RESEARCH ARTICLE OPEN ACCESS

Three Level Security System for Dynamic Group in Cloud

V.Sathana[1], J.Shanthini[2],
M.E[1], Assisatant Professor[2], Dept of Computer Science and Engineering,
Info Institute of Engineering,Coimbatore-India
Anna University
anusathana@gmail.com[1],
shanthinisampath@gmail.com[2],

ABSTRACT

Sharing group resource among cloud users is a major problem, so cloud computing provides an economical and efficient solution. Due to frequent change of membership, sharing data in a multi-owner manner to an untrusted cloud is still a challenging issue. In this paper, We propose a secure multi-owner data sharing scheme, for dynamic group in the cloud. By providing group signature and dynamic broadcast encryption techniques, any cloud user can securely share data with others. Meanwhile, the storage overhead and encryption computation cost of the scheme are independent with the number of revoked users. In addition, we analyze the security of this scheme with rigorous proofs. One-Time Password is one of the easiest and most popular forms of authentication that can be used for securing access to accounts. One-Time Passwords are often referred to as a secure and stronger forms of authentication, and allowing them to install across multiple machines. We provide a multiple levels of security to share data among multi-owner manner. First the user selects the pre-selected image to login. Then selects an image from the grid of images. Then OTP is generated automatically and sent to corresponding e-mail account.

Keywords- Cloud computing, Broadcast encryption

I. INTRODUCTION

Cloud computing is Internet ("cloud") based development and use of computer technology ("computing"). It is a style of computing in which dynamically scalable and often virtualization resources are provided as a service over the internet. 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. 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.

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 [3], 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 an untrusted servers have been proposed [4], [5], [6]. 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

Our contributions. To solve the challenges presented above, we propose a secure multi-owner data sharing scheme for dynamic group in the cloud. The main contribution of this paper include:

To provide security for dynamic group we integrates Image based authentication and one time password to achieve high level of security.

The main Objective of Image based authentication is providing a three levels of security. It is a unique and an esoteric study of using images as password and implementation of an extremely secured system, employing 3 levels of security.

Level 1: Level 1 security provides a simple text based Password.

Level 2: In this security level the user has to select an image from the grid of images. It can eliminate the shoulder attack and the tempest attack.

Level 3: After the successful entry of the above two levels, the Level 3 Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his e-mail.

II. LITERATURE SURVEY

A. Cryptographic Cloud Storage

S. Kamara et al.[9] proposed a security for customers to store and share their sensitive data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security. HoIver, the revocation operation is a sure performance killer in the cryptographic access control system. To optimize the revocation procedure, they present a new efficient revocation scheme which is efficient, secure, and unassisted. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. Thus, the revocation process is accelerated by affecting only one slice instead of the whole data. They have applied the efficient revocation scheme to the cipher text-policy attribute-based encryption based cryptographic cloud storage. The security analysis shows that the scheme is computationally secure.

B. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing

S. Yu et al.[17] focused on many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. The problem of simultaneously achieving fine-grained ness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. They achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. They proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability.

C. Ciphertext-Policy Attribute-Based Encryption: an Expressive, Efficient, and Provably Secure Realization

B. Waters et al.[16] proposed the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, 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 this paper, they propose a secure multi- owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, they analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

D. Sirius: Securing Remote Untrusted Storage

E. Goh et al.[7] presented a SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, 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. Our implementation of SiRiUS performs Ill relative to the underlying file system despite using cryptographic operations. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Using cryptographic operations implementation of Sirius also possible. It only uses the own read write cryptographic access control. File level sharing are only done by using cryptographic access.

E. Broadcast Encryption

A.Fiat et al.[6] proposed a system on multicast communication framework, various types of security threat occurs. As a result construction of secure group communication that protects users from intrusion and eavesdropping are very important. In this paper, they propose an efficient key distribution method for a secure group communication over multicast communication framework. In this method, they use IP multicast mechanism to shortest rekeying time to minimize adverse effect on communication. In addition, they introduce proxy mechanism for replies from group members to the group manager to reduce traffic generated by rekeying. They define a new type of batching technique for rekeying in which new key is generated for both leaving and joining member. The rekeying assumption waits for 30 sec so that number time's key generation will be reduced.

F. Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks

B. Sheng et al.[10] focused on The architecture of two-tiered sensor networks, where storage nodes serve as an intermediate tier betIen sensors and a sink for storing data and processing queries, has been widely adopted because of the benefits of poIr and storage saving for sensors as Ill as the efficiency of query processing. HoIver, the importance of storage nodes also makes them attractive to attackers. In this paper, They propose SafeQ, a protocol that prevents attackers from gaining information from both sensor collected data and sink issued queries. SafeQ also allows a sink to detect compromised storage nodes when they misbehave. To preserve privacy, SafeQ uses a novel technique to encode both data and queries such that a storage node can correctly process encoded queries over encoded data without knowing their values. To preserve integrity, they propose a new data structure called neighborhood chains that allows a sink to verify whether the result of a query contains exactly the data items that satisfy the query. In addition, they propose a solution to adapt SafeQ for event-driven sensor networks. Use a new technique safe q for encode both data and queries. Using new data structure technique called neighbourhood.

G. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing

C. Wang et al.[11] proposed a cloud storage system, consisting of a collection of storage servers, provides long-term storage services over the Internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. They propose a threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back. The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as Ill as forwarding operations over encoded and encrypted messages. Our method fully integrates encrypting, encoding, and forwarding. They analyze and suggest suitable parameters for the number of copies of a message dispatched to storage servers and the number of storage servers queried by a key server.

H. Plutus: Scalable Secure File Sharing on Untrusted Storage

M. Kallahalla et al.[8] presented the Plutus 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. They explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged betIen users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. They have built a prototype of Plutus on Open AFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic

I. Towards Secure and Dependable Storage Service in Cloud Computing

C.Wang et al.[13] presented an emerging services in cloud paradigm, cloud storage enables users to remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. In this paper, the focus on cloud data storage security, which has always been an important aspect of quality of service. By utilizing the homomorphic token with distributed verification of erasure-coded data, unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

J. Ensuring Data Storage Security in Cloud Computing

C.Wang et al.[15] proposed a next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been till understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, the consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only

K. A View of Cloud Computing

M. Armbrust et al.[2] presented a security one of the most often-cited objections to cloud computing; analysts and skeptical companies ask “who would trust their essential data ‘out there’ somewhere?” There are also requirements for auditability, in the sense of Sarbanes-Oxley azon spying on the contents of virtual machine memory; it’s easy to imagine a hard disk being disposed of without being wiped, or a permissions bug making data visible improperly. There’s an obvious defense, namely user-level encryption of storage. This is already common for high-value data outside the cloud, and both tools and expertise are readily available. This approach was successfully used by TC3, a healthcare company with access to sensitive patient records and healthcare claims, when moving their HIPAA-compliant application to AWS [1]. Similarly, auditability could be added as an additional layer beyond the reach of the virtualized guest OS, providing facilities arguably more secure than those built into the applications themselves and centralizing the software responsibilities related to confidentiality and auditability into a single logical layer. Such a new feature reinforces the Cloud Computing perspective of changing our focus from specific hardware to the virtualized capabilities being provided

L. Hierarchical Identity Based Encryption with Constant Size Ciphertext

D. Boneh et al.[4] focused on a Hierarchical Identity Based Encryption (HIBE) system where the ciphertext consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth. Encryption is as efficient as in other HIBE systems. They prove that the scheme is selective-ID secure in the standard model and fully secure in the random oracle model. The system has a number of applications: it gives very efficient forward secure public key and identity based cryptosystems (with short ciphertexts), it converts the NNL broadcast encryption system into an efficient public key broadcast system, and it provides an efficient mechanism for encrypting to the future. The system also supports limited delegation where users can be given restricted private keys that only allow delegation to bounded depth. The HIBE system can be modified to support sublinear size private keys at the cost of some ciphertext expansion.

M. Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud

B. Wang et al.[12] focused on cloud computing and storage services, data is not only stored in the cloud, but routinely shared among a large number of users in a group. It remains elusive, hothever, to design an efficient mechanism to audit the integrity of such shared data, while still preserving identity privacy. In this paper, they propose Knox, a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group. In particular, the utilize group signatures to construct homomorphic authenticators, so that a third party auditor (TPA) is able to verify the integrity of shared data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA. With Knox, the amount of information used for verification, as thell as the time it takes to audit with it, are not affected by the number of users in the group. In addition, Knox exploits homomorphic MACs to reduce the space used to store such verification information. Our experimental results show that Knox is able to efficiently audit the correctness of data, shared among a large number of users Scalable and rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. Hothever, Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature

N. Hail: A High-Availability and Integrity Layer for Cloud Storage:

K.D. Bowers et al.[5] focused on HAIL (High-Availability and Integrity Layer), a distributed cryptographic system that permits a set of servers to prove to a client that a stored file is intact and retrievable. HAIL strengthens, formally unifies, and streamlines distinct approaches from the cryptographic and distributed-systems communities. Proofs in HAIL are efficiently computable by servers and highly compact typically tens or hundreds of bytes, irrespective of file size. HAIL cryptographically verifies and reactively reallocates file shares. It is robust against an active, mobile adversary, i.e., one that may progressively corrupt the full set of servers. They propose a strong, formal adversarial model for HAIL, and rigorous analysis and parameter choices. The show how HAIL improves on the security and efficiency of existing tools, like Proofs of Retrievability (PORs) deployed on individual servers. The also report on a prototype implementation.

O. Trustable Consistency and Reliability of Data in Cloud Computing Using Building Customer Trust in Cloud Computing with Transparent Security

Potential users of cloud services often fear that cloud providers' governance is not yet mature enough to consistently and reliably protect their data. As the trend toward cloud-based services continues to grow, it has become clear that one of the key barriers to rapid adoption of enterprise cloud services is customer concern over data security (confidentiality, integrity, and availability). This algorithm introduces the concept of transparent security and makes the case that the intelligent disclosure of security design, practices, and procedures can help improve customer confidence while protecting critical security features and data, thereby improving overall governance. Readers will learn how transparent security can help prospective cloud computing customers make informed decisions based on clear facts. For the purpose of discussion and debate, a model leveraging the ISO 27000 series standards is presented as a commonly understood framework for disclosure.

P. Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance

Q.Wang et al.[14] presented a distributed data storage has gained increasing popularity for efficient and robust data management in wireless sensor networks (WSNs). The distributed architecture makes it challenging to build a highly secure and dependable yet light height data storage system. On the one hand, sensor data are subject to not only Byzantine failures, but also dynamic pollution attacks, as along the time the adversary may modify/pollute the stored data by compromising individual sensors. On the other hand, the resource-constrained nature of WSNs precludes the applicability of heavy height security designs. To address the challenge, in this article they propose a novel dependable and secure data storage scheme with dynamic integrity assurance. Based on the principle of secret sharing and erasure coding, the first propose a hybrid share generation and distribution scheme to achieve reliable and fault-tolerant initial data storage by providing redundancy for original data components. To further dynamically ensure the integrity of the distributed data shares, they then propose an efficient data integrity verification scheme exploiting the techniques of algebraic signature and spot-checking. The proposed scheme enables individual sensors to verify in one protocol execution the correctness of all the pertaining data shares simultaneously in the absence of the original data

Q. Off-Line Keyword Guessing Attacks on Recent Keyword Search Schemes over Encrypted Data

keyword search scheme over encrypted documents allows for remote keyword search of documents by a user in possession of a trapdoor (secret key). A data supplier first uploads encrypted documents on a storage system, and then a user of the storage system searches documents containing keywords while insider (such as administrators of the storage system) and outsider attackers do not learn anything else about the documents. In this paper, they firstly raise a serious vulnerability of recent keyword search schemes, which lies in the fact that keywords are chosen from much smaller space than passwords and users usually use thell-known keywords for search of document. Hence this fact sufficiently gives rise to an off-line keyword guessing attack. Unfortunately, they observe that the recent public key-based keyword search schemes are susceptible to an off-line keyword guessing attack. The demonstrated that anyone (insider/outsider) can retrieve information of certain keyword from any captured query messages.

R. Deduplication in Cloud Storage Using Side Channels in Cloud Services, the Case of Deduplication in Cloud Storage

G.Ateniese et al.[3] focused on deduplication in Cloud storage. Cloud storage services commonly use deduplication, which eliminates redundant data by storing only a single copy of each file or block. Deduplication reduces the space and bandwidth requirements of data storage services, and is most effective when applied across multiple users, a common practice by cloud storage offerings. The privacy implications of cross-user deduplication are studied. It demonstrates how deduplication can be used as a side channel which reveals information about the contents of files of other users. In a different scenario, deduplication can be used as a covert channel by which malicious software can communicate with its control center, regardless of any firewall settings at the Attacked machine.

III. PROPOSED SYSTEM

Secure environments protect their resources against unauthorized access by enforcing access control mechanisms. So when increasing security is an issue text based passwords are not enough to counter such problems. The need for something more secure along with being user friendly is required. This is where Image Based Authentication (IBA) comes into play. This helps to eliminate tempest attack, shoulder attack. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP) after image authentication. This OTP then can be used by user to access their personal accounts. The image based authentication method relies on the user's ability to recognize pre-chosen categories from a grid of pictures. In this paper I integrates Image based authentication and one time password to achieve high level of security in authenticating the user over the internet.

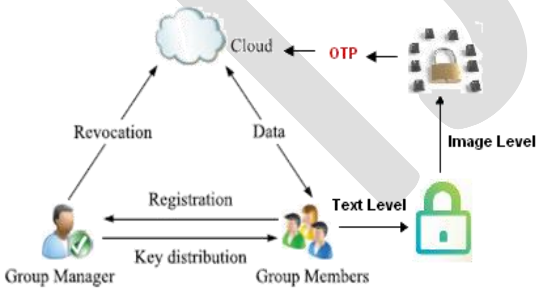

Fig. 1. System Architecture.

The main Objective of 3 Level Security system is a unique and an esoteric study of using images as password and implementation of an extremely secured system, employing 3 levels of security.

Level 1: Security at level 1 has been imposed by simple text -based password.

Level 2: Security at this level has been imposed by using image based authentication (IBA) which helps to eliminate shoulder attack, tempest attack. User has to select three images from the respective grid.

Level 3: After the successful clearance of the above two levels, the Level 3 Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his email id.

IV. DISCUSSION

The intention of the scheme is to propose a secure and efficient three-party key agreement scheme with privacy protection of service requesters by using OTP final confirmation verifier. In this paper, I propose a three-party key agreement scheme to construct a secure transaction mechanism with privacy protection. In our scheme, the major merits include: (1) prevention of some known attacks; (2) satisfaction of the perfect forward secrecy; (3) security against the OTP reveal; (4) privacy protection; (5) no sensitive verifier table and (6) low communication and computation cost.

V. CONCLUSION

In this paper, I design a secure data sharing scheme, for dynamic groups in an untrusted cloud. a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, It 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. A new type authentication system, which is highly secure, has been proposed in this paper.

This system is also more users friendly. This system will definitely help thwarting Shoulder attack, Tempest attack and Brute-force attack at the client side. Though 3-Level Security system is a time consuming approach, it will provide strong security where the need to store and maintain crucial and confidential data secure. Such systems provide a secure channel of communication between the communicating entities. The ease of using & remembering images as a password also support the scope of these systems.

VI. REFERENCES

[1] X.Liu,B.Wang,Y.Zhang, and J.Yan,"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,"IEEE Computer Society,vol. 24,no. 6,June. 2013.

[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] G.Ateniese, R. Burns, R.urtmola, J.Herring, L. Kissner, Z. Peterson, and D.Song, "Deduplication in cloud storage using side channels in cloud services," Oct 2008.

[4] 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.

[5] K. D. Bowers, A. Juels, and A. Oprea, ”Hail: A high-availability and integrity layer for cloud storage,” in Proc. Of CCS’09, 2009, pp. 187-198.

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

[7] 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.

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

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

[11] 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.

[12] 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.

[13] C. Wang, Q. Wang, K. Ren, N. cao, and W. Lou,”Towards Secure and Dependable Storage Services in Cloud Computing,” IEEE Services Computing, pp. 1939-1374, 2011.

[14] Q. Wang, K. Ren, W. Lou, and Y.Zhang, ”Depandable and secure sensor data storage with dynamic integrity assurance,” in proc. of IEEE INFOCOM’09, Rio de Janeiro, Brazil, April 2009.

[15] C. Wang, Q. Wang, Kui Ren, and W. Lou, ”Ensuring Data Storage Security in Cloud Computing,” in proc. of IWQos’09,July 2009,pp.1-9.

[16] 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.

[17] 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.