International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

Secure Cloud File Distribution System for Untrusted Network Environment

[1]William Asiedu, [2]Maxwell Dorgbefu Jnr.
Department of Information Technology Education
College of Technology Education, Kumasi
University of Education, Winneba
Ghana

Abstract **- Cloud computing provides reliable and efficient services for sharing data among cloud users at low maintenance cost. Providing privacy, confidentiality, and integrity of data among users in untrusted network environment is a major issue in cloud computing systems, especially where members frequently change their groups. In this paper, we proposed secure file distribution system for untrusted network environment. Our proposed scheme allows users anonymously share their files among members by using group signature and broadcast encryption techniques. The scheme also provides low storage overheads and computational cost independent of the number of revoked users, and support handheld devices with little computational power, low memory and storage capacity. We subjected our scheme to rigorous proofs and security analysis through stimulation and compare the results with other existing protocols thus, MONA and ODBE by considering computational cost for file generation and access.**

Keywords- Cloud Computing, Privacy, File Distribution, Computational Cost, Group Signature

I. INTRODUCTION

Cloud technology is constituted as an alternative to traditional message dissemination [1] due to its intimate resource-sharing and low-maintenance characteristics. In cloud computing, Cloud Service Providers (CSPs) such as Amazon, Google, HP, Microsoft, and Oracle provide varied services to cloud users with the help of their robust and efficient data centers. Organisations who migrate their data onto the cloud systems benefit from easy access to their files, and large data storage among others. Individuals and organisations make cost savings on investment in network infrastructure network. There will be no need to employ network or database administrators to manage organisational files and documents. Additionally, the risk of losing files is minimised since it is under the control of the cloud providers. Authorized users can simply login and have access to their files, and documents anywhere possible with Internet access. One key advantage of cloud computing systems is large storage system that provide support for organisations. However, cloud service providers are not fully trusted with files and documents especially confidential and sensitive files such as business plans, healthcare records, and trade secrets. Cloud computing systems do their best in preserving data privacy by encrypting the files before uploading the encrypted file into the cloud. Users can easily share their files with other group members in the cloud.

However, designing efficient and reliable cloud computing system that guarantees secure user data sharing scheme for group members, has to consider the following issues:

- Identity privacy:

This is one of the major obstacles for the development of cloud computing systems. Users are much concerned with their identity theft by cloud service providers and attackers, there is therefore the fear to subscribe to cloud services. The fear of disclosure of users' identity to other users and unconditional identity privacy may result in abuse of privacy. Traceability is one of the important aspect of the cloud computing, which enable the group manager to reveal the identity of user if necessary. For example, users with bad intensions may think that, they could not be traced when they share false files with group members. The group manager when deem necessary may open the message to find the identity of the user who sent the message.

- Data storage and sharing services:

Every user in the group should be given the opportunity to fully enjoy the services of data sharing and storing in the cloud which is outlined in multi-owner concept [3]. Users should be given credentials that will enable them to be able to upload (store) and modify files in the cloud. In single-owner manner [4], only the group manager has the right to store and modify data in the cloud. Group members can only view or read the content of the files but not to make any changes or modification(s) to the content of the files.

- Dynamic membership:

When new members join the group and current revocation list of companies are dynamic in practice, it becomes difficult securing shared data among users. Additionally, granting access to new members will pose a challenge when it comes to anonymity. This is because they will find out the contents of data files which were there before they joined the group. Moreover, it is not possible for new members to contact anonymous file owners for decryption keys. However, we have developed robust membership revocation system without updating the private keys of the remaining members in the group. This will also have minimised complex key management system.

In [5], [6], and [7] the authors proposed security scheme in untrusted network servers by allowing data owners to store encrypted data files. They also grant access to authorised users by giving them corresponding decryption keys. Thus Storage Service Providers(SSP) and unauthorised users cannot have access to the content of the data files since they have no idea of the decryption keys. However, it becomes problematic

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

when user participation and revocation increases with respect to data owners and revoked users. Lu et al [7] and [8] propose a scheme by setting a group with single attribute. It fails because they did not address user revocation. [3] and [9] also proposed a fine-grained data access control scheme based on key policy attribute-based encryption (KP-ABE) but it supports only single owner. This paper proposes a scheme that allows any user in a group to securely share data files with others in the cloud (multi-owner), support dynamic groups efficiently and provide secure and privacy-preserving access control.

The remaining part of the paper is organized as follows: section 2 reviews related works. Section 3 discusses the system model, section 4 presents the design goal, section 5 is the proposed system implementation, and finally we concluded in section 6.

II. RELATED WORK

In [21], the authors proposed a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. The mechanisms in Plutus reduce the number of cryptographic keys exchanged between users by using filegroups, distinguishing file read and write access, handling user revocation efficiently, and allowing an untrusted server to authorize file writes. A prototype of [11] has been built on OpenAFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

In [12], the paper presents SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, OceanStore and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. The implementation of SiRiUS performs well relatively to the underlying file system despite its use of cryptographic operations.

In 1998, Blaze, Bleumer and Strauss (BBS) proposed an application called atomic proxy re-encryption in which a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext. It is predicted that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following the recent work of [14], [16] and [18], these papers presents new re-encryption schemes that have a stronger notion of security and demonstrates the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of the experimental file system used in this study demonstrate that proxy re-encryption can work effectively in practice.

Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, in order to tackle this unexplored area in cloud computing, a new secure provenance scheme based on the bilinear pairing techniques is proposed. As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access and provenance tracking on disputed documents. With provable security techniques, it is formally demonstrated that the proposed scheme is secure in the standard model.

Also, this paper presents a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) [19] under concrete and noninteractive cryptographic assumptions in the standard model. The solutions provided allow any encryptor to specify access control in terms of any access formula over the attributes in the system. In most efficient systems, ciphertext size, encryption and decryption time scales increase linearly with the complexity of the access formula. The only previous work which attempted to achieve these parameters was limited to a proof in the generic group model.

This paper presents three constructions within its framework. The first system is proven selectively to be secure under an assumption that is called the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) [22] assumption which can be viewed as a generalization of the BDHE assumption. The next two constructions provide performance tradeoffs to achieve provable security under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions respectively.

The concept of group signatures was first introduced in [15] . In general, a group signature scheme allows any member of the group to sign messages while keeping their identity secret from verifiers. Also, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability. In this paper, a variant of the short group signature scheme [13] will be used to achieve anonymous access control as it supports efficient membership revocation.

Broadcast encryption [16] enables a broadcaster to transmit encrypted data to a set of users so that only authorized and privileged subset of users can decrypt the data. In addition to the above characteristics, dynamic broadcast encryption allows a group manager to dynamically include new members while preserving previously computed information, i.e., user decryption keys need not be recomputed, the morphology and size of ciphertexts are unchanged and the group encryption key requires no modification. The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique in [14], which will be used as the basis for file sharing in dynamic groups

III. SYSTEM MODEL

A cloud computing architecture is considered in relation to a company that uses cloud to enable its staff in the same group or department to share files. The system model consists of three

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

different entities namely: the cloud, a group manager (i.e. the company manager) and a large number of group members (i.e. the staff). The figures; Fig 1a and Fig 1b, represent the system model, and the flow diagram respectively of our proposed system architecture.

The cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to the frameworks in [3], and [7], it is assumed that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes [17], [18], but it will try to learn the content of the stored data and the identities of cloud users.

The group manager takes charge of the generation of the system parameters, user registration, user revocation as well as revealing the real identity of the owner of specific data during a dispute. In the given example, the group manager is the administrator of the company.

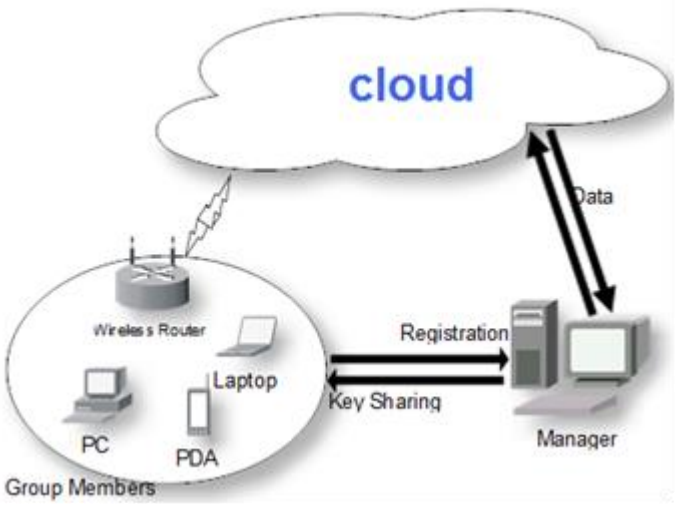


Fig 1a: System model

Therefore, it is assumed that the group manager is fully trusted by the other parties.

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In the example used in the paper, the staff play the role of group members. Note that the group membership is dynamically changed due to staff resignation and new employee participation in the company.

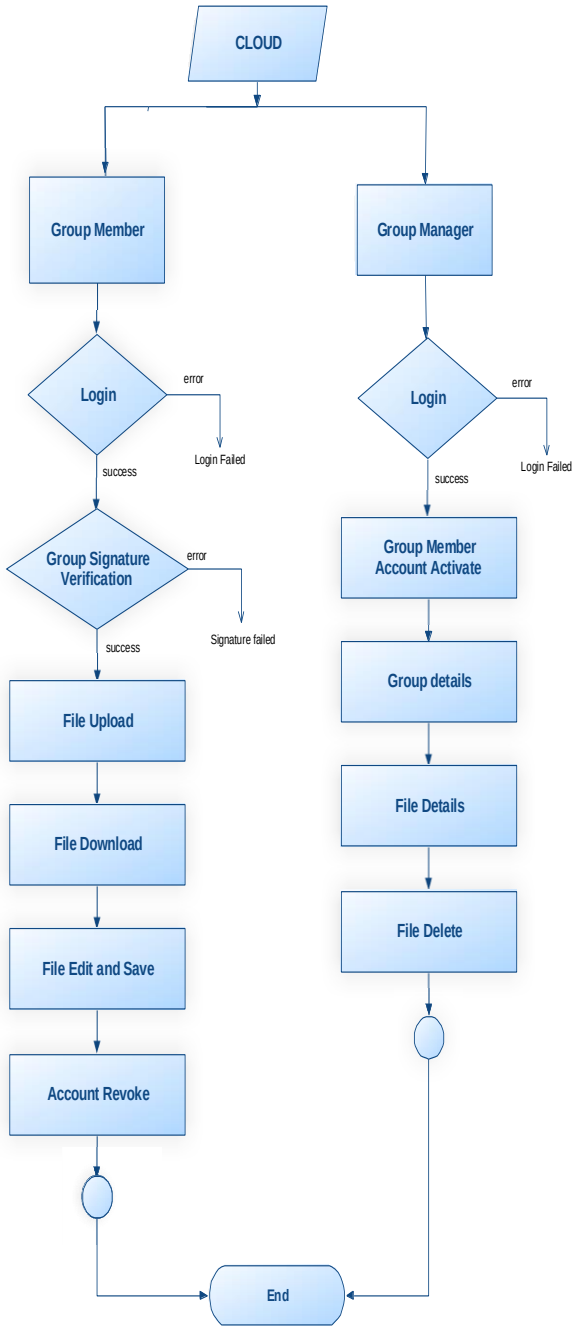


Fig. 1b: Flow diagram

IV. DESIGN GOALS

In this section, the main design goals of the proposed scheme including access control, data confidentiality, anonymity and traceability, and efficiency are described as follows:

a) Access control: The requirement of access control is in two folds. Firstly, the group members are able to use the cloud resource for data operations. Secondly, unauthorized users cannot access the cloud resource at any time and revoked users will be unable to use the cloud once they have been revoked.

b) Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of stored data. An important and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation and revoked users must be unable to decrypt the data moved into the cloud after their revocation.

c) Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing their real identities. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Hence, to tackle the inside attack the group manager should have the ability to reveal the real identities of data owners.

d) Efficiency: Efficiency is defined as any group member can store and share data files with others in the group via the cloud. User revocation can be achieved without involving the remaining users. In other words, the remaining users do not need to update their private keys or reencryption operations. New users can access all the content of data files stored before their participation without contacting the owner of the data.

V. THE PROPOSED SCHEME

To achieve secure data sharing for dynamic groups in the cloud, the group signature and dynamic broadcast encryption techniques are combined. The group signature scheme enables users to anonymously use the cloud resources and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new users. However, each user has to compute revocation parameters to protect their confidentiality from revoked users in the dynamic broadcast encryption scheme. This results in both the computation overhead of the encryption and the increment of the size of the ciphertext with the number of revoked users. Therefore, the heavy overhead and large ciphertext size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this issue, the group manager is tasked with computing the revocation parameters and making the result publically available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the ciphertext size. This is because the computation overhead of users for encryption operations and the ciphertext size are constant and independent of revoked users.

VI. IMPLEMENTATION

In this section, we discuss the implementation of the modules in our proposed system.

A. Cloud Module :

In this module, a local cloud is created to provide abundant storage services. Users can upload their data in the cloud. A module is developed where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain [23]. Similarly, it is assumed that the cloud server is honest but curious that is the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes but will try to know the content of stored data and the identities of cloud users.

B. Group Manager Module :

A group manager takes charge of the followings;

- System parameters generation:

Here the manager computes and publishes the necessary parameters using one-way hash function with secure symmetric encryption algorithm secret key pairs.

- User registration:

The group manager registers the users by computing users key pair and add it to the group user list. The user will receive his private key, which can be used for decryption and group signature generation.

- User revocation:

The group manager will perform user revocation through available public Revocation List(RL). The group manager ensures confidentiality against the revoked users, which they will be based on to encrypt their files.

- Revealing the real identity of a disputed data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The group manager is the Systems Administrator(SA). The group manager has the logs of each and every process in the cloud, and also responsible for user registration as well as user revocation.

C. Group Member Module:

Group members are a set of registered users that will store their private data on the cloud server and Share them with others in the group.

Note that, the group membership is dynamically changed due to possible staff resignation and new employee participation in the company. A group member has ownership of changing the files in the group. Anyone in the group can view files which are uploaded in their group and also modify it.

D. File Security Module :

This module ensures that the following actions are performed in the proposed system:

- File generation
  Group members can share and store data files based on the following operations:
  1. obtaining revocation list from the cloud
  2. verifying he validity of the received revocation list by checking the date.
  3. encrypting the data files using an elliptic curve with 160-bit group order which provides a competitive security level with 1,024-bit RSA [21].
- File storage and deletion
  File stored in the cloud can be deleted by either the group manager or the data owner (i.e. the member who uploaded the file into the server). To delete a file, the group manager computes a signature and sends it with the ID of the data to the cloud. The cloud then effects the data deletion from the storage.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

- File access
  To have access to the content of the file, group members perform the following actions:
  1. The users first get the data file, and revocation list from the cloud server. In this operation, users first adopt their private keys to compute their signatures on the files.
  2. Verifying the validity of the files and decrypting them with their signatures

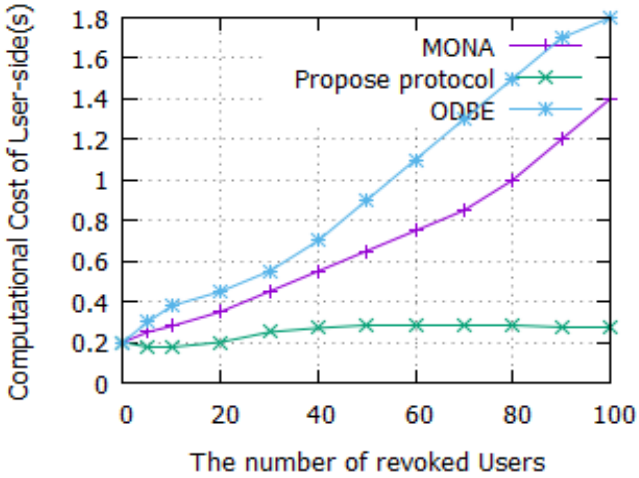
  Group members have unrestricted access to files that they are authorized to view.

E. Group Signature Module :

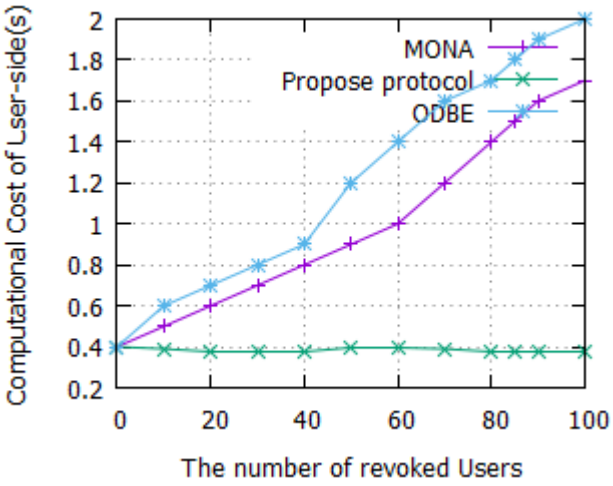
A group signature scheme allows any member of the group to sign messages while keeping their identity secret from verifiers. However, the designated group manager can reveal the identity of the signature's originator when a dispute occurs; thus traceability.

F. . User Revocation Module:

User revocation is performed by the group manager via a publicly available Revocation List (RL). This will help group members encrypt their data files and ensure their protection from revoked users.

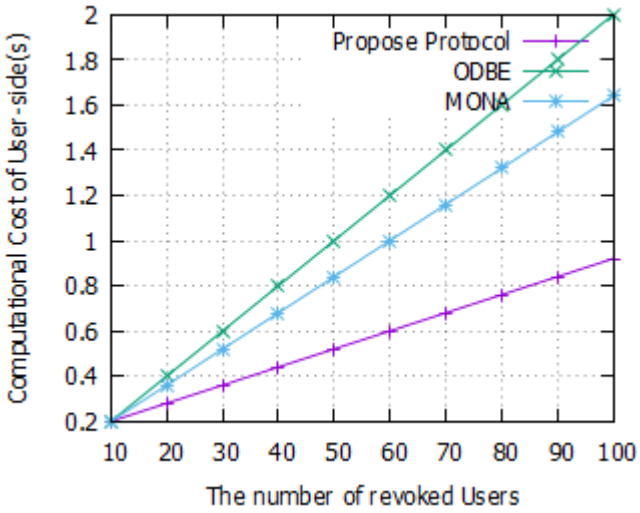


(a)Generating 10MB file

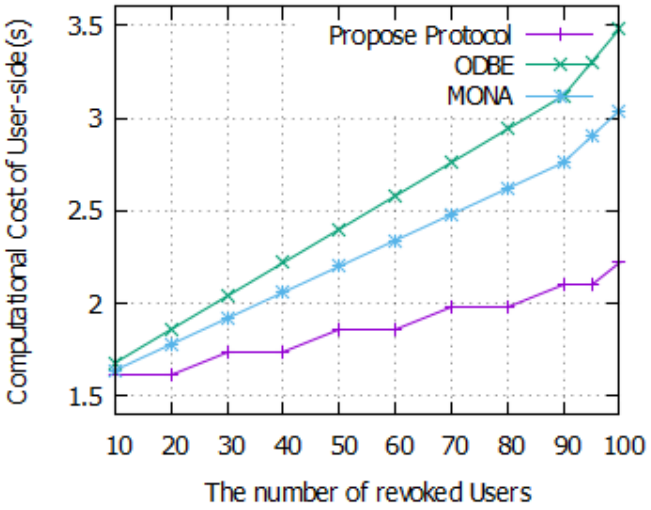


(b) Generating 100MB file

Fig. 2 Comparison of computation cost for file generation between the proposed protocol, MONA and ODBE



(a)Accessing 10MB file



(b)Accessing 100MB file

Fig. 3 Comparison of computation cost for file access between the proposed protocol Mona [10] and ODBE [8].

VII. SIMULATION

The proposed protocol, MONA and ODBE have been simulated using NS2 and its library [12]. Simulation was observed in three areas; on the user's side, manager's side and the cloud's side. An elliptic curve with 160-bit group order was chosen which provides a competitive security level with 1,024-bit RSA.

User computation cost:

In fig. 2, the differences of computational cost of users for data generation operations between this concept and the direct way of MONA [10] and ODBE [8] have been outlined. It can be observed that the computational cost for the proposed protocol is much more insignificant compared to that of MONA and ODBE which have a high computational cost. The reason for the differences in cost is because the parameters (Pr, Zr) can be obtained from the revocation list without sacrificing security in this protocol while several time-consuming operations including point multiplications in G1 and exponentiation in G2 have to be performed by clients to compute the parameters in MONA and ODBE.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

Cloud Computation Cost:

To appraise the performance of the cloud in MONA and ODBE, the computing cost to move different computer computing requests including file propagation, record accession and line excision were tested. Assuming the sizes of requested files are 100MB and 10 MB, the examination results are presented in Fig 3. It can be seen that the process toll of the cloud is deemed acceptable and regularizes when the company of revoked users is banging. This is because the cloud only involves group strain and state verifications to ensure the credibility of the requestor for all dealings. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations, since the size of signed message is constant .

VIII. CONCLUSION

In this paper, a secure information sharing scheme has been programmed in the proposed protocol for energising groups in an untrusted cloud. In this scheme, a human is competent to acquire a connection with others in a group without revelatory sameness seclusion to the cloud. Additionally, the protocol supports efficient individual state and new person connection. Many effective user revocations can be achieved on an overt state list without updating the privy keys of the remaining users and new users can flat decrypt files stored in the cloud before their addition to the system. Moreover, the storage expense and the cryptography figuring outlay are invariant. Large analyses indicate that our proposed grouping satisfies the desirable requirements and guarantees efficiency.

REFERENCES

[1] 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.

[2] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. Int’l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 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. Boneh, X. Boyen, and E. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” Proc. Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[14] C. Delerablee, P. Paillier, and D. Pointcheval, “Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys,” Proc. First Int’l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[15] D. Chaum and E. van Heyst, “Group Signatures,” Proc. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[16] A. Fiat and M. Naor, “Broadcast Encryption,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[17] B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud,” Proc. 10th Int’l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[18] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, pp. 525-533, 2010.

[19] B. Sheng and Q. Li, “Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks,” Proc. IEEE INFOCOM, pp. 46-50, 2008.

[20] D. Boneh, B. Lynn, and H. Shacham, “Short Signature from the Weil Pairing,” Proc. Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001.

[21] D. Pointcheval and J. Stern, “Security Arguments for Digital Signatures and Blind Signatures,” J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.

[22] The GNU Multiple Precision Arithmetic Library (GMP), http://gmplib.org/, 2013.

[23] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL), http://certivox.com/, 2013.

[24] The Pairing-Based Cryptography Library (PBC), http://crypto.stanford.edu/pbc/howto.html, 2013