Decentralized Privacy Preserving Modified MA-CP-ABE-r Scheme Developed for cloud

A.Blessy[1], M.Anandavalli[2]

Abstract-- Cloud computing enables flexible, on-demand and low-cost usage of computing resources. However, those advantages, ironically, are the causes of data loss, privacy, security and revocation issues which emerge because the data owned by different users are stored in some cloud servers instead of under their own control. To deal with these problems, privacy preserving access control scheme in multi authority with efficient encryption & revocation is proposed. In MA-CP-ABE, encryptor intelligently decides who should or should not have access to the data that she encrypts. GID is used where all the keys generated by authorities using PRKG are tied together. Therefore, even if multiple authorities are corrupted, they cannot collect the user's attributes by tracing his GID. . In Modified CP-ABE designed to resist malicious key delegation by issued different secret key to user. An efficient Modified Multi– Authority Ciphertext –Attribute Based Encryption (MA-CP-ABE-r) on Threshold Access Structure with Revocation facility is designed.

Index Terms—Attribute-based Encryption, Multi-authority, Privacy-Preserving Extract Protocol, Access Control.

1. INTRODUCTION

Today for many organizations they need to store their enormous amount of data. Among these, cloud computing is the most cost effective and flexible network storage providers but it has some security issues. Cloud computing provide accuracy, so more data can be centralized into the clouds. Users of this technology are relieved from the data storage and maintenance as they entrust their valuable data in to the clouds. The most important security concerns in cloud are the data security and privacy due to internet based data storage and management. For an organization the extremely important asset is the data. If the data is disclosed the enterprise users will face serious issues from their business competitors and the public. Along with data confidentiality, scalable and flexible access control is also desired by the cloud users. Traditionally, the sensitive data is encrypted and stored on the servers and the decryption keys are disclosed only to the authorized users. It also lacks in flexibility and scalability. This paper focuses on the survey of different encryption schemes and is given in the following sections. Section II presents the literature survey of different encryption schemes and a comparison table and section III concludes with discussions.

- *Blessy is currently working as an Assistant Professor in Computer Science Engineering, Scad Engineering College, Anna University Chennai, India, PH-+918056082493. E-mail: blessy2789@gmail.com*
- *Anandavalli is currently pursuing masters degree in Computer Science Engineering, Scad Engineering College, Anna University Chennai, India,, PH-+917502630474. E-mail: anandi3sri@gmail.com*

2. LITERATURE SURVEY

In cloud computing, there are different existing schemes that provide security, data confidentiality and access control. Users need to share sensitive objects with others based on the recipients' ability to satisfy a policy in distributed systems.One of the encryption schemes is Attribute-Based Encryption (ABE) which is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CP-ABE) scheme

2.1 Identity-Based Encryption

In 1984 Shamir[1] easily constructed an identity-based signature (IBS) scheme using the existing RSA function, he was unable to construct an identity-based encryption (IBE) scheme which became a long-lasting open problem. In 2001, Shamir's[2] open problem was independently solved by Boneh and Franklin by using biometric identity and PKG to generate private key is shown in the Figure 1.This paper take advantage of using Biometric which cannot be imitated. It has the drawback of taking long time to generate private key and use a costly Tamper resistant hardware. In 2005 Sahai and Water[3] proposed a scheme called Fuzzy Identity-Based Encryption (FIBE). In Fuzzy-IBE [1,2], an identity is viewed as a set of descriptive attribute. It allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ώ, if and only if the identities ω and ώ are close to each other as measured by the "set overlap" distance metric. In FIBE, it resists the collusion attack but it generates a key for every attribute so it is complex and time consuming.

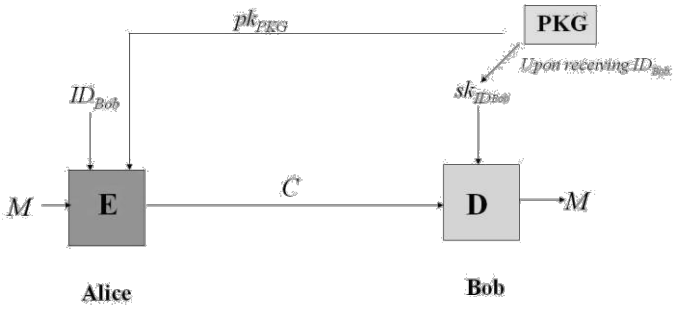

Figure 1: Identity-Based Encryption

Unfortunately, all identity-based cryptographic schemes have inherent weakness, a "key escrow" property. Recall that in IBE and IBS schemes, the PKG issues private keys for user using its master secret key. As a result, the PKG is able to decrypt or sign any messages. In terms of signature, this key escrow property is not desirable at all since the "non-repudiation" property is one of the essential requirement of digital signature schemes. As a countermeasure for the above key escrow problem, Boneh and Franklin [2] suggested that the master secret key of the PKG be distributed using Shamir's secret sharing technique into a number of PKGs.

The user then obtains partial private key shares associated with his identity from the multiple PKGs and reconstructs a whole private key. But this "multiple PKG" method imposes heavy loads on users since they should authenticate themselves to the multiple PKGs, which takes big communication and computational cost. As a result, the use of identity-based cryptography may be limited to the environment where the PKG is unconditionally trusted, for example, inside of a company or a particular organization. The original idea of ABE is to construct a fuzzy (error-tolerant) identity-based encryption (IBE) scheme [1], [2], [15],[16], [17].Therefore Sahai and Waters [3] introduced the concept of Attribute-Based Encryption.

2.2 Key-Policy Attribute Based Encryption

The primary drawback of the Sahai-Waters [3] threshold ABE system is that the threshold semantics are not very expressive and therefore are limiting for designing more general systems. In 2006, Goyal et al[4] introduced the idea of key-policy attribute-based encryption. In their construction a ciphertext is associated with a set of attributes and a user's key can be associated with any monotonic tree access structure. The construction of Goyal et al. can be viewed as an extension of the Sahai-Waters[3] techniques where instead of embedding a Shamir secret sharing scheme[13] in the private key, the authority embeds a more general secret sharing scheme for monotonic access trees.

Goyal et.al. also suggested the possibility of a ciphertext-policy ABE scheme, but did not offer any constructions. This paper take advantage of solving audit log problem. Audit log entries could be annotated with attributes such as, for instance, would only open audit log records whose attributes satisfied the condition that "the user name is Bob", OR (the date is between October 4, 2005 and October 7, 2005 AND the data accessed pertained to naval operations o® the coast of North Korea)". They provide the guarantee that even if multiple rogue analysts collude to try to extract unauthorized information from the audit log, they will fail.

The data is stored on the server in an encrypted form while different users are still allowed to decrypt different pieces of data per the security policy .This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. Their approach has the drawbacks that Encryptor has no access control. In their scheme, the attributes associated with audit log entries would be available to all analysts. This may present a problem in highly secret environments where even attributes themselves would need to be kept hidden from analysts.

Sahai and Waters left an open question that whether it is possible to construct an ABE scheme where the secret keys can come from multiple authorities [3]. In 2007, Chase answered this question affirmatively by proposing a multi-authority KP-ABE scheme[5]. In this scheme, there are multiple authorities, one of which is called central authority. The central authority knows the secret keys of the other authorities. The central authority randomizes the user's secret keys by selecting random polynomials.

In 2007, Ostrovsky [6] construct an Attribute-Based Encryption (ABE) scheme that allows a user's private key to be expressed in terms of *any* access formula over attributes, including Non-Monotone one but it is a complicated one.

In 2009, Melissa Chase and Chow proposed another multi-authority KP-ABE scheme [7] which improved the previous scheme [5] and removed the need of a central authority. Chase and Chow provided an anonymous key issuing protocol for the GID where a 2-party secure computation technique is employed. Use N-2 tolerant. Advantage of their protocol is users cannot trace by GID. In their scheme, the user can *only* obtain secret keys anonymously from N−1 authorities; while he can be traced when he shared his secret keys with others.

The main overhead is on the side of the authority, and even so, it seems a fairly small cost to pay in exchange for guaranteeing security when any N − 2 out of N authorities are corrupted. From [4],[5],[6],in KP-ABE there is no control over who access to the data ,she encrypts .Lack of flexibility and scalability.

2.3 Ciphertext–Policy ABE

In 2007, the first CP-ABE scheme was proposed by Bethencourt, Sahai and Waters [8].They proposed a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. They described an efficient system that was expressive in that it allowed an encryptor to express an access predicate f in terms of any monotonic formula over attributes. Here central authority generates the global key and issues the secret key for the user. Their approach has the drawbacks that it cannot guarantee security of data as server can be compromised.

In 2007, Ling Cheung[9],proposed CP-ABE schemes in which access structures are AND gates on positive and negative attributes.Here they introduced hierarchical attributes which reduced both ciphertext size and encryption/decryption time while maintaining CPA security. Their approach has the drawbacks that it only allows a fixed number of system attributes and is limited to an AND gate (does not enable thresholds). These two limitations actually make it less expressive.

In 2011, Brent Waters[10] proposed a tool to prevent collusion attack,is to randomize each key with an freshly chosen exponent t. During decryption, each share will be multiplied by a factor t in the exponent. Intuitively, this factor "bind" the components of one user's key together so that they cannot be combined with another user's secret key components.In Brent Water [10], they use decryption key in the form of SK = (K = $g^{\alpha}h^{t}$,L=g^{t} ,K χ=$U^{t}\chi$,□χ ∈ S). However, the idea of using as the personalized information for the key owner to achieve traceability is infeasible.

However, in CP-ABE, the decryption privilege of a decryption key is shared by multiple users who possess the corresponding attributes, so that any malicious owner of a decryption key would have the intention or be very willing to leak partial or even his entire decryption privilege for financial interest or any other incentive, especially when there is no risk of getting caught is a issue of *Malicious Key Delegation*.

2.4 Access structure policy

In traditional access control schemes, a central authority can control a user's access to sensitive data. Firstly, since a user's identity needs to be validated by the authority, in a large distributed system, it is a difficult task to manage numerous users identities. Secondly, all users must trust the central authority. If the authority is malicious, he can impersonate any user without being detected. Being different from the traditional access control schemes, attribute-based access control [3], [8], [11], are the schemes that allow users to be validated by the descriptive attributes instead of their unique identities. Furthermore, a user can

Share his data by specifying an access structure so that all the users whose attributes satisfy it can access the data without knowing their identities. Therefore, attribute-based access control schemes are efficient primitives to share data with multiple users without knowing their identities.

Traditional encryption schemes cannot express a complex access policy, and additionally, the sender must know all the public keys of the receivers. Attribute-based encryption (ABE) introduced by Sahai and Waters [3] is a more efficient encryption scheme and it can express a complex access structure. Goyal,Pandey, Sahai and Waters proposed an ABE scheme[4] for fine-grained access policy where any monotonic access structure can be expressed by an access tree.

A monotonic access structure is an access structure where, given a universal set P, if a subset S□of P satisfies the access structure, all subsets S of P which contain S□satisfy the access structure. In an access tree, there is a tree access structure where interior nodes consist of AND and OR gates and the leaves consist of the attributes. Each interior node x of the tree specifies a threshold gate (kx, nx), where nx is the number of the children of x and kx □nx. Thereafter, when kx = nx, the gate is an AND gate. When kx = 1, the gate is an OR gate. If a set of attributes satisfies the tree access structure, the corresponding secret keys can be used to reconstruct the secret embedded in the vertex of the tree.In monotonic access structure, group of user can combined their attributes to satisfies the Universal set .This can compromise the owner privacy.

Subsequently, Ostrovsky, Sahai and Waters proposed an ABE scheme [6] with a non-monotonic access structure where the secret keys are labeled with a set of attributes including not only the positive but also the negative attributes. Their access structure is complicated and less expressive. A (k, n)-threshold access structure is an access structure [3] where, given a universal set P with |P| = n, a subset S of P satisfies the access structure if and only if it contains at least k elements in P. This solves the collusion attack.

2.5 Multi Authority ABE

Multi-authority ABE schemes we are aware of are Chase's original proposal [5] (which has already been discussed in Section B) and the very recent Lin *et al.* extension [12]. Lin, Cao, Liang and Shao proposed a multi-authority ABE scheme without a central authority [12] based on the distributed key generation (DKG) protocol and the joint zero secret sharing (JZSS) protocol [20]. To initialize the system, the multiple authorities must cooperatively execute the DKG protocol and the JZSS protocol twice and k times, respectively, where k is

the degree of the polynomial selected by each authority. Each authority must maintain k + 2 secret keys. This scheme is K resilient, namely the scheme is secure if and only if the number of the colluding users is no more than k, and k must be fixed in the setup stage. Both schemes are KP-ABE and operate in a setting where multiple authorities are responsible for disjoint sets of attributes. The disadvantages of Chase's scheme have already been discussed in Section B.

The scheme of [12], like the scheme we will present here, has the advantage that it does not rely on a central authority. However, their scheme only achieves m-*resilience*, in that security is only guaranteed against a maximum of m colluding users. (In contrast, the results of [5] and our new results consider a much stronger model, which remains secure against any number of colluding users.) And this is not merely an issue of formal security: Lin *et al.* demonstrated a collusion attack of m+1 users[12].

In their scheme m is the number of secret keys that each authority obtains from a distributed key generation protocol. (This also means m must be determined when the system is initialized.) Clearly, for a large scale system, m should set reasonably high in order to guarantee security (a very loose desirable lower bound should be N2, where N is the number of authorities). This imposes burdens on the interactive distributed key generation protocol among all the authorities, and on their secure storage. Finally, O(m) online modular operations are required by each authority to issue secret keys to a user.

In 2008 ,Sasha propose Distributed Attribute based Encryption[18] ,to avoid single trusted server.DABE allows an arbitrary number of authorities to independently maintain attributes and the very recent they extension [19].This paper has Central authority. Drawback of their approach is trust on single server.

Chase and Chow[7] proposed a improving privacy and secure MA-ABE (which has already been discussed in Section B).Here central authority is removed.

2.6 Decentralizing Attribute-Based Encryption

In 2011, Allison lewko [14],proposed a new multi-authority ABE scheme named decentralizing CP-ABE scheme.This scheme improved the previous multi-authority ABE schemes that require collaborations among multiple authorities to conduct the system setup. In this scheme, no cooperation between the multiple authorities is required in the setup stage and the key generation stage, and there is no central authority. Note that the authority in this scheme can join or leave the system freely without reinitializing the system.

2.7. Attribute Revocation

In 2005, attribute revocation is done by extending each user attribute with an expiration date but it requires the users to periodically go to the authority for key reissuing and thus is inefficient. In 2007, it is done by associating the secret key with a expiration date but it places a lower load on the authority and just disable a user secret key at a designated time, but are not able to revoke a user attribute/key on the ad hoc basis. In 2010, it comes with a problem that is the revocation of a single attribute will need update of universal attribute set of the whole system. In 2011, integrating the technique of proxy re-encryption with CP-AB**E** enable the authority to delegate tasks of reissuing secret keys to proxy servers.

3. CONCLUSION

A Modified Multi – Authority Ciphertext-Policy Attribute Based Encryption (MA-CP-ABE-r) on Threshold Access Structure with Revocation facility is proposed and implemented to overcome all those security, privacy, overhead and revocation issues.

REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proceedings: Advances in Cryptology - CRYPTO'84 (G. R. Blakley and D. Chaum, eds.), vol. 196 of Lecture Notes in Computer Science, (Santa Barbara, California, USA), pp. 47–53,Springer, August 19-22 1984.

[2] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings: Advances in Cryptology-CRYPTO'01*(J. Kilian, ed.), vol. 2139 of *Lecture Notes in Computer Science*, (Santa Barbara, California, USA), pp. 213– 229, Springer, August 19-23 2001.

[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings: Advances in Cryptology - EUROCRYPT'05* (R.Cramer,ed.), vol. 3494 of *Lecture Notes in Computer Science*, (Aarhus,Denmark), pp. 457–473, Springer, May 22-26 2005.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Procedings: ACM Conference on Computer and Communications Security-CCS'06 (A. Juels, R. N. Wright, and S. D. C. di Vimercati,eds.), (Alexandria, VA, USA), pp. 89–98, ACM, Ooctober 30-November 3 2006.

[5] M. M. Chase, "Multi-authority attribute based encryption," in *Proceedings:Theory of Cryptography Conference-TCC'07* (S. P. Vadhan,ed.), vol. 4392 of *Lecture Notes in Computer Science*, (Amsterdam,The Netherlands), pp. 515–534, Springer,Feb 21-24 2007.

[6] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute- based encryption with non-monotonic access structures," in Proceedings:ACM Conference on Computer and Communications Security-CCS'07 (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria,Virginia, USA), pp. 195–203, ACM, October 28-31 2007.

[7] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proceedings: ACM Conference on Computer and Communications Security- CCS'09* (E. Al Shaer, S. Jha, and A. D. Keromytis, eds.), (Chicago, Illinois, USA), pp. 121–130, ACM, November 9-13 2009.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings: IEEE Symposium on Security and Privacy (S & P'07)*, (Oakland, California, USA), pp. 321– 34, IEEE, May 20-23 2007.

[9] L. Cheung and C. Newport, "Provably secure ciphertext policy - abe," in Proceedings: ACM Conference on Computer and Communi cations Security - CCS'07 (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria, Virginia, USA), pp. 456–465, ACM, October 28-31 2007.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proceedings:Public Key Cryptography - PKC'11* (D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, eds.), vol. 6571 of *Lecture Notes in Computer Science*, (Taormina, Italy), pp. 53–70, Springer, March 6-9 2011.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,and fine-grained data access control in cloud computing," in *Proceedings: IEEE International Conference on Computer Communications-INFOCOM'10*,

[12] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multiauthority attribute based encryption without a central authority," in *Proceedings: International Conference on Cryptology in India- INDOCRYPT'08* (D. R. Chowdhury, V. Rijmen, and A. Das, eds.) vol. 5365 of *Lecture Notes in Computer Science*, (Kharagpur, India), pp. 426–436, Springer, December 14-17 2008

[13] A. Beimel, Secure Schemes for Secret Sharing and Key Distribution. Phd thesis, Israel Institute of Technology, Technion, Haifa, Israel, June 1996.

[14] A. Lewko and B. Waters, "Decentralizing attribute - based encryption," in Proceedings: Advances in Cryptology-EUROCRYPT'11 (K. G. Paterson, ed.), vol. 6632 of Lecture Notes in Computer Science, (Tallinn, Estonia), pp. 568–588, Springer, May 15-19 2011

[15] C. Gentry, "Practical identity-based encryption without random oracles," in *Proceedings: Advances in Cryptology-EUROCRYPT'06* (S. Vaudenay, ed.), vol. 4004 of *Lecture Notes in Computer Science*, (St. Petersburg, Russia), pp. 445–464, Springer, May 28-June 1 2006.

[16] B. Waters, "Efficient identity-based encryption without random oracles," in *Proceedings: Advances in Cryptology-EUROCRYPT'05* (R. Cramer, ed.), vol. 3494 of *Lecture Notes in Computer Science*, (Aarhus, Denmark), pp. 114–127, Springer, May 22-26 2005.

[17] D. Boneh and X. Boyen, "Efficient selective-id secure identity based encryption without random oracles," in *Proceedings: Advances in Cryptology-EUROCRYP'04* (C. Cachin and J. Camenisch, eds.), vol. 3027 of *Lecture Notes in Computer Science*, (Interlaken, Switzerland), pp. 223–238, Springer, May 2011

[18] S. M¨uller, S. Katzenbeisser, and C. Eckert, "Distributed attributebased encryption," in *Proceedings: Information Security and Cryptology-ICISC'08* (P. J. Lee and J. H. Cheon, eds.), vol. 5461 of *Lecture Notes in Computer Science*, (Seoul, Korea), pp. 20–36, Springer, December 3-5 2008.

[19] S. M¨uller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Bulletin of the Korean Mathematical Society, vol. 46, no. 4, pp. 803–819, 2009.

[20] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust threshold DSS signatures," Information and Computation, vol. 164, no. 1, pp. 54–84, 2001.