www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 18740-18744

A Survey on Multi Owner Data Sharing for Dynamic Groups in the Cloud Securely

Sushma Nallamalli[1], SivaNagaRaju Rajulapati[2], Chandrajit Yadav Loya[3]
[1,2,3] Associate Professor Department Of computer Scinece and Engineering,
DMS SVH College Of Engineering, Machilipatnam, Andhra Pradesh
sushmanallamalli@gmail.com
sivanagaraju.cse@gmail.com
yadav.loya@gmail.com

Abstract: ***Cloud computing is the developing computer paradigm, where data owners can remotely store and modify their data on the premise of pay-as-use manner and enjoy on demand high-quality applications. The fundamental service provided by the Cloud is Data Storage which makes it a primary source for customers to utilize cloud for online data store and share. As it requires low maintenance it provides an economical and efficient solution for sharing group resource among cloud users .But, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership in the multi owner group. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users which was a very tedious work. To resolve this problem recently the best efficient method MONA presented for secured multi owner data sharing for dynamic groups in the cloud has been proposed in which a group signature is used so that the revoked member is not able to upload or download files .By including group signature and stateless broadcast encryption techniques, any cloud user can anonymously share data with others .Meanwhile, the storage overhead, length of the signature and the running time of the signing algorithm are independent with the number of group members.***

Keywords: Cloud Computing, dynamic groups, multi owner, privacy-preserving, dynamic broadcast, encryption, data sharing, User Revocation

1. Introduction

1.

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 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 staff in the same group or department to store and share files in the cloud. By utilizing the cloud, the staff 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.

2.

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.

3.

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.

4.

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, 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.

5.

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[1], a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions are:

- A secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the un trusted cloud is proposed.
- It is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.
- To provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource? Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.
- A rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead is provided.

2. Literature Survey

Goh, H. Shacham, N. Modadugu, and D. Boneh [2] the use of SiRiUS is compelling in situations where users have no control over the file server (such as Yahoo! Briefcase or the P2P file storage provided by Farsite). They believe that SiRiUS is the most that can be done to secure an existing network file system without changing the file server or file system protocol. 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.

B. Wang, B. Li, and H. Li, [3] in this paper, we propose Knox, a privacy-preserving auditing scheme for shared data with large groups in the cloud. They utilize group signatures to compute verification information on shared data, so that the TPA is able to audit the correctness of shared data, but cannot reveal the identity o f the signer on each block. With the group manager's private key, the original user can efficiently add new users to the group and disclose the identities of signers on all blocks. The efficiency of Knox is not affected by the number of users in the group.

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 [9] the data centers hardware and software is what we will call a cloud. When a cloud is made available in a pay-as-you-go manner to the general public, they call it a public cloud; the service being sold is utility computing. They use the term private cloud to refer to internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing that we discuss here. Thus, cloud computing is the sum of SaaS and utility computing, but does not include small or medium-sized data centers, even if these rely on virtualization for management. People can be users or providers of SaaS, or users or providers of utility computing. They focus on SaaS providers (cloud users) cloud providers, which have received less attention than SaaS users.

S. Kamara and K. Lauter [4] in this paper consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. They describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve the goal. Survey the benefits such architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

A. Fiat and M. Naor [6] they introduce new theoretical measures for the qualitative and quantitative assessment of encryption schemes designed for broadcast transmissions. The goal is to allow a central broadcast site to broadcast secure transmissions to an arbitrary set of recipients while minimizing key management related transmissions. They present several schemes that allow centers to broadcast a secret to any subset of privileged users out of a universe of size so that coalitions of users not in the privileged set cannot learn the secret.

V. Goyal, O. Pandey, A. Sahai, and B. Waters [6] they develop a new cryptosystem for One-grained sharing of encrypted data that call Key-Policy Attribute-Based Encryption (KP-ABE). In cryptosystem, cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. They demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE). The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a ciphertext if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file reencryption and user secret key update to cloud servers. However, the single owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

By Observing all this analysis we have a greater challenging issue that is how we can securely share data with the others by the multiple-owner manner for the dynamic groups in the un trusted cloud along with preserving identity privacy. Now in this paper, we are surveying new protocol MONA, for secure data sharing in the cloud computing.The MONA offers some unique features when compared with the others. The unique features in a more elaborated way are as follows:

- Any group member can share data files with others and can also store the data files in the cloud.
- In this the number of revoked users is independent with the complexity of encryption and also the size of cipher texts.
- There is no need of updating the private keys of the remaining users whenever the user revocation occurs
- The new users can directly access the files that are stored n the cloud without their participation.

3. System Design

3.1 Existing System

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.

The 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. 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.

In the literature study we have seen many methods for secure data sharing in cloud computing, however most methods failed to achieve the efficient as well as secure method for data sharing for groups. To provide the best solutions for the problems imposed by existing methods, recently the new method was presented called MONA [1]. This approach presents the design of secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Therefore practically in all cases MONA outperforms the existing methods.

Fig 3.1 Existing System Model

Revocation List

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. The revocation list is characterized by a series of time stamps (t1 < t2 <,…, tr). Let IDgroup denote the group identity. The tuple (Ai, xi, ti) represents that user i with the partial private key (Ai, xi) is revoked at time ti. P1, P2, …, Pr and Zr are calculated by th e group manager with the private secret as follows: here x1=y1, x2=y2 and xr=yr.

$$\begin{cases} P_1 = \dfrac{1}{\gamma + x_1} \cdot P \in G_1 \\ P_2 = \dfrac{1}{(\gamma + x_1)(\gamma + x_2)} \cdot P \in G_1 \\ P_r = \dfrac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)} \cdot P \in G_1 \\ Z_r = Z^{\dfrac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)}} \in G_2. \end{cases}$$

Motivated by the verifiable reply mechanism in [7], to guarantee that users obtain the latest version of the revocation list, we let the group manger update the revocation list each day even no user has being revoked in the day. In other words, the others can verify the freshness of the revocation list from the contained current date tRL. In addition, the revocation list is bounded by a signature sig(RL) to declare its validity. The signature is generated by the group manager with the BLS signature algorithm [8]. Finally, the group manager migrates the revocation list into the cloud for public usage.

Disadvantage

However as per reliability and scalability concern this method needs to be workout further as if the group manager stop working due to large number of requests coming from different groups of owners, then entire security system of MONA will fail. In revocation list the time given for each user is fixed so after the time expires user cannot access the data until group manager update the revocation list and give it to the cloud.

3.2 Design Goals

We describe the main design goals of the proposed system including access control, data confidentiality, anonymity and traceability, and efficiency as follows:

Access control: First, authorized group members are able to access the cloud data. Second, unauthorized users cannot access the cloud data at any time, and revoked users will not be capable of accessing the cloud once they are revoked.

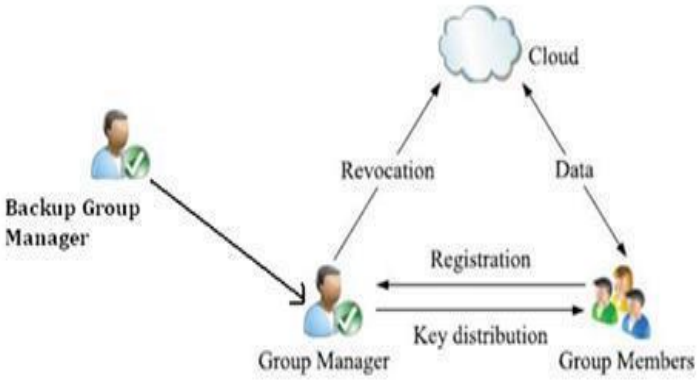
Data confidentiality: Data confidentiality requires that unauthorized users are not capable to access the content of the stored data. An important and challenging issue for data confidentiality for dynamic groups. Specifically, new users should access the data stored in the cloud before their participation, and revoked users are unable to access the data after the revocation. Data owner will store the data on the cloud and share among the group members and data owner will modify the data and delete the data in the cloud.

Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity is an effective protection for users identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a malicious information to get the important information. Thus, to remove the inside attack, the group manager should have the ability to verify the real identities or members of data owners. If the one group member access the data and delete or modify the data by other group members data can be easily traceable in the cloud.

Efficiency: The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud . User revocation is achieved by without involving the remaining users. The remaining users do not need to update their private keys or re encryption operations. New group member can access all the content data files stored on cloud before his participation without contacting with the data owner.

3.3. Proposed System

To achieve the reliable and scalable in MONA, in this paper we are surveying the new framework for MONA. In this method we are further presenting how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability.



To overcome the disadvantage of existing system MONA, in the proposed MONA is if the group manager stop working due to large number of requests coming from different groups of owners, then backup group manager will remain available. Here user gets extra time for accessing data after the time out by sending request to the cloud.

Scheme Description

This section describes system, initialization, user registration, user revocation, file generation, file deletion and file access.

System Initialization

The group manager takes charge of system initialization as follows:
Generating a bilinear map group system S=(q, G1, G2,e(.,.)).
The system parameters including (S, P, H, H0 ,H1 ,H2, U, V , W , Y , Z, f, f1, Enc()), where f is a one-way hash function: {0,1}* —> Z*q ; f1 is hash function: {0,1}* —> G1; and Enck() is a secure symmetric encryption algorithm with secret key k.

User Registration

For the registration of user i with identity IDi, the group manager randomly selects a number xi belong to Z*q and computes Ai, Bi as the following equation:

$$\begin{cases} A_i = \dfrac{1}{\gamma + x_i} \cdot P \in G_1 \\ B_i = \dfrac{x_i}{\gamma + x_i} \cdot G \in G_1. \end{cases}$$

Then, the group manager adds (Ai, xi, IDi) into the group user list, which will be used in the traceability phase. After the registration, user i obtains a private key (xi, Ai, Bi), which will be used for group signature generation and file decryption.

Revocation List

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. The list is characterized by time stamp t1,t2,…tr. In the proposed system once the user time stamp is over he need not wait for the group manager to update the time stamp or revocation list, the user can immediately send request for extra time for accessing the data to the cloud. Then the cloud will send that request to the group manager who can give permission

File Generation

To store and share a data file in the cloud, a group member performs the following operations:

Getting the revocation list from the cloud. In this step, the member sends the group identity IDgroup as a request to the cloud. Then, the cloud responds the revocation list RL to the member. Verifying the validity of the received revocation list. First, checking whether the marked date is fresh or not. Second, verifying the contained signature sig(RL) by the equation e(W, f1 (RL)) = e(P, sig(RL)). If the revocation list is invalid, the data owner stops this scheme. Encrypting the data file M. Selecting a random number T and computing fT. The hash value will be used for data file deletion operation. In addition, the data owner adds (IDdata, T) into his local storage. Constructing the uploaded data file as shown in Table 2, where tdata denotes the current time on the member, and a group signature on (IDdata, C1, C2, C, f(T); tdata) computed by the data owner through private key (A, x).

Group ID	Data ID	ciphertext	hash	Time	Signature
ID_{group}	ID_{data}	C_1, C_2, C	$f(\tau)$	t_{data}	σ

Table 1.Message Format

Uploading the data shown in Table.1 into the cloud server and adding the IDdata into the local shared data list maintained by the manager. On receiving the data, the cloud will first check the validity. If the algorithm returns true, the group signature is valid; otherwise, the cloud abandons the data. In addition, if several users have been revoked by the group manager, the cloud also performs revocation verification. Finally, the data file will be stored in the cloud after successful group signature and revocation verifications.

File Deletion

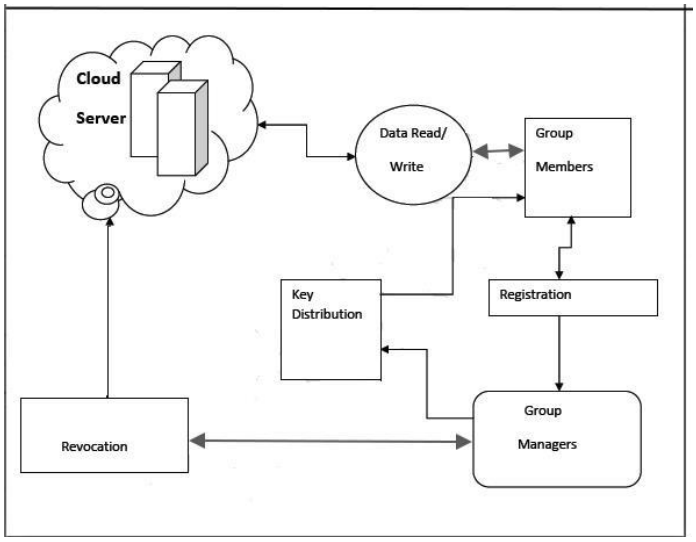
File stored in the cloud can be deleted by either the group manager or the data owner (i.e., the member who uploaded the file into the server). To delete a file IDdata, the group manager computes a signature and sends the signature along with IDdata to the cloud.

A secure multi-owner data sharing scheme is provided. It implies that any user in the group can securely share data with others by the untrusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. A secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

Advantages of Proposed System

- Any user in the group can store and share data files with others by the cloud.
- The encryption complexity and size of cipher texts are independent of the number of revoked users in the system.
- User revocation can be achieved without updating the private keys of the remaining users.
- A new user can directly decrypt the files stored in the cloud before his participation.

4. Mona Architecture:



The architecture model consists of three main different entities: The Cloud Server, Group Manager (admin) and a large number of Group Members.

- Cloud Server: Cloud is operated by cloud service providers and provides priced abundant storage services.
- Group Manager: Group Manager takes the charge of system parameters like user registration, user revocation, secret key generation.
- Group Members: Group members are the set of registered users that will store their private data into the cloud server and can download it and share the data with others in the group

Cloud Server: Cloud is the large repository of resources. Cloud is responsible for storing all user's data and granting access to the file within a group to other group members based on publically available revocation list which is maintained by group manager. We assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data, but will try to learn the content of the stored data.

Group Manager: The group manager is acted by the administrator of the company. Therefore we assume that the group manager is fully trusted by the other parties Group manager perform various operations such as system parameters generation, user registration, group creation, assign group signature, generation of private key using bilinear mapping and assign to the requested user, maintain revocation list and migrate this list into cloud for public use, and traceability.

Group Members: Group members are a collection of registered users that will store their private data into the cloud server and share them with others in the group.

Algorithms Used:-

Signature Generation - The group signature and file key generation can be done by using the Triple DES encryption process.

Signature Verification – The verification of group signature key and file key's with the Triple DES decryption process.

Revocation Verification - To check the user revocation which is used for the verification of user's list.

5. Simulation

To Study the performance we simulate MONA by using C programming language which provides a competitive security level with 1,024-bit RSA. The simulation consists of three components. Client side, Manager Side as well as cloud side.

Client Computation Cost: The computation cost in MONA increases with the number of revoked users, as clients require to perform signature generation and signature verification algorithms to compute the parameters and check whether the data owner is a revoked user or not.

Cloud Computation Cost: To evaluate the performance of the cloud in Mona, we test its computation cost to respond various client operation requests including file generation, file access, and file deletion. Assuming the sizes of requested files are 100 and 10 MB. It can be seen that the computation cost of the cloud is deemed acceptable, even when the number of revoked users is large. This is because the cloud only involves group signature and revocation verifications to ensure the validity of the requestor for all operations. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations.

6. Conclusion

In conclusion, cloud computing is very attractive environment for business world in term of providing required services in a very cost effective way. However, assuring and enhancing security and privacy practices will attract more enterprises to world of cloud computing. Thus to achieve the reliability and scalability in MONA, in this paper we are surveying the new framework for MONA. Mona, for dynamic groups in a un trusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant and length of the signature and the running time of the signing algorithm are independent of the number of group members. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

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, JUNE 2013

[2] 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.

[3] 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

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

[5] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[6] 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.

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

[8] 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.

[9] 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.