Fortified and Revocable Access Control for Multi-Authority Cloud Storage using CPABE

Bhuvaneswari Thangaraj
PG scholar,
Maharaja Engineering College,
Avinashi, India,

S. Umarani
Assistant Professor,
Maharaja Engineering College, Avinashi.

D. Sharmila
Head of the Department,
Bannari Amman Institute of Technology Sathyamangalam.

***Abstract*—Security and data privacy is paramount to cloud users seeking to protect their gigabytes of vibrant business data from the inquisitive eyes of unauthorized users who are attempting to exceed their authority and also it becomes a challenging issue in cloud storage systems. Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is observed as one of the most seemly technologies for data access control in cloud storage, because it gives more direct control access strategies to the cloud data owners. This CP-ABE scheme provides intrinsic security mechanisms designed to minimize the security attacks and threats in cloud system. In this paper, we design an expressive, efficient, fortified and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.**

Keywords*— *Adversary, Attribute Based Encryption, Secret and Update Keys

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principal of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. The authority can be the registration office in a university, the human resource department in a company, etc. The data owner defines the access policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies. There are two types of CP-ABE systems: single-authority CP-ABE where all attributes are managed by a single authority, and multi-authority CP-ABE where attributes are from different domains and managed by different authorities.

To design the data access control scheme for multi authority cloud storage systems, the main challenging issue is to construct the underlying Revocable Multi authority CP-ABE protocol. In, Chase proposed a multi-authority CP-ABE protocol, however, it cannot be directly applied as the underlying techniques because of two main reasons:

1) Security Issue: Chase's multi-authority CP-ABE protocol allows the central authority to decrypt all the cipher texts, since it holds the master key of the system;

2) Revocation Issue: Chase's protocol does not support attribute revocation.

A new revocable multi-authority CP-ABE protocol is proposed based on the single-authority CP-ABE. It is used extend the multi authority scenario and make it revocable. Apply the techniques in Chase's multi-authority CP-ABE protocol to tie together the secret keys generated by different authorities for the same user and prevent the collusion attack. Specifically, separate the functionality of

the authority into a global certificate authority (CA) and multiple attribute authorities (AAs). The CA sets up the system and accepts the registration of users and AAs in the system. It assigns a global user identity uid to each user and a global authority identity aid to each attribute authority in the system. Because the uid is globally unique in the system, secret keys issued by different AAs for the same uid can be tied together for decryption. Also, because each AA is associated with an aid, every attribute is distinguishable even though some AAs may issue the same attribute.

To deal with the security issue in, instead of using the system unique public key (generated by the unique master key) to encrypt data, our scheme requires all attribute authorities to generate their own public keys and uses them to encrypt data together with the global public parameters. This prevents the certificate authority in our scheme from decrypting the ciphertexts.

To solve the attribute revocation problem, assign a version number for each attribute. When an attribute revocation happens, only those components associated with the revoked attribute in secret keys and ciphertexts need to be updated. When an attribute of a user is revoked from its corresponding AA, the AA generates a new version key for this revoked attribute and generates an update key. With the update key, all the users, except the revoked user, who hold the revoked attributes can update its secret, key (Backward Security). By using the update key, the components associated with the revoked attribute in the ciphertexts can also be updated to the current version. To improve the efficiency, delegate the workload of ciphertexts update to the server by using the proxy re-encryption method, such that the newly joined user is also able to decrypt the previously published data, which are encrypted with the previous public keys, if they have sufficient attributes (Forward Security). Moreover, by updating the ciphertexts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys.

To achieve revocation on attribute level, some re-encryption- based attribute revocation schemes are proposed by relying on a trusted server. The cloud server cannot be fully trusted by data owners, thus traditional attribute revocation methods are no longer suitable for cloud storage systems. Ruj, Nayak and Ivan proposed a DACC scheme, where an attribute revocation method is presented for the Lewko and Waters' decentralized ABE scheme. Their attribute revocation method does not require a fully trusted server. But, it incurs a heavy communication cost since it requires the data owner to transmit a new ciphertext component to every non-revoked user.

1) We propose a Fortified and Revocable Access Control for Multi-Authority Cloud Storage,an expressive, efficient and more secured data access control scheme for multi-authority cloud storage systems, wich is a enhance security scheme and has better performance and efficient computation than existing access control schemes.

2) We construct a new Fortified and Revocable Mutlti-Authority CP-ABE scheme with efficient enryption and decryption. Specially, we design the main computation of the encryption and decryption by using key splitter based method.

3) We also design and efficient speedy attribute revocation method for multi-authority CP-ABE scheme that achives both forward and backward security. It reduces computaion and communication cost

The continuing of this paper is systematized as follows.

Section 2: Risks and Issues in existing access control Schemes
Section 3: Defines the System Model Framework
Section 4: Gives the detailed architecture and Implementation of our scheme by using Multi-authority CP-ABE
Section 5: Performance and Security Analysis of proposed Scheme
Section 6: Conclusion

II. ISSUES IN EXISTING ACCESS CONTROL SCHEMES

Security and reliability are main challenges of cloud computing. Clients are not likely to entrust their data that on cloud will not be accessed by other clients. To achieve security on cloud there are so many techniques and algorithm available.

Some of these techniques are:

- ✓ Encryption: Technique use complex algorithm to hide the original information with the help of encryption key.
- ✓ Authentication: Process which require creating a user name and password.
- ✓ Authorization: Practice which provides the list of authorized clients, who can access data stored on cloud system.

Some of the issues with the existing access control schemes are summarized as follows:

Technique 1: *A Secured Cost Effective Multi-Cloud Storage in Cloud Computing*

- ✓ **Journal name:** International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013
- ✓ **Author Name:** Prof.V.N.Dhawas,Pranali Juikar,Neha Patekar,Neha Lendghar,Sushant Vartak
- ✓ **Disadvantages:** Complexity in implementation and dividing more securable data

Technique 2: *A Secure Cloud Storage System with Secure Data Forwarding*

- ✓ **Journal name:** International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013
- ✓ **Author Name:** Aarti P Pimpalkar, Prof. H.A. Hingoliwala
- ✓ **Disadvantages:** Only Partial decryption is performed by the key server and additional image login leads to unsecure access

Technique 3: *Secured Cloud Storage using Raptor Codes*

- ✓ **Journal name:** International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013
- ✓ **Author Name:** Aarti P Pimpalkar, Prof. H.A. Hingoliwala
- ✓ **Disadvantages:** Identification of new symbols in traditional code is capable of recovering all the input symbols even in face of a fixed fraction of erasures.

Technique 4: *Data Security Algorithms for Cloud Storage System using Cryptographic Method*

- ✓ **Journal name:** International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013
- ✓ **Author Name:** Prakash G L, Dr. Manish Prateek, and Dr. Inder Singh
- ✓ **Disadvantages:** Performance issues and the Properties of the overheads are not analyzed

Technique 5*: Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage (CP-ABE)*

- ✓ **Journal name:** IEEE Transaction on Parallel and Distributed Systems, Vol.25, No. 7, July 2014
- ✓ **Author Name:** Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE
- ✓ **Disadvantages:** Issues computation efficiency and the revocation method

III. SYSTEM MODEL

A. SYSTEM MODEL

Figure 1 shows the System Model for data access control in multi-authority cloud storage is considered. There are five types of entities in the system.

1) *A certificate authority (CA)*
2) *Attribute authorities (AAs)*
3) *Data owners or vendors (owners)*
4) *Cloud server (server)*
5) *Data consumers (users)*

CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs. For each legal user in the system, the CA assigns a global unique user identity and also generates a global public key for the user. Each user will be issued a Social Security Number (SSN) as its global identity. Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In the proposed scheme, every attribute is associated with a multiple AA, but each AA can manage an arbitrary number of attributes. AA has full control over the structure and semantics of its attributes Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a Secret key and update key for each user reflecting his/her attributes.

Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities. The secret key is splitd into N pieces and stored into multiple key servers. Each owner first distributes the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

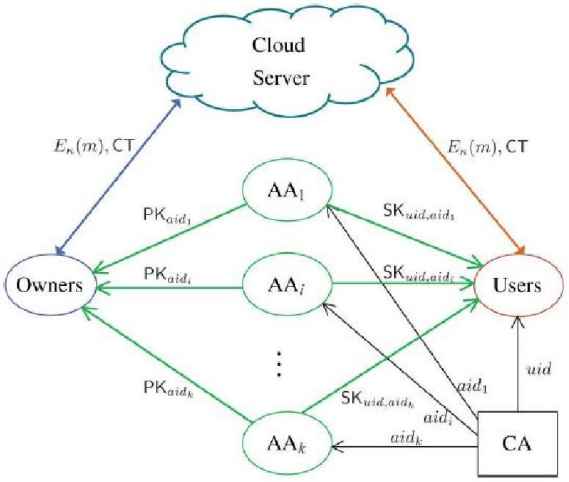

Figure 1. System Model of DAC in Multi Authority Cloud Storage

Then, the owner sends the encrypted data to the cloud server together with the ciphertexts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the ciphertext; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data. The proposed scheme is able to surface the below challenges:

1) Protect user's privacy against each single authority.
2) Tolerant against authority compromise, and compromising of up to (N − 2) authorities does not bring the whole system down.
3) Provides the detailed analysis on security and performance to show feasibility of our scheme.
4) The real toolkit of multi-authority based encryption scheme is implemented

B. FRAMEWORK

The framework has been built using the below defined components of layers.

The proposed scheme is used to control the outsourced data and provide the standard quality of the cloud storage service for the cloud users with an efficient encryption and decryption computations and multiple key server with key splitter techniques. This multi-authority CP-ABE provides authority that is answerable for attribute management, efficient computation, key distribution and the revocation methods.

There are seven layers defined in the proposed scheme. The functionality of those layers can be summarized as follows:

- ✓ **Proxy layer:** This proxy layer acts as interface between the users and the rest of the servers available in the cloud.
- ✓ **Cloud data server layer:** Data server has two different entities can be recognized as the cloud users and the cloud service provider. Multiple data servers are proposed in this scheme to avoid the traffic.
- ✓ **Cloud data storage server layer:** All the data and the files are stored in these storage servers which are stored by the both individual customers and organizations. Similar to data server there are multiple storage servers are introduced to handle big volume of data
- ✓ **Cloud Key server layer:** Multiple key servers are proposed in this scheme for efficient computation and attribute revocation method. Key server is used to store the secret key that are encrypted or fragmented by the key splitter.
- ✓ **Key splitter:** Key splitter is used to divide cryptographic key K in n safe pieces K1, K2, Kn Such that knowledge of any J pieces can be used to compute K easily. These pieces are assigned to N nodes. Shamir's algorithm is to divide Key in n parts, Kz, Kn such that there is a special part Kt which contains the information of all other parts, and K cannot be computed without Kt. However, K cannot be computed without especial part Kt.
- ✓ **Cloud consumers layer:** Cloud users are the one who have the data to be stored in the cloud and depend on cloud for data computation and transformation. Cloud consumers can be both customers and individual organizations.
- ✓ **Cloud service provider (CSP):** This layer owns, built and manages the storage servers in distributed manner and functions as live cloud computing systems.

IV. REVOCABLE ACCESS CONTROL SCHEME

The existing framework of the scheme is modified and to make it more practical to cloud storage systems, in which data owners are not involved in the key generation. Specifically, a user's secret key is not related to the owner's key, such that each user only needs to hold one secret key from each authority instead of multiple secret keys associated to multiple owners. The efficiency of the attribute revocation method is greatly improved.

Specifically, in our new attribute revocation method, only the ciphertexts that associated with the revoked attribute needs to be updated, all the ciphertexts that associated with any attribute from the authority (corresponding to the revoked attribute) should be updated.

A new revocable multi-authority CP-ABE protocol is proposed based on the single-authority CP-ABE proposed by Lewko and Waters in [16]. That is used to extend multi authority scenario and make it revocable. Apply the techniques in Chase's multi-authority CP-ABE protocol to tie together the secret keys generated by different authorities for the same user and prevent collusion attack.

A. Architecture

In Revocable architecture, as discussed in previous section, we proposed sever layered architecture in order to improve the cloud security and accessibility. The proposed scheme is able to safe guard each user's privacy again single or even multiple authorities and it is lenient against authority mediation and compromising of up to N-2 node authorities does not bring the whole system down

The framework of the scheme is modified and to make it more practical to cloud storage systems, in which data owners are not enrolled in the key generation. Specifically, a user's secret key is not related to the owner's key, such that each user only needs to hold one secret key from each authority instead of multiple secret keys associated to multiple owners. The attribute revocation method's efficiency is greatly improved. Specifically, in this new

proposed attribute revocation method, only the ciphertexts that associated with the revoked attribute needs to be updated, all the ciphertexts that associated with any attribute from the authority (corresponding to the revoked attribute) should be updated.

Moreover, in our new attribute revocation method, both the key and the ciphertext can be upgraded by using the same update key, instead of requiring the owner to create update information for each ciphertext, such that owners are not required to store each random number generated during the encryption. The expressiveness of our access control scheme is highly improved, where the limitation that each attribute can be removed and only appear at most once in a ciphertext.

B. Implementation

Figure 2 Display the system model of fortified and revocable access control for multi-authority cloud storage using CP-ABE algorithm. There are five methods proposed in this paper:

1. **Key Generation and Storage**
2. **Key Splitter**
3. **Key Transfer**
4. **Key Retrieval**
5. **Distributed Key Storage**

Methods are summarized as follows**:**

- ✓ **Key Generation and Storage**: User can generate new symmetric cryptographic key K or can store already existing cryptographic keys as required using proposed technique. Key splitter will split the key into n pieces and store each part in different server. One main piece lets Kn of key will be assigned to consumer of application. This piece of key has information of all other pieces and actual key cannot be regenerated without this piece.

- ✓ **Key Splitter**: User can split the cryptographic key K into pieces and store it into multiple key servers in distributed manner. Key server can be located in different locations in order to tighten the security of the cloud data. Each piece of key is store in distributed server, so that hacker cannot access or retrieve the keys directly. Key splitter is one of intrinsic method introduced in fortified and revocable access control for multi-authority cloud storage.

- ✓ **Key Transfer:** User can transfer completely computed key or the component of key on public cloud for data processing. Public Key Cryptographic Standard (PKCS7) will used to transfer such key that is developed by RSA Laboratories and used to wrap data in an envelope to securely transfer it. This protocol used to wrap message in an envelope and signed by sender. Receiver knows the encryption key to decrypt the encrypted message.

- ✓ **Key Retrieval:** On the request of key retrieval all, the components will fetch the key from key store through computational server. Client machine will prompt consumer of application to enter his/her piece of key. Original Key will compute on the fly after taking information from consumer on consumer's terminal.

- ✓ **Distributed Key Storage:** The goal of this module is to divide cryptographic key K in n safe pieces K1, K2, Kn Such that knowledge of any J pieces can be used to compute K easily. These pieces are assigned to N nodes. Shamir's algorithm is to divide Key in n parts, Kz, Kn such that there exists a special part Kt which contains the information of all other parts, and K cannot be computed without Kt. However, K cannot be computed without especial part Kt.

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

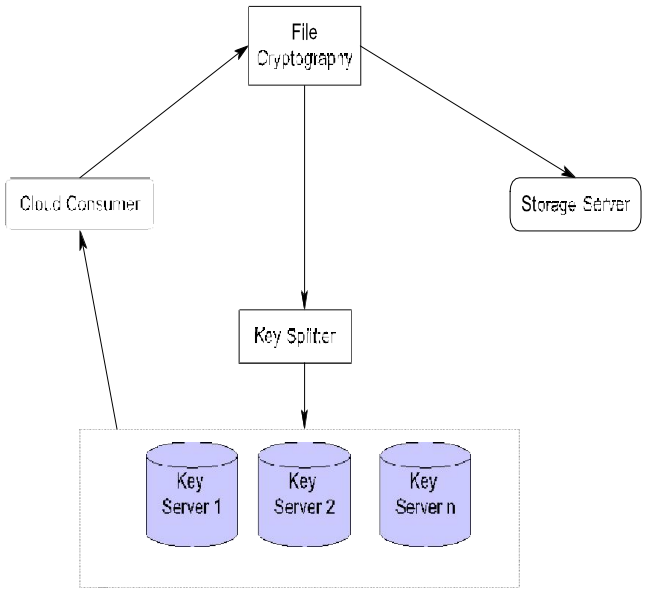

Figure 2. System Model: Fortified and Revoked Access Control for MACS

V. BENEFITS IN PERFORMANCE AND SECURITY

A. PERFORMANCE ANALYSIS

Performance of the cloud storage system can be improved with our new proposed scheme. The performance improvements as follows:

- ✓ Separate the functionality of the authority into a global certificate authority and multiple attribute authorities which would increase the enactment of the system.

- ✓ Assigns a global UID and global AID to each user in the system to distinguish from other user in order to improve the cloud system performance. UID-User Identity, AID-Authority Identity.

B. SECURITY ANALYSIS

- ✓ Proposes great and enhanced security challenge to data access control in the cloud storage systems.
- ✓ It achieves both forward and backward security. The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt (backward security). The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient attributes (Forward Security).
- ✓ Increased data and file security, it is very difficult for an intruder to access, misuse and destroy the original form of data in the file available in the cloud storage system.
- ✓ Improve the data and file security in public cloud computing environment by storing file contents in different servers.

VI. CONCLUSION

This paper mainly describes about the methods and algorithms, which are used for providing the high end of security in cloud storage system and accessing data effectively and securely. On measuring the different previous works, we analyzed the advantages and disadvantages of each work and finally we derived the new technique, which over comes the drawbacks of previous work by analyzing all the information's in all state of exploration and by providing the more secured cloud environment. Finally we conclude that CPABE scheme provides multiple authorities that are responsible for attribute management and key distribution. In this new scheme, we enhanced the computational efficiency, attribute revocation efficiency and also enriched the security in the cloud storage system. This fortified multi-authority CP-ABE is a capable technique, which can be applied in any information systems and online social networks and other big data related applications.

REFERENCES

[1] P. Mell and T. Grance, ''The NIST Definition of Cloud Computing,'' *National Institute of Standards and Technology*, Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. *IEEE Symp. Security and privacy (S&P'07)*, 2007, pp. 321-334.

[3] B. Waters, ''Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,'' in Proc. 4th *Int'l Conf. Practice and Theory in Public Key Cryptography (PKC'11),* 2011, pp. 53-70.

[4] V. Goyal, A. Jain,O. Pandey, andA. Sahai, ''Bounded Ciphertext Policy Attribute Based Encryption,'' in Proc. 35th *Int'l Colloquium on Automata, Languages, and Programming (ICALP'08)*, 2008, pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ''Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,'' in Proc. *Advances in Cryptology-EUROCRYPT'10*, 2010, pp. 62-91.

[6] M. Chase, ''Multi-Authority Attribute Based Encryption,'' in Proc. *4th Theory of Cryptography Conf. Theory of Cryptography (TCC'07)*, 2007, pp. 515-534.

[7] M. Chase and S.S.M. Chow, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in Proc. *16th ACM Conf. Computer and Comm. Security (CCS'09)*, 2009, pp. 121-130. [8] A.B. Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11, 2011, pp. 568-588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. *5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10)*, 2010, pp. 261-270.

[10] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' *IEEE Trans. Parallel Distributed Systems*, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[11] J. Hur and D.K. Noh, ''Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,'' *IEEE Trans. Parallel Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, July 2011.

[12] S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. *6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11)*, 2011, pp. 411-415.

[13] S. Ruj, A. Nayak, and I. Stojmenovic, ''DACC: Distributed Access Control in Clouds,'' in Proc. *10th IEEE Int'l Conf. TrustCom, 2011*, pp. 91-98.

[14] K. Yang and X. Jia, ''Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,'' in Proc. *32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12)*, 2012, pp. 1-10.

[15] D. Boneh and M.K. Franklin, ''Identity-Based Encryption from the Weil Pairing,'' in Proc. 21st Ann. Int'l Cryptology Conf.: *Advances in Cryptology - CRYPTO'01*, 2001, pp. 213-229. [16] A.B. Lewko and B. Waters, ''New Proof Methods for Attribute- Based Encryption: Achieving Full Security through Selective Techniques,'' in Proc. 32st Ann. *Int'l Cryptology Conf.: Advances in Cryptology - CRYPTO'12*, 2012, pp. 180-198.

[16] Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE. "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage". *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, VOL. 25, NO. 7, JULY 2014

BIOGRAPHY

Ms. Bhuvaneswari Thangaraj has received her Bachelor degree in Information Technology (B.Tech) from Anna University, Chennai, India. Currently she is pursuing Master degree in Information Technology (M.Tech) in Maharaja Engineering College from Anna University. Her areas of interests include Cloud Systems, Artificial Intelligence, Networking, data mining etc.