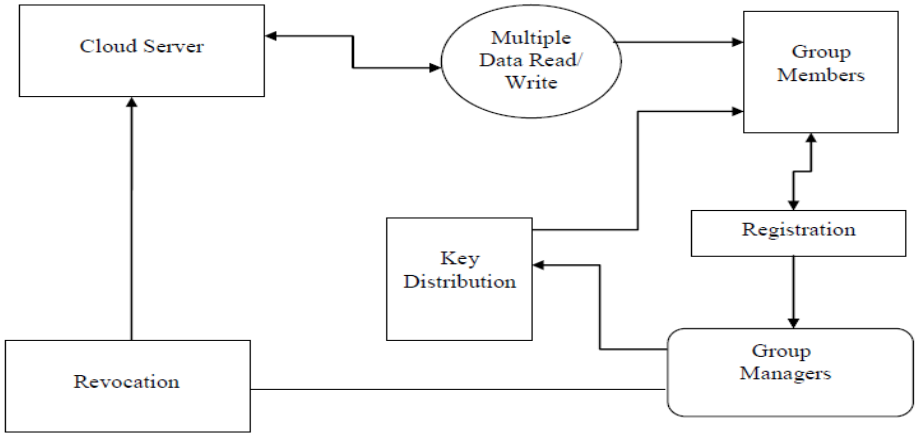

Fig. 1: Software Architecture for Proposed System

IV. PROPOSED SYSTEM

We proposed the integration of group signature and dynamic broadcast encryption techniques to acquire a reliable and secure cloud data sharing scheme for frequent change of membership. Group signature security of this proposed scheme is based on the Strong Diffie-Hellman (SDH) assumption and Decision Linear assumption that allows cloud users in the group to make use of the resources and sign messages without revealing the identity in the cloud. The dynamic Broadcast Encryption techniques uses scheme parameter called random-resiliency and carried out the process of sharing the files with other and enabling the group manager to include new user dynamically whilst protecting already computed data and information.

Group manager are compelled to calculate the revocation parameters and transfer the result in the cloud which can be publicly accessible for users. In this way, the storage overhead and encryption computation cost are not affected with the number of revoked users. Data owner can create a set of access control rules on data and send the data along with the access control policy so that the data owner can have physical access control over his data. Such a design with access control policy "lock" the data while a member attempting to make illegal copies of the data and prevent from various malicious attacks. This design also support multiple read, create and write on the data stored in the cloud server and authenticate the member based on the captcha and text level for storing and updating the data.

The Fig. 2 represents the use of access control policy/rules on data where only register group member can read, create and modify the data. Authorized member send the data request (D_{req}) to the cloud server. The cloud server grants the access control key along with the data (D_{rec} + AC_k) to the register member. The member needs to perform

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

encryption using encrypted key (E_k) for read and modify the data. Only the group member having the encrypted key distributed by group manager after the verification and authentication using captcha and text level can encrypt the data. The register member can create a new data (C_n) by setting his/her own access control policy and stored in the cloud. In the similar way, register member modify data (D_m) and sends along with access control policy and update the cloud server.

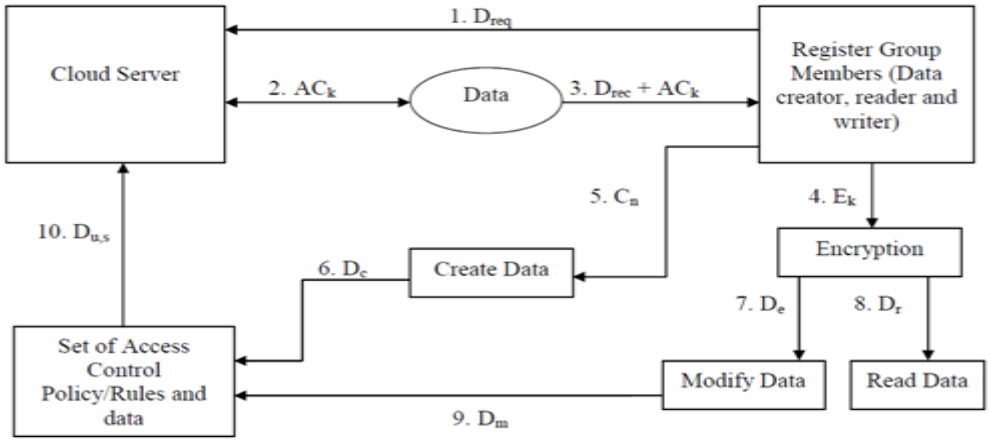

Fig. 2: Use of Access Control Policy on data

1. D_{req} = Request data,
2. AC_k = Access Control key
3. $D_{rec} + AC_k$ = Receive data and Access key
4. E_k = Process for Encryption
5. C_n = Create new data
6. D_c = Created data
7. D_e = Encrypted data
8. D_r = Read data
9. D_m = Modified data
10. $D_{u,s}$ = Update and store data to cloud
11.

Attribute Based Access Control (ABAC) method is used in our proposed system to create a set of access control policy. Attribute based access control extends role based access control especially with the features including delegation of attribute authority, decentralization of attributes and interference of attributes. ABAC provides policies for sensitivity of credentials allowing organization to maintain their autonomy while collaborating efficiently. In addition, it provides an automated trust negotiation, which is auditable as and when that capability is required.

The Fig. 3 illustrates the working mechanism of access control policy before updating and storing the data files in the cloud. The attribute of register group member and data to be created and modified is provided to ABAC mechanism along with the Access Control Policy and Environment condition. ABAC mechanism consists of Policy Enforcement Point and Policy Decision Point which evaluates the attributes, access control rules and environment condition to provide access control decision/policy. Policy Decision Point (PDP) is responsible for computing access decisions by evaluating Digital policy and Meta policy. Policy Enforcement Point (PEP) is responsible for enforcing policy decisions in response to a request from a register group member requesting access to resources.

The attributes of the subject may contain the identifier, name, organization, and the other information. The attributes of the object may include the type, name classification and so on. The attributes of the resource may include resource name, identifier, and other information. And the attributes of the environment condition may contain current date, time, and federated domains.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

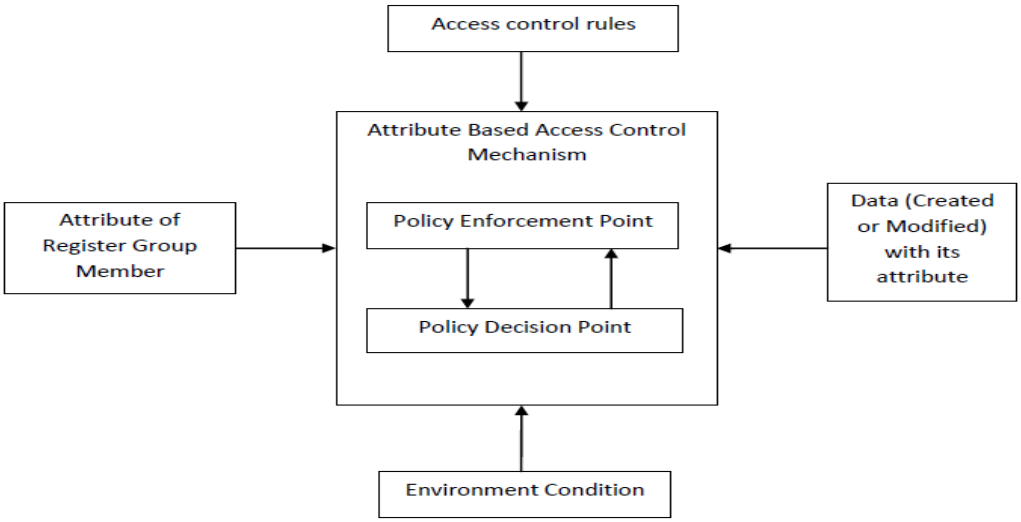

Fig 3: Working Mechanism of Access Control Policy

V. DISCUSSION

The use of access control policy/rules along with newly created and modified data gives the data owner physical access control over his data. Therefore, group member having access to the data can utilize the content of data files in such a way that abide the rules of access control policy set by the data owner. Such a design with access control policy "lock" the data if a member attempting to make illegal copies of the data and prevent data from various malicious attacks and mendacious user. User revocation can be acquired easily as group manager are compelled to compute the revocation parameter and make the result publicly available in cloud. Authentication of group member based on captcha and text level for storing and updating data in cloud ensures the security of data at higher level. Finally, the system proposed in this paper also supports multiple read, create and write on the data stored in the cloud server.

VI. CONCLUSION

This paper introduce a reliable cloud data sharing scheme ensuring security for frequent change of membership which involves the integration of group signature and dynamic broadcast encryption techniques. The proposed system is proficient of allowing cloud user in the group to share and store data securely and makes use of resources with others without disclosing real identity and user privacy to the cloud. Moreover, the system proposed in this paper supports dynamic group efficiently, provide features like secure and privacy-preserving access control, anonymity and traceability property for revealing the identity when dispute occurs between the cloud users. In addition, the proposed system enables group manager to include new user dynamically, preserves the already computed information by calculating the revocation parameters and migrating the result in the cloud server which can be publicly accessible for cloud users. User revocation can be easily achieved by using publicly available revocation list without updating the private key of the remaining users and a new user can directly decrypt the content of data files stored without contacting data owner in the cloud before their participation. The proposed scheme supports multiple read and writes on the content of data stored and set of Access Control policy/rules along with data created by data owner which helps from different malicious attack. Furthermore, the storage overhead and encryption computation cost remains constant with the number of revoked users.

REFERENCES

1. 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, Jun 2013.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

2. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, Vol. 53, no. 4, pp. 50-58, Apr. 2010.
3. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
4. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
5. 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.
6. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
7. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
8. 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.
9. B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.
10. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.
11. D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.
12. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
13. D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.
14. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, Proceedings of Crypto 1986, volume 263 of LNCS, pages 186–194. Springer-Verlag, Aug. 1986.
15. A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.
16. Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud" , 2014, http://www.springer.com/978-3-642-38585-8
17. B. cha, J Seo and J. Kim. 2011. Design of Attribute Based Access Control in cloud computing Environment. Proceeding of International conference on IT convergence and Security, Springer. pp. 41-50.
18. V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller and K. Scarfone. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162, January 2014.http://dx.doi.org/10.6028/NIST.SP.800-162