Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 5 (2015), pp. 3975-3985

http://www.ripublication.com

Towards Secure And Trust-Worthy Sharing Of Data In Private Cloud Using Oaep Algorithm

S. Selvakumar and Dr. A. Rengarajan

Research Scholar, Department of Computer Science and Engineering,
Karpagam University Coimbatore, Tamil Nadu, India.
Email: selva_harur@yahoo.co.in Tel: +91-9486131020
Professor, Department of Computer Science and Engineering,
Vel Tech Multitech Dr.RR Dr.SR Engineering College,
Email: rengu_rajan@yahoo.com Tel: 8056133788 / 9841310814

ABSTRACT

Cloud computing is a type of computing where data owners can remotely store their data in the cloud to enjoy various applications and services from a shared pool of computing resources. In general, private cloud environment is set for a specific organization. It can either be managed internally or can be managed externally (i.e.), through a third-party auditor. Outsourcing of data services, computational services, access control and trust-worthiness are the major features of a private cloud. Even though encryption of data is performed before outsourcing the data, it doesn't guarantees secure and trusted sharing of data, at times it results in loss of data, or loss of integrity. Data outsourcing eliminates the physical control of the data (i.e.), the owners of the data no longer physically possess the storage of their data thereby affecting security. Computational outsourcing eliminates the correctness of the data. Access of data in private cloud is generally restricted to data owner. Another important factor is trust-worthiness, where private cloud in general is highly trust-worthy. The data to be stored in cloud is encrypted before the storing process. In order to provide solutions for security issues concerning data and computational outsourcing, we implement a new concept, of generating padding bits in order to provide more security to data.

Index Terms: Cloud computing, Data outsourcing, Computation outsourcing, Access control, Trust-worthiness pad bits.

1. INTRODUCTION:

Cloud computing is a technology where one can store their data or any kind of resources in a remote server. The data stored in the remote server can be either only accessed by the owner of the resource or it can be allowed for public access. There are two main kinds of cloud, namely, public and private cloud.

Generally private cloud is more secure when compared to public cloud. This is because, in public cloud, the data can be accessed by public user, based on owner's permission where as in private cloud, only the owner will be accessing the data or the resource.

Private cloud environment is specifically used by single organization. Private clouds are deployed inside a company's firewall and traditionally run by on-site servers. This infrastructure can be managed either internally or externally by a third-party.

Private clouds offer some of the benefits of a public cloud like elastic on-demand capacity, self service provisioning, and service based access.

Several services are offered by the private cloud for their customers. Services are as follows: virtualization, multi-tenancy, consistent deployment, security and access control. The user's can store their data in a remote server and at the same time they can access various applications and services. The user need not worry about the storage management as the cloud takes care of the storage.

Computational outsourcing deals with the process of outsourcing the computations that has to be performed on the data stored on the private cloud. During computational outsourcing there may occur security issues like, loss of correctness of data, loss of integrity and availability of data.

The data in the private cloud is managed by the **Third Party Auditor (TPA)**. The Third Party Auditor audits and maintains the data stored in the private cloud. The auditing is done in order to check the integrity of the data that is stored by the data owner. The Third Party Auditor performs auditing in an efficient way such that there is no leakage of data and no local copy is created. It is important to check whether the Third Party Auditor is trust-worthy, reliable and also their access should be restricted in case of private cloud.

2. RELATED WORKS:

In [1] author propose publicly auditable cloud data storage in order to deploy cloud data storage and other services. Also to regain security based on outsourced data, efficient methods are implemented in order to check the correctness of data and integrity of data.

In traditional methods, to protect the data and to maintain the integrity of the data, traditional cryptographic methods such as Message Authentication Codes(MACs) was used. The data owners will be maintaining a small amount of MAC for the data files that are outsourced. When outsourced data is to be retrieved, one can verify the integrity of data by calculating the MAC of received data file.

In [2] author proposes the use of ring signature. Ring signature is a set of keys that are generated for a group of members. The set of keys are shared among the users where, one of the key is used to encrypt the data. The key is not revealed to any persons in

the group. But even this has a disadvantage, on request, the group manager may reveal the key, thereby security is lost.

In [3] author proposes the use of hybrid-attribute and re-encryption. Attribute based encryption allows only authorized user to access the content stored in the cloud and this is based on attribute-based policy. The use of re-encryption technique makes revocation to be more efficient than normal encryption technique.

In [4] author proposes a new architecture were security is considered as a key factor such that the cloud tenants have flexible security and security related functionalities. The cloud infrastructure is made secure thereby the data stored in the cloud is also made secure.

In [5] here the cloud service providers provide users scalable and efficient data storage and also the cost is lowered using traditional approaches. In [6], [7] the author tells about the integrity of the data stored in the cloud. However the data is affected, and integrity is lost, this is because the data stored in cloud is easily accessible by all, hence it is easily corrupted due to hardware/software failures.

In [8] the cloud service provider may not inform about the data errors to the users and this makes the integrity problem even worse. [9] In order to maintain integrity, the data should be verified and then it should be utilized. Integrity check on data must be performed before its being utilized, then only the necessary computations can be performed effectively, with marginal cost.

3. PROBLEM STATEMENT:

Private cloud is known for its high privacy and restricted access of the data stored in cloud. Strong requirements for control and security usually drive a preference for Private Cloud, where they own the cloud resources and control the location of those resources.

Private cloud provide more control on stored data when compared to public cloud. Even though the data stored in private cloud is more secure when compared to public cloud, there arises some security challenges due to outsourcing. Main challenges faced in private cloud are computational service outsourcing, access control and trust-worthiness.

a) Data Outsourcing:

Data outsourcing relieves the burden of local data storage and maintenance and also it eliminates their physical control of storage dependability and security. Data outsourcing to a cloud is applicable for any kind of applications that requires data to be kept in separate storage. Clients that engage cloud provider, pay only for amount of storage they used, related computation and for network communication. From owner's point of view, outsourcing of data service has advantages like, minimization of cost, economically attractive, provides scalability. But outsourcing data leads to several security issues, this is because, the owner of the data doesn't have direct control over data. Therefore security issues like data integrity loss, data loss, incorrectness, etc.

b) Computational Outsourcing:

Computational outsourcing refers to process of outsourcing the computations and workloads to a third party server. The third party server may be a trustworthy or at times they might be untrustworthy. In case of outsourcing the computations to a third party audit, the computational cost is reduced and also efficiency is increased.

c) Access Control:

The access control, which is one of the major aspect to be considered during the setting up of cloud environment. Access control helps to prevent unauthorized access to data and protects data stored in the cloud. There are several access control policies like, Mandatory Access Control (MAC), Role Based Access Control (RBAC), based on different environments.

d) Trust-worthy:

Trust-worthiness is one of the major factor to be considered while storing data in cloud. Nowadays computing as a service is increased and is popular, users employ cloud resources to accomplish their task. The cloud computing environment that is used by the user must be trust-worthy and reliable. Private cloud is more trust-worthy when compared to public and other cloud environments. Based on the privacy and security, the cloud provider can be considered to be trustworthy.

Even though there are many advantages in private cloud, it has its own disadvantages. When privacy and security of data is to concerned, computation outsourcing causes loss of correctness, data can be corrupted or lost, and loss of integrity. If there is no proper access control, any one can access the data stored in the private cloud. Proper access control must be defined in order to prevent the access of data by unauthorized users. If there is no proper access control mechanism, this may lead to loss of trust-worthiness. Even though the data stored in private cloud are encrypted, privacy issues occur when computational services are outsourced and if there is no proper access control mechanism..

4. SYSTEM MODEL:

In order to provide more security to the data stored in the private cloud, along with encryption we are implementing an efficient and secure pad bit generation algorithm. The padding bit is an additional bit that is generated randomly for each used, is appended along with the encrypted data in order to increase the security. This kind of validation is done in order to increase the reliability of the data stored in the cloud storage.

4.1 Padding Technique:

The system model that we are implementing minimizes the security and privacy issues that are possible to occur due to data service outsourcing and computational outsourcing. Here we are using Padding Bits along with encryption process.

Pad bits are *random* bits that are generated by pad bit generator. There are several kinds of padding, say bit padding, byte padding, zero padding. In **bit padding**

technique, pad bits are of the form *0's* and *1's*, **byte padding** made up of *hexadecimal* values. **Zero padding** technique consists of **0's** alone, which is not secured and hence not approved by any of the encryption standards.

In normal padding technique, random material is just appended to the data/message. This appending technique does not implement any specific method or algorithm for generating random bits, this does not provide any kind of security. In modern padding techniques several algorithms are implemented to generate pad bits. The pad bits are generated in random method, in such a way that, it is hard for the attacker to manipulate either the pad bits or the plaintext. A special technique called as **Random Oracle Model** is implemented. This is the latest technique for generating random bits, where breaking the padding scheme and manipulating the plaintext is really hard. This is because, Random Oracle Model uses mathematical function, here a number of query is generated and each query is randomly mapped to a response. The **randomness property** here used is that, one cannot identify which response is mapped to which query, this makes it more secure and hard to break the padding scheme.

Whenever a new user enters the private cloud, a sequence of pad bits along with reference index is generated. The pad bit sequence is known only to the owner of the data.

Padding bits are generated using pad bit generation algorithm. Here we use OAEP algorithm along with RSA, to generate pad bits. The pad bits are generated randomly and its highly difficult to predict the pad bits, due to its randomness. It uses a policy of **All-or-none transform**, that is, either the complete plaintext is retrieved by deriving the correct cryptographic hash bits or the entire text is lost, even if one of the cryptographic hash bit changes. This policy makes this algorithm highly efficient and secure to implement.

Another interesting thing about this algorithm is, it uses a special function called as, **Trapdoor-oneway permutation function**. The main advantage of using this function is, its easy to perform computation in forward direction, whereas reverse or opposite computation is very tough, thereby making it hard for the attacker to manipulate the plaintext. This makes it more secure and also its hard to manipulate or break the message.

The addition of pad bits to the data stored in the private network, is done, in order to ensure high security and privacy. As the pad bits are known only to the user, and also the pad bit sequence is generated randomly, the possibilities for attacking or destroying or hacking the data is very less when compared to traditional encryption technique. Security is high, data integrity and availability is made possible and original data is returned to the data owner.

4.2 Implementation:

The system model that we are implementing minimizes the security and privacy issues that are possible to occur due to computational outsourcing and access control policies. Here we are using Padding Bits along with encryption process.

Padding bits are random bits that are generated by pad bit generator. Whenever a new user enters the private cloud, a sequence of pad bits along with reference index is

generated. The pad bit sequence is known only to the owner of the data.
The data to be stored in private cloud are encrypted with help of secure key generator, before they are being stored. Along with encryption these pad bits are added to the data and are stored in the private cloud.
The data owner in order to retrieve data from the private cloud, has to submit the pad bit sequence. If the pad bit of the data owner matches with the reference index, then the data can be retrieved. When data is to be retrieved from the cloud, the pad bits are removed and then the data is sent to the data owner.
The addition/removal of pad bits are taken care by Account Centre. The account centre updates credit value for each transaction, along with pad bits. If the transaction is successful, positive credit value is updated, and if transaction is a failure, negative credit value is updated.
The Secure Key Centre has two parts, namely, secure key generator and key index. The secure key generator generates the encryption key which is used for encrypting the data to be stored in the private cloud. Each secure key/encryption key has a corresponding key index. When data is to be stored in cloud, it is encrypted with the help of secure key generator. The encrypted data along with pad bits is delivered to private network. When data is to be retrieved, the pad bits are removed and then it is decrypted with the help of decryption key. This process of removing pad bits and decrypting the data is referred to as data preprocessing.

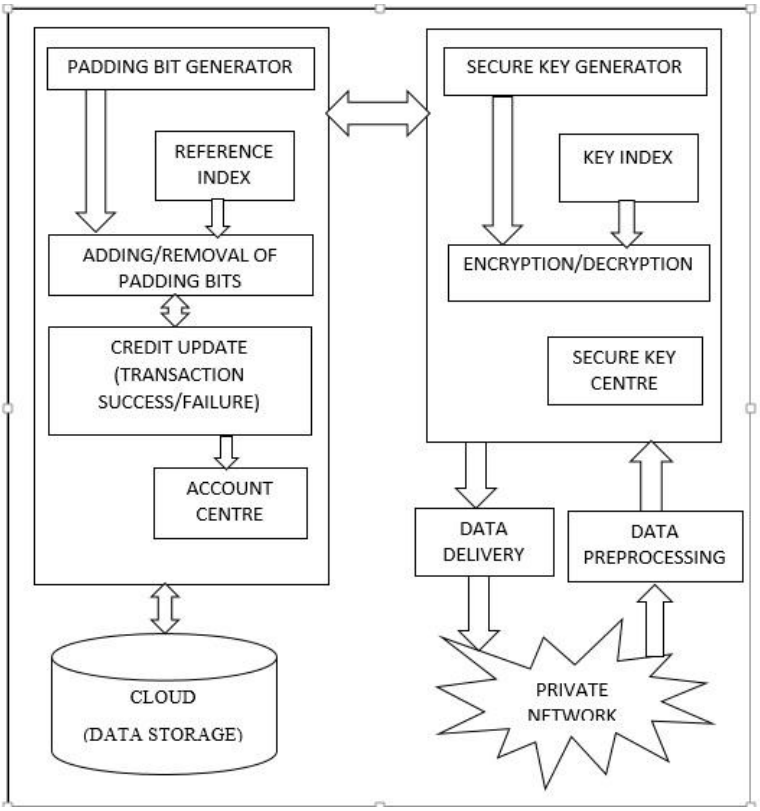

Fig 1. System Architecture of implemented model

Padding bits are generated using pad bit generation algorithm. Here we use OAEP algorithm along with RSA, to generate pad bits. The pad bits are generated randomly and its highly difficult to predict the pad bits, due to its randomness. It uses a policy of All-or-nothing, that is, either the complete plaintext is retrieved by deriving the correct cryptographic hash bits or the entire text is lost, even if one of the cryptographic hash bit changes. This policy makes this algorithm highly efficient and secure to implement.

The addition of pad bits to the data stored in the private network, is done, in order to ensure high security and privacy. As the pad bits are known only to the user, and also the pad bit sequence is generated randomly, the possibilities for attacking or destroying or hacking the data is very less when compared to traditional encryption technique. Security is high, data integrity and availability is made possible and original data is returned to the data owner.

5. PROPOSED ALGORITHM:

We are implementing **Optimal Asymmetric Encryption Padding (OAEP) Algorithm** for pad bit generation. This algorithm is a common algorithm which is often used along with RSA algorithm for secure encryption. It is a form of feistel network structure which uses a pair of random numbers to convert the plain text into asymmetric encryption.

The older padding techniques totally differ from modern padding technique. The older techniques doesn't possess randomness quality, whereas the modern technique possess it and this makes it more secure form of padding technique.

The OAEP algorithm makes use of a special mathematical function, called as **Random Oracle Model**, which makes mapping of queries with random responses. This makes the ciphertext more secure and data integrity is also maintained.

RSA uses asymmetric encryption technique, which means that, it uses two keys for encryption and decryption, namely, private and public key. The public key is used to convert plaintext to ciphertext, which is referred to as encryption process. The private key is used to convert ciphertext to plaintext, this process is referred to as decryption.

Also this algorithm uses a special function called Trapdoor-oneway permutation function. In this function forward computation is easy, whereas reverse or backward computation is hard, thereby making it hard for the attacker to manipulate the plaintext.

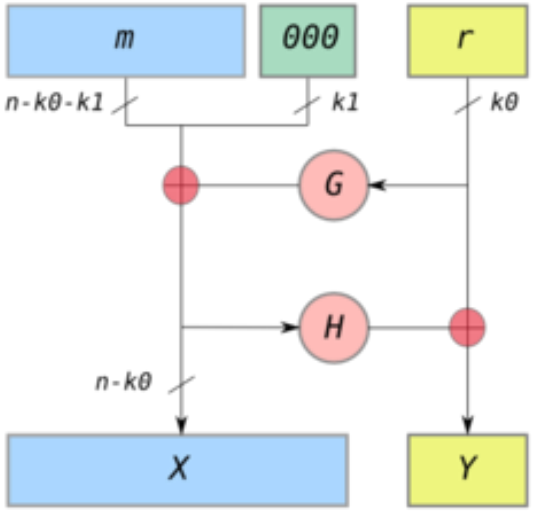

Fig 2. Optimal Asymmetric Encryption Padding Diagram

In the above diagram,

- ➢ n denotes the number of bits in the RSA modulus.
- ➢ k_0 and k_1 represents integers fixed by the protocol.
- ➢ m is the plaintext message, an $(n - k_0 - k_1)$-bit string
- ➢ G and H are typical cryptographic hash functions.
- ➢ For adding pad bits to data, the procedure is as follows:
- ✓ messages are padded with k_1 zeros to be $n - k_0$ bits in length.
- ✓ r is a random bit consisting of k_0-bit string
- ✓ G expands the k_0 bits of r to $n - k_0$ bits.
- ✓ X value is calculated m00..0 ⊕ G(r)
- ✓ H reduces the $n - k_0$ bits of X to k_0 bits.
- ✓ Y value is calculated as r ⊕ H(X)

The output is X || Y where X is shown in the diagram as the leftmost block and Y as the rightmost block.

- ➢ For removal of pad bits from data, the procedure is as follows:
- ✓ recover the random string as r which is calculated as Y ⊕ H(X)
- ✓ recover the message as m00..0 = X ⊕ G(r)

There are 2 goals that are satisfied by OAEP algorithm. They are:

- Randomness, used to convert a deterministic encryption scheme into an probabilistic scheme.
- It prevents partial decryption of ciphertexts, by ensuring that an attacker cannot recover even a part of the plaintext.

These two goals of OAEP algorithm along with RSA makes it more secure and reliable. OAEP can be used to build an **all-or-none transform**, that is to recover the plaintext completely, we must recover the entire X and Y. Even if a single cryptographic hash bit is changed, it changes the entire result of plaintext. This makes it more secure form of encryption.

6. CONCLUSION:

Cloud computing has been envisioned as next-generation architecture and it is used by many organizations and IT enterprises for data storage. Private clouds are specifically used within a company's firewall in order to store their company data. Data centres are built within their organization. Physical attack is not possible as they are present within the company premises, but at times the data stored in the private cloud are prone to several attacks.

Proper policies must be defined for access control, and only authorized users must be allowed to access the data. At times, even the cloud admin can be an untrusted/unauthorized person and this may lead to security issues.

Even though traditional encryption techniques are secure, there are more chances for hacking of data stored in the cloud (either public or private cloud). So here we implement an algorithm which generates padding bits along with encryption key to make the data stored in the cloud highly secure, and also making it less prone to vulnerable attacks.

Since the padding bits are known only to the data owner and they possess the randomness quality, the chances for damage, loss of data, or unavailability, or loss of correctness of data stored is very less when compared to traditional techniques. Still there are a few chances for attack. There may be pros and cons of their practical implementation. Providing complete security to the cloud computing environment is still a big challenge and researches are going on to make the cloud environment more secure.

7. REFERENCES:

[1] Cong Wang and Kui Ren, Illinois Institute of Technology, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, 2010 pp. 19-24.

[2] B. Wang, B. Li, H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE Transactions on Cloud Computing, Vol. 2, No. 1, 2014, pp. 43-56.

[3] K. Tysowski & M.A. Hasan, 'Hybrid Attribute-and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds' IEEE Transactions on Cloud Computing, Vol. 1, No. 2, 2013, pp. 172-186.

[4] Varadharajan. V & Tupakula. U, "Security as a Service Model for Cloud Environment", IEEE Transactions on Network and Service Management, Vol.11, No. 1, pp. 60-75, 2014.

[5] 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.

[6] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud, " IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[7] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses, " Computer, vol. 45, no. 1, pp. 39-45, 2012.

[8] 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.

[9] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys, " Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[10] The MD5 Message-Digest Algorithm (RFC1321).https: //tools.ietf.org/html/rfc1321, 2014.

[11] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores, " Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.

[12] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems, " Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[13] H. Shacham and B. Waters, "Compact Proofs of Retrievability, " Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.

[14] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing, " Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.

[15] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession, " Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing, " Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[17] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds, " Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.

[18] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service, " Proc. IEEE INFOCOM, 2012.

[19] B. Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud, " Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2013.

[20] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems, " Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.

[21] C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage, " IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[22] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud, " Proc. IEEE INFOCOM, pp. 2904-2912, 2013.

[23] B. Wang, H. Li, and M. Li, "Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics, " Proc. IEEE Int'l Conf. Comm. (ICC'13), pp. 539-543, 2013.

[24] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures, " Proc. 24th Ann. Int'l Cryptology Conf. (CRYPTO'04), pp. 41-55, 2004.

[25] 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 (ACNS'12), pp. 507-525, June 2012.

[26] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud, " IEEE Trans. Services Computing, 20 Dec. 2013, DOI: 10.1109/TSC.2013.2295611.

[27] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, " Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003.

[28] E. Brickell, J. Camenisch, and L. Chen, "Direct Anonymous Attestation, " Proc. 11th ACM Conf. Computer and Comm. Security (CCS'04), pp. 132-145, 2004.

[29] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing, " Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514-532, 2001.

[30] D. Cash, A. Kupcu, and D. Wichs, "Dynamic Proofs of Retrievability via Oblivious RAM, " Proc. 32nd Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT), pp. 279-295, 2013.

[31] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure MultiOwner Data Sharing for Dynamic Groups in the Cloud, " IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June2013.

[32] 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.

[33] A. Juels and B.S. Kaliski, "PORs: Proofs of Retrievability for Large Files, " Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp.584-597, 2007.

[34] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession, " Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm'08), 2008.