Mobile Cloud Security Using Decentralized Attribute Based Access Control

[1] Bhagyashri Gaikwad, [2] Poonam Gupta, [3] Geeta Attkar
[1] Student, [2] Professor, [3] Professor
[1] G.H.Raisoni College of Engineering and Managemet
Pune, India

Abstract: Fine-grained access control may be a demand for data stored in untrusted servers like clouds. Attributable to the big volume of data, decentralized key management schemes are most popular over centralized ones. Usually encryption and decryption are quite expensive and not practical when user's access data from resource constrained devices. We have a tendency to propose a decentralized attribute based mostly encryption (ABE) scheme with quick encryption, outsourced decryption and user revocation. Our scheme is incredibly specific to the context of mobile cloud because the storage of encrypted data and the partial decryption of ciphertext are dependent on the cloud and users with mobile devices will upload data to the cloud or access data from it by incurring little cost for encryption and decryption respectively. The main idea is to divide the encryption into two phases, offline preprocessing phase that is finished once the device is otherwise not in use and an online phase once the data is actually encrypted with the policy. This makes encryption faster and a lot of efficient than existing decentralized ABE schemes. For decryption outsourcing, data users ought to generate a transformed version of the decipherment key permitting an untrusted proxy server to partially decrypt the ciphertext while not gaining any data concerning the plaintext. Data users will then fully decrypt the partially decrypted ciphertext while not performing any costly pairing operations. We also introduce user revocation during this scheme while not incurring too much further price within the online phase. Comparison with other ABE themes shows that our scheme considerably reduces computation times for each data owners and data users and extremely suitable to be used in mobile devices**.**

Index Terms **- - Privacy preserving, Attribute-based Encryption, Decentralized Key Management, Mobile Devices, Computational model, Cloud, Sensitive data, secure self-destructing, fine-grained access control.**

I. INTRODUCTION

Consider the common state of affairs wherever data owners wish to upload their data for long-run storage to untrusted servers such as the cloud. The data could at the start reside in resource forced devices such as mobile phones, wireless sensors or smartcards. The aim is to store the data over a long time and permit multiple users to access the data. Cloud Service providers (CSPs) these days provide such on the face of it unlimited storage facilities and are so rapidly gaining quality among individual data owners yet as enterprises with limited budgets. In spite of the advantages provided by CSPs, they are assumed to be malicious and data owners usually don't trust them with their sensitive data. So, any data keep within the cloud should be encrypted. Moreover, data owners might need to impose access control measures on data in order that only users who have sure credentials will access it. For instance, a hospital might need to upload to the cloud the results of a run recording the response of cancer patients to a replacement drug. This data is sensitive and the hospital might want only the doctor attending a patient or a researcher concerned within the drug discovery to have access to the data. Encryption schemes like attribute-based encryption (ABE) provide great flexibility in terms of access control on encrypted data and are ideal for this scenario. In practice, decentralized or multi-authority ABE schemes are terribly helpful as they are doing not would like any central authority for generation and distribution of coding keys associated with completely different attributes. For instance, the doctor who wants to access a patient's health record for diagnosis could also be provided the relevant key by the hospital however; a medical researcher could also be given access to an equivalent data by a medical analysis organization. User attributes are subject to periodic changes due to change in the work environment, location etc. Thus, a user who was antecedently granted access to data could now not qualify for the access. Unless antecedently allotted keys are updated and therefore the user is revoked, the user could still access the data in spite of a change in his attributes. Therefore, user revocation may be a necessary and helpful property for ABE schemes.

The use of those sophisticated encryption schemes pose one severe problem. The encryption, revocation key generation and decryption phases are typically very costly, involving many bilinear pairing operations, and resource forced devices are not appropriate for performing such operations fast enough. To address this downside, we have a tendency to propose a decentralized attribute based encryption (ABE) scheme with quick encryption, outsourced decryption and user revocation. Our scheme is incredibly specific to the context of mobile cloud because the storage of encrypted knowledge and the partial decryption of ciphertext are addicted to the cloud and users with mobile devices will upload data to the cloud or access data from it by incurring very little price for encryption and decryption respectively. As an answer to the costly encryption problem, we have a tendency to divide the encryption phase into an offline part and an online phase, such that, most of the costly operations are performed offline once the user doesn't immediately expect the encryption to be completed, the device is charging or otherwise not in use. The online phase has very little computations in order that users will get on with their work while not the device's performance being affected in any respect. Data users are relieved from performing costly decryption operations by outsourcing such operations to a proxy server. The proxy server, employing a transformed decryption key, partially decrypts the ciphertext. However, the partial decryption method does not reveal any information to the malicious proxy server. Then, the data user must perform only some easy operations to derive the final plaintext from the partially decrypted ciphertext. Similarly, revocation keys is generated offline, with a few computations within the on-line phase for key transformation before they are given to the proxy server.

Attribute-based encryption (ABE), introduced by Sahai and Waters, enables senders to encrypt a message such that only receivers that satisfy certain criteria can decrypt.

In most ABE schemes, one central authority capable of verifying all the attributes/credentials issued for every user issues decryption keys. In reality, mostly, completely different authorities monitor completely different attributes of a person. As an example, a research organization will certify that a person is associate affiliated researcher but only the hospital will certify that a person could be a doctor associated with it. Chase initial provided a multi-authority ABE scheme. In their basic scheme, every authority controls a collection of attributes and decryption is possible only by a user who possesses at least a pre-specified number of attributes from every authority. Later, Chase and Chow improved Chase's schemes in terms of security of encryption and user privacy. These schemes were proved selectively secure. Lewko and Waters' theme is fully secure and uses the dual encryption method of security proof. Unlike the threshold schemes of Chase and Chow, during this theme, the user will code exploitation any Boolean formula over attributes issued by any chosen set of authorities. Both Chase and Lewko and Waters use the idea of global identifier to replace the central authority. The global identifier links secret writing keys issued to a user by completely different authorities. However, as pointed out in, its use conjointly leads toloss of user privacy, as colluding authorities will simply generate a user's profile by noting attributes issued against his international identity. A number of schemes have since been proposed on privacy preserving multi-authority ABE. Li et al. showcase the use of multi-authority ABE for encrypting personal health records (PHR) to be keep in semitrusted cloud servers. Their theme allows dynamic modification of access policies or file attributes, economical on-demand user/attribute revocation and break-glass access throughout emergencies. Ruj et al. propose an ABE-based suburbanized access control (DACC) for data keep in the cloud wherever multiple key distribution centers (KDC) distribute secret keys to the users as opposed to data owners themselves giving out secret keys corresponding to completely different attributes. also within the context of multiauthority cloud, the efficient easy-ACCESS scheme provides the advantages of shorter decryption keys, lower computation cost through delegation of decryption to a decryption service provider and obvious security (under selective security model).

II. PRELIMINARIES

A. Bilinear Mapping

Let G1, G2 and GT be cyclic groups of the same prime order p. Then a bilinear map from G1 ×G2 is a function e : G1 × G2 → GT such that ∀P ∈ G1,Q ∈ G2,a,b ∈Zp, e(Pa,Qb) = e(P,Q)ab. The map is called an admissible bilinear mapping if e(g1,g2) generates GT, where g1 and g2 are generators of G1 and G2 respectively, and e is efficiently computable. The map we consider here is symmetric, with e : G×G → GT, where G and GT are cyclic groups of the same prime order p.

B. Access Structures

Definition 1. Access Structure [4]. "Let {P1,P2,...,Pn} be a set of parties. A collection A ⊆ 2{P1,P2,...,Pn} is monotone if ∀B,C: if B ∈ A and B ⊆ C implies C ∈ A. An access structure is a monotone collection A of non-empty subsets of {P1,P2,...,Pn} (that is, A⊆ 2{P1,P2,...,Pn}\φ). The sets in A are called authorized sets, and the sets not in A are called the unauthorized sets."

C. Linear Secret Sharing Schemes

Our construction uses linear secret sharing scheme.

Definition 2. Linear Secret Sharing Schemes (LSSS) (adapted from [1], [2]). "A secret sharing scheme π over a set of parties P is called linear over Zp if 1) the shares of the parties form a vector over Zp. 2) there exists a matrix A with l rows and n columns called the share-generating matrix for π. There exists a function ρ which maps each row of the matrix to an associated party (i.e., for i = 1,...,l, ρ(i) is the party associated with row i). When we consider the column vector v = (s,r2,...,rn), where s ∈ Zp is the secret to be shared, and r2,...,rn ∈ Zp are randomly chosen, then Av is the vector of l shares of the secret s according to π. The share (Av)i belongs to party ρ (i)".

III. SYSTEM DESCRIPTION

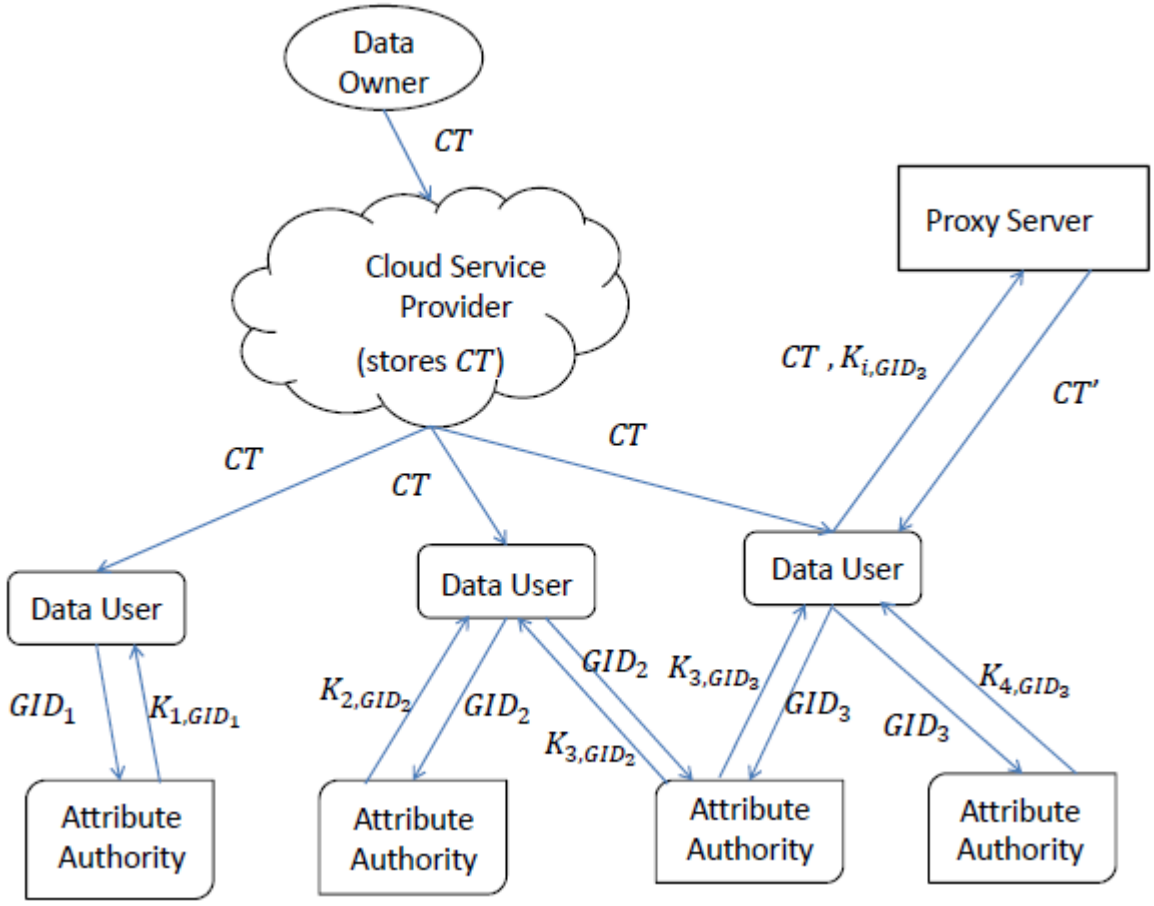
Our system has the subsequent entities as below.

a. The Data Owner (DO) is an entity that owns data and uploads it to cloud storage when encrypting it. Data owners do not want the CSP to find out something regarding their data and permits access to the data users whose attributes satisfy a given policy. Data owners might have to use resource-constrained devices (e.g., mobile phones, sensors, smartcards) to perform encryption on their data. All devices employed by DO are assumed trusted.

b. The Cloud Service provider (CSP) provides storage facilities for data happiness to data owners. The CSP is honest-but-curious. The CSP will attempt to determine information from the data stored in it however doesn't modified or deletes data.

c. Data Users (DU) want to access data outsourced by the DO to the CSP. They can access this data if they satisfy a given policy. They must collect decryption keys corresponding to their attributes from Attribute Authorities. Data users are untrusted and will attempt to access data to that they are not authorized. They will additionally collude. Every data user has a global identifier (GID), such as Social Security number or passport number that they need to submit to the attribute authorities to obtain the decryption keys. All devices used by DU for decryption are assumed trusty. There are more than one Attribute Authorities (AA) dominant completely different user attributes and generate the general public key and decryption key corresponding to these attributes. Data users acquire their attributes and corresponding decryption keys from relevant attribute authorities on submitting their global identifiers (GID). For example, the Motor Vehicle's department may be an AA that certifies that an explicit data user will drive. Similarly, a university could certify a data user to be a student of that university. Some AAs could also be corrupted. On receiving a transformed decryption key from the data user, the proxy server (PS) performs partial decryption of the encrypted cipher text for the data user. This helps in decreasing the decryption load on data user's devices while not the proxy server knowing something about the encrypted data. The proxy server could try to learn as much data as potential from the ciphertext but doesn't affect the correctness of the transformation. It may be either a district of the cloud server or a separate entity.

d. The System Manager (SM) defines the system parameters. We tend to assume that there exists authentication channels before uploading the data.



IV. FRAMEWORK

Our multi-authority ciphertext-policy attribute based encryption scheme with online/offline encryption and outsourced decryption(OO-MA-DO-CPABE scheme) consists of the following algorithms:

1) Global Setup(λ) → GP. The Global Setup algorithms takes as input the security parameter λ and outputs the global parameters GP of the system.

2) Authority Setup(GP) → PK,MSK. Each authority runs the Authority Setup algorithm that takes as input the global parameters GP and outputs the public key PK and the private key SK corresponsing to each attribute controlled by the authority.

3) Online.Encrypt(GP,IC,IS,PK,(A, ρ),m) → CT. The Online.Encrypt algorithm takes as input the message m, the access matrix (A, ρ), the intermediate ciphertext IC, the intermediate state IS, the global parameters GP and the relevant public keys PK from appropriate authorities and produces the ciphertext CT.

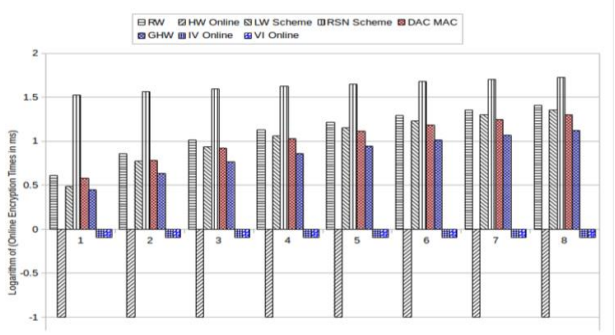
4) KeyGen(GID,i,MSK,GP) → Ki,GID. The KeyGen algorithm takes as input the global parameters GP, an attribute i belonging to an authority, the secret key SK for this authority and the user's global identity GID. It outputs the key Ki,GID for the attribute-identity pair.

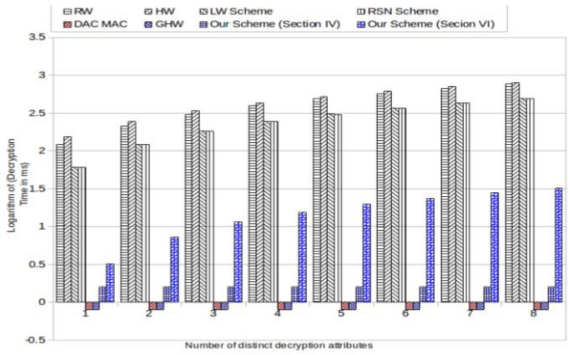
5) KeyTransform(Ki,GID) → Ti,GID. The data user's device uses a random number in Zp to transform the key Ki,GID given to the user by an attribute authority into a new key Ti,GID which is sent to a proxy server to enable partial decryption.

6) PartialDecrypt(CT,Ti,GID,GP) → CT0. The PartialDecrypt algorithm run by the proxy takes as input the global parameters GP, the ciphertext CT and a collection of keys corresponding to the attribute-identity pairs all with the fixed identity GID. If the collection of attributes satisfies the access matrix associated with the ciphertext, then it outputs a partially decrypted message CT0 which is given to the user for full decryption; else, decryption fails.

7) FullDecrypt(CT0) → m. The FullDecrypt algorithm run by the data user's device takes as input the partially decrypted message CT0 and computes the fully decrypted message m...

V. PERFORMANCE ANALYSIS





VI. CONCLUSION

We propose associate ABE scheme appropriate for mobile clouds. It combines the helpful properties of decentralization, quick encoding, outsourced decryption and user revocation. All significant computations associated with encoding are performed throughout the offline section creating the entire encryption phase quicker and additional economical than existing decentralized ABE schemes. Associate un trusty proxy server partly decrypts the cipher-text while not gaining any data concerning the plaintext. Knowledge users will then absolutely decrypt the partly decrypted cipher text while not performing any costly pairing operations. Our scheme supports user revocation while not acquisition a lot of extra value within the on-line section. Overall, not like different existing works, our theme hits a decent balance between encoding and decipherment performance, whereas supporting extra helpful properties like decentralization and user revocation.

REFERENCES

[1] A. Beimel. Secure schemes for secret sharing and key distribution. Ph.D. Thesis, Israel Institute of Technolgy, Technion, Haifa, Israel, 1996.

[2] M. Green, S. Hohenberger, and B. Waters. Outsourcing the decryption of ABE ciphertexts. In 20th USENIX Security Symposium, San Francisco, CA, USA, August 8-12, 2011, Proceedings, 2011.

[3] N. Balani and S. Ruj. Temporal access control with user revocation for cloud data. In 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, Beijing, China, September 24-26, 2014, pages 336–343, 2014.

[4] A. Beimel. Secure schemes for secret sharing and key distribution. Ph.D. Thesis, Israel Institute of Technolgy, Technion, Haifa, Israel, 1996.

[5] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA, pages 321–334. IEEE Computer Society, 2007.

[6] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In Proceedings of the 15th ACM conference on Computer and communications security, pages 417–426. ACM, 2008.

[7] R. Canetti, H. Krawczyk, and J. B. Nielsen. Relaxing chosen-ciphertext security. InD.Boneh,editor,AdvancesinCryptology-CRYPTO2003,23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, volume 2729 of Lecture Notes in Computer Science, pages 565–582. Springer, 2003.