INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 4, Issue 4 AUG 2015

A Revocable Multi-Authority CP-ABE Scheme for Remote Storage Systems and Online Social Networks

[1] Mr. N NAVEEN KUMAR, [2] MUMMADI RAMA KRISHNA

[1] Assistant Professor, Department of CSE, School of Information Technology, Jawaharlal Nehru Technological University , Kukatpally,Hyderabad, Telangana, India.

[2]M.Tech Student, Department of SE, School of Information Technology, Jawaharlal Nehru Technological University , Kukatpally,Hyderabad, Telangana, India.

ABSTRACT—Data access management is a good thanks to make sure the knowledge security within the cloud. Because of knowledge outsourcing and untrusted cloud servers, the info access management becomes a difficult issue in cloud storage systems. Cipher text-Policy Attribute-based Encryption (CP-ABE) is considered one in all the foremost appropriate technologies for knowledge access management in cloud storage, as a result of it provides data homeowners additional direct management on access policies. However, it's troublesome to directly apply existing CP-ABE schemes to knowledge access management for cloud storage systems due to the attribute revocation downside. during this paper, we tend to style associate communicative, efficient and revocable knowledge access management theme for multi-authority cloud storage systems, wherever there area unit multiple authorities co-exist and every authority is ready to issue attributes severally. Specifically, we tend to propose a revocable multi-authority CP-ABE scheme, and apply it because the underlying techniques to style the info access management theme. Our attribute revocation technique can with efficiency reach each forward security and backward security. The analysis and simulation results show that our projected knowledge access management theme is secure within the random oracle model and is additional economical than previous works.

1. INTRODUCTION

Cloud, that offers services for knowledge house owners to host their storage is a crucial service of cloud computing data within the cloud. This new paradigm of knowledge hosting and data access services introduces a good challenge to knowledge access management. as a result of the cloud server can\'t be absolutely trusted by knowledge house owners, they'll not have confidence servers to do access management. Cipher text-Policy Attribute-based coding (CP-ABE) is considered one amongst the foremost appropriate technologies for knowledge access management in cloud storage systems, because it offers the info owner additional direct management on access policies. In CP-ABE theme, there's associate authority that's responsible for attribute management and key sharing. The authority may be the registration workplace in a very university, the human resource department in a very company, etc. The data owner defines the access policies and encrypts knowledge per the policies. every user are issued a secret key reflecting its attributes. A user will rewrite the info solely when its attributes satisfy the access policies. There square measure 2 forms of CP-ABE systems: single-authority CP-ABE wherever all attributes square measure managed by one authority, and multi-authority CP-ABE wherever attributes square measure from totally {different |completely different} domains and managed by different authorities. Multi-authority CP-ABE is more applicable for knowledge access management of cloud storage systems, as users could hold attributes issued by multiple authorities and knowledge house owners may share the info mistreatment access policy outlined over attributes from totally different authorities.

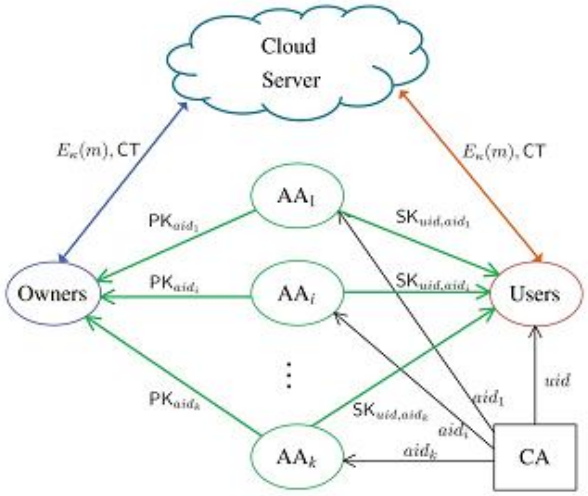
2. RELATED WORK

Cipher text-Policy Attribute-Based cryptography (CP-ABE) may be a promising technique that\'s designed for access management of encrypted information. There area unit 2 varieties of CP-ABE systems: single authority CP-ABE wherever all attributes area unit managed by one authority, and multi-authority CP-ABE wherever attributes area unit from totally different |completely different} domains and managed by different authorities. Multi-authority CP-ABE is more acceptable for the access management of cloud storage systems, as users could hold attributes issued by multiple authorities and the data homeowners could share the information exploitation access policy outlined over attributes from totally different authorities. However, due to the attribute revocation drawback, these multi-authority CP-ABE schemes can\'t be directly applied to information access management for such multi-authority cloud storage systems. To achieve revocation on attribute level, some re-encryption-based attribute revocation schemes are projected by counting on a sure server. we all know that the cloud server can\'t be totally sure by information homeowners, thus ancient attribute revocation ways aren't any longer suitable for cloud storage systems. Ruj, Nayak and Ivan projected a DACC theme where associate attribute revocation technique is given for the Lewko and Waters' decentralized ABE theme. Their attribute revocation technique doesn't need a totally sure server.

3. SYSTEM MODEL AND SECURITY MODEL

A. System Model:

We contemplate an information access system in multi-authority cloud storage, as represented in Figure. There square measure 5 forms of entities within the system: a certificate authority (CA), attribute authorities (AAs), knowledge house owners (owners), the cloud server (server) and knowledge customers (users). The CA could be a international sure certificate authority within the system. It sets up the system and accepts the registration of all the users and AAs within the system. for every legal user within the system, the CA assigns a world distinctive user identity thereto and additionally generates a world public key for this user.



However, the CA isn't concerned in any attribute management and therefore the creation of secret keys that square measure related to attributes. as an example, the CA is the social insurance Administration, associate government agency of the government. Every user are going to be issued a social insurance range (SSN) as its international identity. each AA is associate freelance attribute authority that\'s liable for entitling and revoking user's attributes per their role or identity in its domain. In our theme, each attribute is related to one AA, however every AA will manage associate discretional range of attributes. Each AA has full management over the structure and linguistics of its attributes. Every AA is liable for generating a public attribute key for every attribute it manages and a secret key for every user reflective his/her attributes.

B. Security Model:

In multi-authority cloud storage systems, we tend to create the following assumptions:

- The CA is totally sure within the system. it\'ll not collude with any user, however it ought to be prevented from decrypting any cipher text by itself.
- Each AA is sure however may be corrupted by the adversary.
- The server is curious however honest. it\'s interested in the content of the encrypted knowledge or the received message, however can execute properly the task appointed by every attribute authority.
- Each user is corrupt and should conspire to get

unauthorized access to knowledge.

I. Decisional Q-Parallel Bilinear Diffie-Hellman Exponent Assumption:

We recall the definition of the decisional q-parallel Bilinear Diffie-Hellman Exponent (q-parallel BDHE) problem in [3] as follows. Chooses a group G of prime order p according to the security parameter. Let $a, b_1, \ldots, b_q, s \in Z_p$ be chosen at random and g be a generator of G. If an adversary is given

$$\vec{y} = \Big(g, g^s, g^a, \ldots, g^{(a^q)}, , g^{(a^{q+2})}, \ldots, g^{(a^{2q})} \\ \forall_{1\le j\le q}\ g^{s\cdot b_j},\ g^{a/b_j}, \ldots, g^{(a^q/b_j)}, , g^{(a^{q+2}/b_j)}, \ldots, g^{(a^{2q}/b_j)} \\ \forall_{1\le j,l\le q, l\ne j}\ g^{a\cdot s\cdot b_l/b_j}, \ldots, g^{(a^q\cdot s\cdot b_l/b_j)}\Big),$$

it must be hard to distinguish a valid tuple $e(g,g)^{a^{q+1}s} \in G_T$ from a random element R in G_T.

An algorithm $\mathcal{B}$ that outputs $z \in \{0,1\}$ has advantage ϵ in solving q-parallel BDHE in G if

$$\left|Pr\left[\mathcal{B}(\vec{y}, T = e(g,g)^{a^{q+1}s}) = 0\right] - Pr[\mathcal{B}(\vec{y}, T = R) = 0]\right| \ge \epsilon.$$

4. OUR DATA ACCESS CONTROL SCHEME

We propose the careful construction of our access management theme that consists of 5phases: System data format, Key Generation, encoding, information cryptography and Attribute Revocation. To design the info access management theme for multi-authority cloud storage systems, the most difficult issue is to construct the underlying voidable Multi-authority CP-ABE protocol. In [6], Chase planned a multi-authority CP-ABE protocol, however, it can\'t be directly applied because the underlying techniques owing to two main reasons:

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

2) Revocation Issue: Chase's protocol doesn't support attribute revocation.

We propose a replacement voidable multi-authority CP-ABE protocol supported the single-authority CP-ABE planned by Lewko and Waters in [16]. that\'s we tend to extend it to multi-authority state of affairs and build it voidable. we tend to apply the techniques in Chase's multi-authority CP-ABE protocol [6] to tie along the key keys generated by totally different authorities for constant user and stop the collusion attack. Specifically, we tend to separate the practicality of the authority into a world certificate authority (CA) and multiple attribute authorities (AAs). The CA sets up the system and accepts the registration of users and AAs within the system.7 It assigns a world user identity uid to every user and a world authority identity aid to every attribute authority within the system. as a result of the uid is globally distinctive in the system, secret keys issued by totally different AAs for constant uid are often tied along for coding. Also, as a result of every AA is related to associate degree aid, each attribute is distinguishable even if some AAs might issue constant attribute. To manage the protection issue, rather than mistreatment the system distinctive public key (generated by the distinctive master key) to cipher information, our theme needs all attribute authorities to get their own public keys and uses them to cipher information in conjunction with the world public parameters. This forestalls the certificate authority in our theme from decrypting the cipher texts. To solve the attribute revocation downside, we tend to assign a version range for every attribute. Once associate degree attribute revocation happens, solely those elements associated with the revoked attribute on the QT keys and cipher texts need to be updated. Once associate degree attribute of a user is revoked from its corresponding AA, the AA generates a replacement version key for this revoked attribute associate degreed generates an update key. With the update key, all the users, except the revoked user, who hold the revoked attributes will update its secret key (Backward Security). By mistreatment the update key, the components related to the revoked attribute within the cipher text also can be updated to this version. To improve the potency, we tend to delegate the employment of cipher text update to the server by mistreatment the proxy re-encryption methodology, specified the recently joined user is additionally able to decode the antecedently printed information, which are encrypted with the previous public keys, if they need sufficient attributes (Forward Security). Moreover, by updating the cipher texts, all the users have to be compelled to hold solely the latest secret key, instead of to stay records on all the previous secret keys.

5. SECURITY ANALYSIS

A. Backward Security:

During the key key-update part, the corresponding AA generates associate degree update key for every non-revoked

user. as a result of the update secret\'s associated with the user's international identity uid, the lifted user cannot use update keys of different non-revoked users to update its own secret key, albeit it will compromise some non-revoked users. Moreover, suppose the revoked user will corrupt some other AAs (not the AA adore the revoked attributes), the item HðxaidÞ vxaid aid aid within the secret key will prevent users from change their secret keys with update keys of different users, since aid is merely far-famed by the AAaid and unbroken secret to any or all the users. This guarantees the backward security.

B. Forward Security:

After every attribute cancellation operation, the version of the revoked attribute is updated. Once new users be a part of the system, their secret keys square measure related to attributes with the newest version. Yet, advanced printed cipher texts square measure encrypted beneath attributes with new version. The cipher text update scientific rule in our protocol will update advanced printed cipher texts into the newest attribute variation, specified fresh joined users will still decode advanced printed cipher texts, if their attributes will satisfy access policies related to cipher texts. This guarantees the forward security.

6. IMPLEMENTATION ISSUES

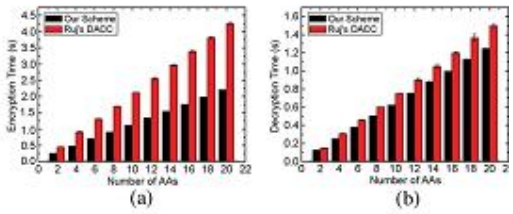
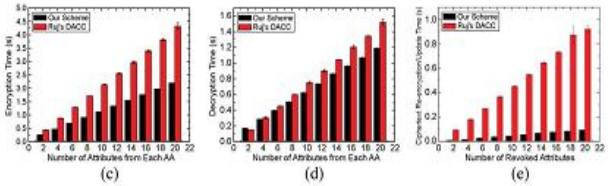


Fig. 3. Comparison of Computation Time. (a) Encryption.

We compare the computation potency of each secret writing and decipherment in 2 criteria: the amount of authorities and also the range of attributes per authority. Figure describes the comparison of secret writing time versus the number of authorities, wherever the concerned range of attributes per authority is ready to be ten. Figure provides the encryption time comparison versus the amount of attributes per authority, wherever the concerned range of authority is ready to be ten. it\'s simple to search out that our theme incurs less secret writing time than DACC theme.



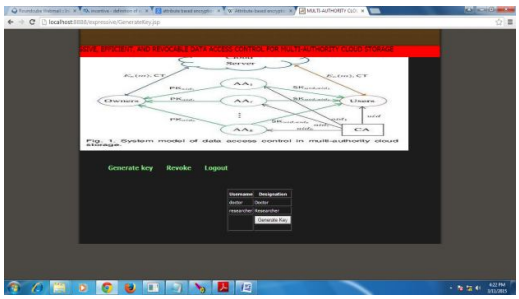
›) Decryption. (c) Encryption. (d) Decryption. (e) Re-encryption.

Figure shows the comparison of cryptography time versus the quantity of authorities, wherever the quantity of attributes the user holds from every authority is ready to be ten. Suppose the user has identical variety of attributes from every authority, Figure describes the cryptography time comparison versus the quantity of attributes the user holds from every rule. In Figure shows, the quantity of authority for the user is fastened to be ten. it\'s not tough to confirm that our theme incurs less cryptography on the user than DACC theme. Figure describes the time of cipher text update/re-encryption versus the quantity of revoked attributes, and our theme is added efficient than. The cipher text update/re-encryption adds the most computation overhead of the attribute revocation. In our forum version, once crony attribute is revocate from its corresponding rule AAaid0, all the cipher texts that area entity related to any attributes from AAaid0 ought to be updated. during this paper, yet, the attribute revocation technique solely needs the update of cipher texts that area unit related to the revoked attribute.

7. EXPERIMENTS

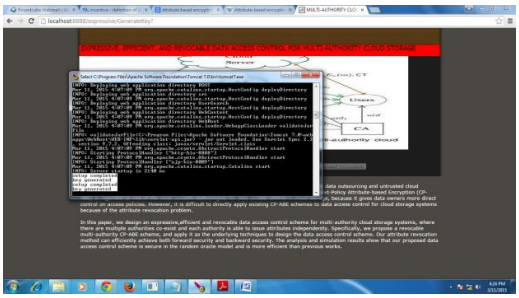
7.1 Experimental Results:

The storage overhead on every user in our theme comes from the key keys issued by all the AAs.

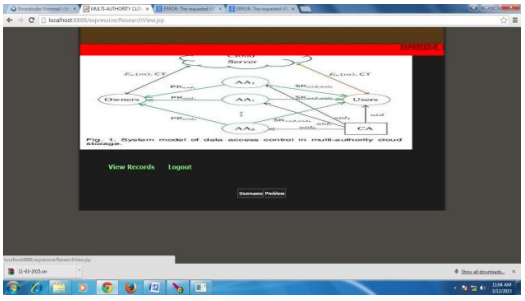


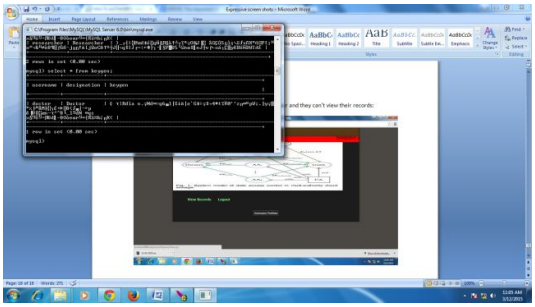
However, within the storage overhead on every user consists of each the key keys issued by all the AAs and

therefore the cipher text elements that related to the revoked attribute x, as a result of once the



cipher text is re-encrypted, a number of its elements associated with the revoked attributes ought to be sent to every non-revoked user UN agency holds the revoked attributes. Within the user must hold multiple secret keys for multiple knowledge home owners, which implies that the storage overhead on every user is additionally linear to the quantity of house holders no within the system.





As we tend to delineate before, there area unit 2 necessities of the attribute revocation: 1) The revoked user (whose attribute is revoked) cannot decode new cipher texts encrypted with new public attribute keys (Backward Security); 2) the recently joined user United Nations agency has ample attributes ought to even be ready to decode the antecedently printed cipher texts, which area unit encrypted with previous public attribute keys (Forward Security).

8. CONCLUSION

In this paper, we tend to projected a revocable multi-authority CPABE theme that may support economical attribute revocation. Then, we tend to created a good ability access management theme for multi-authority cloud storage systems. We bear to additionally fixed that our theme was demonstrable secure within the random oracle model. The revocable multi-authority CP-ABE could be a promising technique, which may be applied in any remote storage systems and on-line social networks etc.

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.Securityand 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, and A. Sahai, ‘‘Bounded Ciphertext Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquiumon 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,’’inProc.AdvancesinCryptology-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.