ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

Enhanced Data Access Control for Multi Authority Cloud Storage

Pranay Khobragade, Nilima Dongre
Dept. of Information Technology, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, India

Abstract*—Data access control is an effective way to ensure the data security in the cloud. The safety of information becomes a biggest concern in cloud storage systems, because of data redistribution and insecure cloud servers. CP-ABE is considered as one of the greatest acceptable technologies for information access control mechanism in cloud storage, because it gives more straightforward control to the creator of data on access mechanism. However, it is hard to precisely use available CP-ABE schemes to information access policies for cloud storage systems due to attribute revocation issue. In this paper, we construct efficient data access restriction methods for multi-authority cloud storage systems, where there are many authorities present and all are able to get attributes individually. Particularly, we introduce a revocable multi-authority CP-ABE scheme, and implement it as the basic method to create the data access restriction system. Our attribute revocation process can effectively accomplish both forward security and backward security. We also propose A proxy signature scheme which permits an entity to delegate its signing rights to another, and a ring signature, a verifier is convinced that a signature is computed using one of group members private keys, but the verifier is not able to determine which one. This property can be used to preserve the identity of the signer from a verifier.

***Keywords*—Information tracking, Data masking, Manipulating attacks, Blindly Removal, Steganography, and Watermarking.**

I. INTRODUCTION

Cloud storage is an essential service of cloud computing which offers services for information owners to upload their information in the cloud. This latest paradigm of information uploading and information access control mechanism introduces a few difficulties to information access restriction mechanism. Because the cloud server cannot be completely dependable by information creator, they could stop being dependent on servers to do access control. CP-ABE is regarded as one of the best suitable method for information access restriction mechanism in cloud storage systems, because it gives the creator of information straightforward control on access policies. In CP-ABE mechanism, there is a management for attribute management and key distribution. The management can be the registration office in a university, the human resource department in a company, etc. The creator of information describes the access policies and encrypts information as per the policies. Each person will be getting a secret key having its attributes. A person can decrypt the information only when its attributes fulfill the access policies.

CP-ABE systems can be categorized as: single-authority CP-ABE where all characteristics can be handled by a single authority, and multi-authority CP-ABE where characteristics are from distinct domains and handled by distinct authorities. Multi-authority CP-ABE is more convenient for information access restriction of cloud storage mechanism, as users may get attributes issued by many authorities and information creator may also proved the information using access mechanism explained over attributes from various superiorities. For ex-ample, in an E-health mechanism, information creator may provide the information using the access control mechanism Doctor AND Researcher, where the entity Doctor is entitled to a medical organization and the entity Researcher is entitled to the administrators of a clinical trial. However, it is hard to straightly appeal this multi-authority CP-ABE mechanism to multi-authority cloud storage systems due to the attribute revocation issue.

Cloud computing is a new concept of computing technique, by which computer resources are provided dynamically via Internet. It attracts considerable attention and interest from both academia and industry. However, it also has at least three challenges that must be handled before applied to our real life. First of all, data confidentiality should be guaranteed. When sensitive information is stored in cloud servers, which is out of users control in most cases, risks would rise dramatically. The servers might illegitimately scan users information and access secret information. On the other hand, unauthorized users may also be able to intercept some ones data (e.g. server compromise). Secondly, personal information (defined by a users attributes) is at risk because ones identity is authenticated according to his information. As people are becoming more concerned about their privacy these days, the privacy-preservability is very important. Preferably, any authority or server alone should not know any clients personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers.

Various techniques have been proposed and/or used to address the aforementioned problems. One of them was Identity based encryption (IBE) in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. This is different from Public-key Encryption, in that the encrypter does not need to issue extra key to decrypter for each cipher text. In the IBE, the private key, which contains the identity of the holder, is distributed to every user only once when he joins the system.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

In multi-authority cloud storage mechanism, persons characteristic can be alternated irrationally. A person may be request some new characteristic or revert some present characteristic. And his permission of data access should be changed accordingly. However, present characterized revert mechanism [9], [10], [11], [12] may depend on a reliable server or lover the potential, they are not good enough to handle the characteristic revert difficulties in information access prevention mechanism in multi-authority cloud storage mechanism.

In this paper, we 1st introduce a revert multi-authority CP-ABE mechanism, where a reliable and defended revert mechanism is introduced to deal with the characteristic revert issue in the system. Our characteristic revert mechanism is good enough to acquire optimal cost of communication and computation, and is safely achieve both backward security (The user removed from the system cannot decipher any new encrypted data) and forward security (The new members can also decipher the old data). Our method does not rely on the server to be absolutely dependable due to the ever-changing keys of users and not the server. Even if the server is not fully dependable in few schemes, our method can still ensure the backward security. Then, we use our revert multi authority CP-ABE mechanism as the basic method to build the user friendly and protective information access restriction method for multi-authority cloud storage systems.

II. LITERATURE SURVEY

P. Mell and T. Grance, [1] denes meaningful scenario of cloud computing and is planned to handle as a means for extensive observation of cloud services and deployment strategies, and to contribute a baseline for analysis from what is cloud computing to how to actually use cloud computing. The service and deployment models created form a simple taxonomy that is not design to prescribe or inhibit any particular method of deployment, service delivery, or business operation.

J. Bethencourt, A. Sahai, and B. Waters, [2] presents a system for realizing complex access control on encrypted data called Cipher text Policy Attribute Based Encryption. By using this technique encrypted data can be kept confidential even if the storage server is untrusted; moreover, this methods are secure against collusion attacks.

B. Waters, [3] present a new methodology for realizing Cipher text Policy Attribute Encryption (CP-ABE) under concrete and non interactive cryptographic assumptions in the standard model.

V. Goyal, A. Jain,O. Pandey, andA. Sahai, [4] present the first construction of a cipher text policy attribute based encryption scheme having a security proof based on a number theoretic assumption and supporting advanced access structures.

A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, [5] present two fully secure functional encryption schemes. The First result is a fully secure attribute-based encryption (ABE) scheme. The second result is a fully secure (attribute-hiding) predicate encryption (PE) scheme for inner-product predicates.

M. Chase, Multi-Authority Attribute Based Encryption, [6] Scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys, and it also shows how to apply our techniques to achieve a multi authority version of the large universe fine grained access control ABE.

M. Chase and S.S.M. Chow, [7] propose a solution which removes the trusted central authority, and protects the users privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice.

A.B. Lewko and B. Waters, [8] propose a Multi-Authority Attribute-Based Encryption (ABE) system in which any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reject their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities.

S. Yu, C. Wang, K. Ren, and W. Lou, [9] focus on an important issue of attribute revocation which is cumbersome for CP-ABE schemes. They resolve this challenging issue by considering more practical scenarios in which semi-trustable on-line proxy servers are available.

M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, [10] propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, they leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file.

J. Hur and D.K. Noh, [11] propose an access control mechanism using cipher text policy attribute based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group.

S. Jahid, P. Mittal, and N. Borisov, [12] propose EASiER, an architecture that supports fine-grained access control poli-cies and dynamic group membership by using attribute-based encryption.

S. Ruj, A. Nayak, and I. Stojmenovic, [13] propose a new model for data storage and access in clouds. this scheme can avoids storing multiple encrypted copies of same data.

K. Yang and X. Jia, [14] design an access control frame-work for multi-authority systems and propose an

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

efficient and secure multi-authority access control scheme for cloud storage. They also propose a new technique to solve the attribute revocation problem in multi-authority CP-ABE systems.

D. Boneh and M.K. Franklin, [15] propose a fully functional identity based encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model assuming a variant of the computational Diffie- Hellman problem.

A.B. Lewko and B. Waters, [16] develop a new methodology for utilizing the prior techniques to prove selective security for functional encryption systems as a direct ingredient in devising proofs of full security. In particular, they present a Cipher text Policy Attribute-Based Encryption scheme that is proven fully secure while matching the efficiency of the state of the art selectively secure systems.

COMPARATIVE ANALYSIS

A. Comparison

TABLE I: Comparison

Year	Name of Paper	Method	Result	Advantages	Drawbacks
2006	Cipher text policy attribute based encryption	Cipher text policy attribute based encryption	Secure against collusion attacks	In untrusted server the encrypted data can be kept confidential	It is proved secure under the generic group heuristic
2009	Improving privacy and security in multi-authority attribute-based encryption	Multi-authority ABE scheme	Removes the trusted central authority, and protects the users privacy	System does not rely on a central authority	Concern of security of the encryption and privacy of the users
2010	Attribute based data sharing with attribute revocation	Cipher text policy Attribute based encryption	It enables the authority to revoke user attributes with minimal effort	It places minimal load on authority upon attribute revocation events	CP-ABE schemes are not able to achieve provable security and user revocation is extremely hard
2011	Attribute-based access control with efficient revocation in data outsourcing systems	Cipher text policy attribute-based encryption	System is efficient and scalable to securely manage the outsourced data	Enabling user access control enhances the backward/forward secrecy of outsourced data	Revocation of any attribute or any single user in an attribute group would affect the other users in the group
2011	DACC: distributed access control in clouds	Distributed access control in clouds	The cipher texts cannot be decrypted by the cloud	The secret keys can be distributed using key distribution centers (KDCs)	This technique is only efficient in honest net-works, if not then we have to take care of net-work
2013	Scalable and secure sharing of personal health records In cloud computing using ABE	Attribute-based encryption	Through implementation and simulation, it occurs that system is both scalable and efficient	It enables dynamic modification of access policies, supports efficient on-demand user/attribute revocation	The scheme has much smaller secret key size

B. Analysis

J. Bethencourt, A. Sahai, and B. Waters, [2] proposed Cipher text-Policy Attribute-Based Encryption scheme where they present a system for realizing complex access control on encrypted data.

M. Chase and S.S.M. Chow, [7] proposed Multi-authority ABE scheme that tells the solution which removes the trusted central authority, and protects the users privacy by preventing the authorities from pooling their information on particular users.

S. Yu, C. Wang, K. Ren, and W. Lou, [9] proposed Cipher text-Policy Attribute Based Encryption scheme where they focus on an important issue of attribute revocation which is cumbersome for CP-ABE schemes.

J. Hur and D.K. Noh, [11] proposed an access control mechanism using cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

S. Ruj, A. Nayak, and I. Stojmenovic, [13] proposed Distributed Access Control in Clouds which avoids storing multiple encrypted copies of same data.

M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, [10] proposed Attribute-Based Encryption scheme in which a novel patient centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers and focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users.

A proxy signature method is a type of the typical digital signature method, which allows proxy users to produce sig-natures on behalf of a real user. The Ring signature produces homomorphic verification, so that local user is able to analyze and share information without entirely downloading it, and yet they do not understand who is the user of each block.

IV. PROPOSED SYSTEM

To implement the information access restriction mechanism for multi authority cloud storage systems, the primary concern is to build the basic Revert method for Multi-authority CP-ABE protocol. The multi-authority CP-ABE protocol cannot be directly applied as the underlying techniques because of two main reasons:

1. Security Problem: Chases multi-authority CP-ABE scheme gives authority to the central authority to decipher all the encrypted text, since it carries the main key of the system.

2. Revocation Problem: Chases protocol does not support characteristic revert mechanism.

To overcome these issues we propose an enhanced revocable multi-authority CP-ABE protocol

Proposed Methodology: The enhanced revocable multi authority CP-ABE protocol is based on the single authority CP-ABE. That is we extend it to multi authority scenario and make it revocable. We apply the methods in multi-authority CP-ABE scheme to bind each other with the secret keys produced by multiple organizations for the same person and secure from the collusion attack.

Concerning with the security problem, rather we use the system uncommon public key (produced by peculiar master key) to encrypt information. Our method needs all attribute authorities to produce their own public keys and uses them to encrypt information and global public parameters with each other. This protects the certificate authority in our mechanism from deciphering the encrypted data.

To solve the characteristic revert issue, we allocate a version number for each characteristic. When a characteristic reverts occurs, only factor related to the revert characteristic in secret keys and encrypted data need to be modified.

We introduce the comprehensive development of our access restriction mechanism, which contains following seven phases:

A) System Initialization
B) Key Generation
C) Data Encryption
D) Data Decryption
E) Attribute Revocation
F) Proxy Signature
G) Ring Signature

A. System Initialization

The system initialization contains CA Setup and AA Setup.

1) CA Setup: The CA arranges the system by applying the CA setup method, which takes input as preservation constrains. The CA 1st selects two multiplicative groups G and G_T with the equivalent prime order p and a bilinear map e : G G ! G_T . It also selects a hash method that compares the string to a component in G, such that the protection will be increased in the random oracle. Then, the CA selects two arbitrary numbers a,b ¤ Z_p as the global master key GMK = (a,b) of the system and enumerate the global public parameters.

The CA accepts both User Registration and AA Registration.

1) User Registration: Every user should register to the CA during the system initialization. If the person is a legitimate person in the system, the CA then allocate a globally uncommon persons identity uid to this persons. For each person or user uid, the CA 1st produce two arbitrary numbers as its global secret keys GSK_{uid}. It then produces the persons global public keys GPK_{uid}.

2) AA Registration: Each AA should also register itself to the CA during the system initialization. If the AA is a legitimate authority in the system, the CA rst allocate a global attribute authority identification aid to this AA. Then, the CA posts the other global public/secret key of every user $\left(GPK_{uid}{}^{0}; GSK_{uid}\right)$ to the AA_{aid}. It also sends a verification key to the AA_{aid}, which can be used to verify the certificates of users issued by the CA.

2) AA Setup: For each attribute it generates Secret key and public key.

1) Secret Key Let S_{aid} defines the group of all attributes maintained by each attribute authority AA_{aid}. It selects three arbitrary numbers $\alpha_{aid}, \beta_{aid}, \mu_{aid}$ as the authority secret key $SK_{aid} = (\alpha_{aid}, \beta_{aid}, \gamma_{aid})$,

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

where α_{aid} is used for information encoding, β_{aid} is used to categorize attributes from peculiar AAs and α_{aid} is used for attribute revocation.

2) Public Key for each attribute

$PK_{x_{aid}}(PK_{1,x_{aid}} = H(x_{aid})^{\upsilon_{xaid,yaid}}, (PK_{2,x_{aid}} = H(x_{aid})^{\upsilon_{xaid,yaid}})$

where υ_{aid} is a version key

B. Key Generation

Each persons uid is needed to verify itself to the AA_{aid} before it can be assigned some attributes from the AA_{aid}. The user submits its certificate Certificate (*uid*) to the AA_{aid}. The AA_{aid} then verify the person by using the verification key taken from the CA.

If it is a legitimate person, the AA_{aid} characterize a group of attributes $S_{uid;aid}$ to the persons *uid* on the basis of its needs or identity in its administration department. Otherwise,

it aborts. Then, the AA_{aid} produces the persons secret key $SK_{uid;aid}$ by following the secret key generation procedure SKeyGen. If the user uid does not hold any attribute from

AA_{aid}, the secret key $SK_{uid;aid}$ only contains the first com-ponent $K_{uid;aid}$.

1) Each person uid is needs to verify itself to the AA_{aid} before it can be assigned some attributes from the AA_{aid}.
2) The AA_{aid} then authenticates the user by using the verification key issued by the CA.
3) If it is a legal user, the AA_{aid} entitles a set of attributes to the user *uid* according to its role or identity. Otherwise, it aborts.

C. Data Encryption

Before uploading information m to cloud servers, the information holder applies some rules on the information as follows.

Step 1. It sorts the information into its several components followed by its level of details.

Step 2. It encodes the components of information with other content keys by using symmetric encryption mechanism.

Step. 3. It then designs an access policy for each content key and encode it by applying the encryption algorithm.

The encryption procedure needs global public parameters GPP, a group of public keys and an access mechanism as an input over all the involved attributes. To encrypt the content key the encryption method 1st needs an arbitrary encryption exponent and a random vector. Then, it randomly chooses and computes the cipher text.

D. Data Decryption

The decryption method can be designed as follows,

Step 1. It takes the cipher text CT which consists of an access structure, a global public key and a global secret key of the person and a group of secret keys from all the involved AAs.

Step 2. If the persons desires can match the access structure, then the person will get key

$$\prod_{k \in I_A} e(g,g)^{\alpha_{aid}} k^s$$

Step 3. Person need this to decrypt the cipher text as,

$$k = C / \prod_{aid_k\ I_A} e(g,g)^{\alpha_{aid}} k^s$$

Step 4. Then, the person can use the decrypted content key to latter decrypt the encrypted information component.

E. Attribute Revocation

As we explained earlier, there are two conditions of the attribute revocation:

a) The revoked person cannot decipher current encrypted data having updated public attribute keys (Backward Security).

b) The new person who has considerable attributes should also be able to decipher the existing or presented cipher texts, which are encrypted with different public attribute keys before (Forward Security).

Consider an attribute $\tilde{x}_{aid'}$ is revoked from the persons uid' by the $AA_{aid'}$. The attribute $\tilde{x}_{aid'}$ is stand for the Revoked Attribute and the persons uid' is stand for the Revoked Person.

We also imply the Non-revoked person, which stand for the group of person who has the revoked attribute $\tilde{x}_{aid'}$ but have not been discarded. Our revocation method follows three steps:

1) Update Key Generation: When an attribute is taken away from a person the authority uses the update key generation algorithm to calculate the update keys.

Step 1. The procedure requires the secret key, the revoked attribute and its present version key.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

Step 2. Then it produces a latest version key for revoked at-tribute, and latest update key to update the encrypted data.

Step 3. The $AA_{aid'}$ then creates an uncommon update key for secret key update by each non-revoked persons uid and produce the update key to update encrypted data.

Step 4. The $AA_{aid'}$ provides the $UKs, \tilde{x}_{aid'}$, uid to non-revoked persons uid and provides $UKs, \tilde{x}_{aid'}$ to the cloud server.

Step 5. The $AA_{aid'}$ updates public key of revoked attribute and broadcast it on its public bulletin board.

Step 6. Then, the authority makes announcement for all the users that the public attribute key of the revoked attribute is updated.

2) Secret Key Update by Non Revoked Users: Upon acquiring the update key $UKs, \tilde{x}_{aid'}$, uid the persons uid then update his/her secret key by applying the latest secret key update procedure SK Update.

The algorithm is as follows,

$$\tilde{SK}_{uid,aid'} = (\tilde{K}_{uid,aid'} = K_{uid,aid'},$$

$$\tilde{K}'_{uid,aid'} = K'_{uid,aid'},$$

$$\tilde{K}_{\tilde{x}\,aid,uid} = K_{\tilde{x}\,aid,uid.} UK_{s,\tilde{x}\,aid,uid,}$$

$$\forall x_{aid'} \in S_{uid,aid'} / \{\tilde{x}_{aid'}\} : K_{x\,aid,uid} = K_{x\,aid,uid})$$

Remark only the entity related with the revoked attribute $\tilde{x}_{aid'}$ in the secret key has right to be updated, while other entities are kept as it is.

3) Cipher text Update by Cloud Server: All the encrypted data that is related with the revoked attribute are need to be updated to its newest version. Afterwards the creator of information will do the updates on the encrypted data, which will carry the heavy burden on creator of information. To enhance the reliability, we shift the task of updating encrypted data from creator of information to the cloud server, such that it can remove the burden of transmission between creator of information and cloud server, and the calculated cost on creator of information.

F. Proxy Signature

The proxy signature scheme allows an original signer to delegate his signing right to a proxy signer to sign the message on behalf of an original signer. The steps of the scheme are as follows:

a) Generation: The original singer entity A should do the following:

Step 1	Select an integer $i \in Z_{p-1}$.
Step 2	compute $t_1 = g^i$ mod p
Step 3	find $b = u_A + i * t_1$ mod p-1
Step 4	pass (b, t_1) to a proxy signer entity B in a Secure channel.

b) Signing: Entity B should do the following:

Step 1	verifies $g^b \equiv e_A * t_1^i$ mod p.
Step 2	signs the message m_P on behalf of entity A.
Step 3	employs b as a substitute to u_A
Step 4	implements an ordinary signing process.
Step 5	the generated proxy signature on m_p is $(m_P, s_b, (m_p)t_1)$

c) Verification: Entity V should do the following:

Step 1	find $e^- = e_A * t_1^i$ mod p, as the new public key
Step 2	a verification of proxy signature is implemented by the same verifying process as in an original signature scheme.

G. Ring Signature

Using ring signatures, a person are satisfied that a signature is calculated using one of group participant's private keys, but the person is enable to find which one.

The ring signature can be achieved using following three ways, There are keygen, ring sign and ring verify,

1) In keygen, his/her public key and private key is generated for each user in the group.
2) Ring sign, in the group the person is capable to produce a signature on its block identifier and on a block with his/her and all the group representatives' public key.
3) In ring verify a verifier is to check whether a given block is signed by a group representative.

V. CONCLUSION

In this paper, we introduce a revocable multi-authority CP- ABE mechanism that can handle considerable attribute revocation. Then, we design a powerful information access restriction method for multi-authority cloud storage systems. Our method is efficiently protects the system in the arbitrary oracle model. The revocable multi-authority CP-ABE is an efficient method, which can be adapted in any remote storage systems and online social networks etc. We also used proxy signature and ring signature. A proxy signature method is a variation of the common digital signature method which allows a proxy user to produce signatures on place of an original user. Ring signature to designs homomorphic verification, so that public user is able to analysis and share

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

information without completely downloading it, and yet it cannot be determine who is the user on each block.

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, ‘‘Cipher text-Policy Attribute-Based Encryption,’’ in Proc. IEEE Symp. Security and privacy (S&P’07), 2007, pp. 321-334.

[3] B. Waters, ‘‘Cipher text-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, and A. Sahai, ‘‘Bounded Cipher text 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, and W. 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. Trust Com, 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.

AUTHOR BIOGRAPHY

Pranay Khobragade student of M.E (Final) in Information Technology of R.A.I.T College of Engg, Nerul, New Mumbai.

APPENDIX

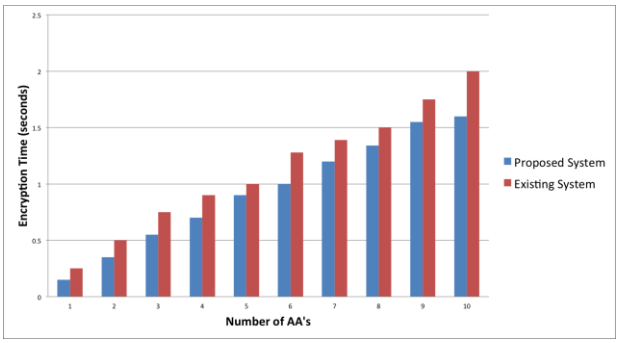

Fig. 1: Encryption Time vs Number of AA’s

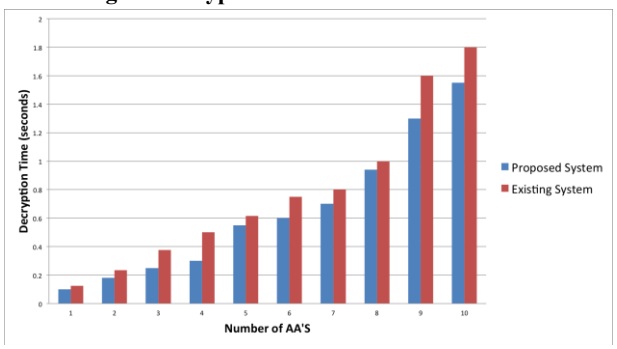

Fig. 2: Decryption Time vs Number of AA’s

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

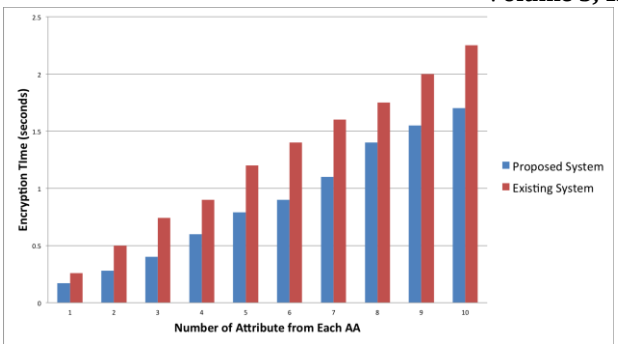

Fig. 3: Encryption Time vs Number of Attributes from each AA

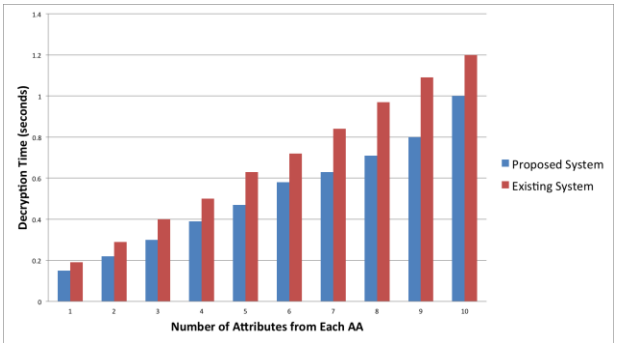

Fig. 4: Decryption Time vs Number of Attributes from each AA

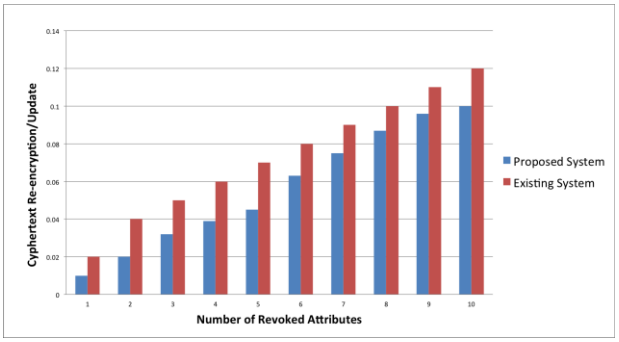

Fig. 5: Cyphertext Update vs Number of Revocation