Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.647 – 656

RESEARCH ARTICLE

IMPROVING DATA SECURITY IN CRYPTO-BASED DATA SHARING WITH THIRD PARTY AUDITING

D.Sangeetha[#1], L.Gomathi[*2]

[1]Research Scholar, Muthayammal College of Arts and Science

[2]Assitant Professor, Muthayammal College of Arts and Science

Abstract: ***The encryption standard provides key assumption to the analytical with the recent adoption and diffusion of the data sharing paradigm in distributed systems such as online social escrow problem. The key generation center could decrypt any messages addressed to specific users networks or cloud computing, there have been increasing demands and concerns for distributed data security. One of the most challenging issues in data sharing systems is the enforcement of access policies and the support of policies updates. Cipher text policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. However, the advantage comes with a major drawback which is known as a key by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users. In addition, applying CP-ABE in the data sharing system introduces another challenge with regard to the user revocation since the access policies are defined only over the attribute universe. Therefore, in this study, we propose a novel KP-ABE scheme for a data sharing system by exploiting the characteristic of the system architecture, To propose a RBAC and HIBR Key policy which is constructed using the secure two-party computation between the key generation center and the data-storing center, and also fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE. Also third party Auditing (TPA) organize the security. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.***

Key Words: CP-ABE, KP-ABE, TPA

I. INTRODUCTION

The network and computing technology enables many people to easily share their data with others were using online external storages. People can share their lives with friends by uploading their private photos or messages into the online for ease of sharing with their primary doctors or for cost saving. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Attribute-based encryption (abe) is a promising cryptographic approach that achieves a fine-grained data access control it provides a way of defining access policies based on different attributes of the requester, environment, or the data object. Especially, cipher text policy attribute-based encryption (cp-abe) enables an ncryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access, which is the traditional access control approach of such as the reference monitor. Nevertheless, applying cp-abe in the data sharing system has several challenges. in cp-abe, the key generation center (kgc) generates private keys of users by applying the kgc's master secret keys to users' associated set of attributes. Thus, the major benefit of this approach is to largely reduce the need for processing and storing public key certificates under traditional public key infrastructure (pki). However, the advantage of the cp-abe comes with a major drawback which is known as a key escrow problem. The kgc can decrypt every cipher text addressed to specific users by generating their attribute keys.

II. RELATED WORK

Key-policy attribute-based encryption

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Key-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC) in authentication. In addition, we provide an implementation of our system and give performance measurements.

Outsourcing data policy access control in cloud authentication

Furthermore, in cloud computing, data owners may share their outsourced data with a number of users, who might want to only retrieve the data files they are interested in. One of the most

popular ways to do so is through keyword-based retrieval. Keyword-based retrieval is a typical data service and widely applied in plaintext scenarios, in which users retrieve relevant files in a file set based on keywords.

However, it turns out to be a difficult task in cipher text scenario due to limited operations on encrypted data. Besides, to improve feasibility and save on the expense in the cloud paradigm, it is preferred to get the retrieval result with the most relevant files that match users' interest instead of all the files, which indicates that the files should be ranked in the order of relevance by users' interest and only the files with the highest relevances are sent back to users.

III.LITREATURE SURVEY

Cipher text-Policy Attribute-Based Encryption

Authors: John Bethencourt, Brent Waters

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

Fuzzy Identity-Based Encryption

Cipher text-Policy Attribute-Based Encryption: An Expressive, Ecient, And Provably Secure Realization

Authors: Brent Waters, University Of Texas at Austin

We present a new methodology for realizing Cipher text-Policy Attribute Encryption (CP-ABE) under concrete and non interactive cryptographic assumptions in the standard model. Our solutions allow any encrypted to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model. We present three constructions within our framework. Our _rst system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Di_e-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our next two constructions provide performance trade to achieve provable security respectively under the (weaker) decisional Bilinear-Die-Hellman Exponent and decisional Bilinear Di_e- Hellman assumptions. Key-Policy ABE, attributes are used to annotate the cipher texts and formulas over

these attributes are ascribed to users' secret keys. The second type, Cipher text-Policy ABE, is complementary in that attributes are used to describe the user's credentials and the formulas over these credentials are attached to the cipher text by the encrypting party. In addition provided a construction for Key-Policy ABE that was very expressive in that it allowed the policies (attached to keys) to be expressed by any monotonic formula over encrypted data. The system was proved selectively secure under the Bilinear Die-Hellman assumption. However, they left creating expressive Cipher text Policy ABE schemes as an open problem.

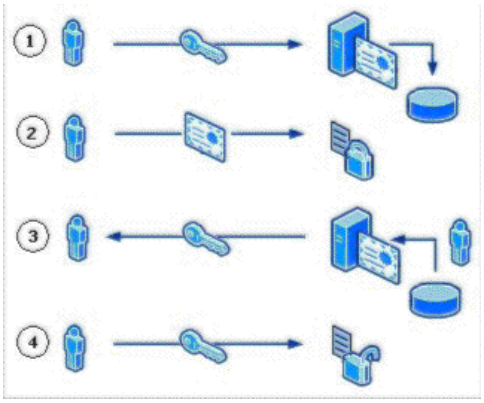
Revocation Systems With Very Small Private Keys

In this work, we design a method for creating public key broadcast encryption systems. Our main technical innovation is based on a new \two equation" technique for revoking users. This technique results in two key contributions: First, our new scheme has cipher text size overhead O(r), where r is the number of revoked users, and the size of public and private keys is only a constant number of group elements from an elliptic-curve group of prime order.. We give two versions of our scheme: a simpler version which we prove to be selectively secure in the standard model under a new, but non-interactive assumption, and another version that employs the new dual system encryption technique of Waters to obtain adaptive security under the d-BDH and decisional Linear assumptions. Second, we show that our techniques can be used to realize Attribute-Based Encryption (ABE) systems with non-monotonic access formulas, where our key storage is significantly more efficient than previous solutions. This result is also proven selectively secure in the standard model under our new non-interactive assumption. We believe that our new technique will be of use elsewhere as well. We create public key revocation encryption systems with small cryptographic private and public keys. Our systems have two important features relating respectively to public and private key size. First, public keys in our two systems are short (just 5 group elements and 12 group elements respectively) and enable a user to create a cipher text that revokes an unbounded number of users. This is in contrast to other systems where the public parameters bound the number of users in the system and must be updated to allow more users. Second, the cryptographic key material that must be stored securely on the receiving devices is small. Keeping the size of private key storage as low as possible is important as cryptographic keys will often be stored in tamper-resistant memory, which is more costly. This can be especially critical in small devices such as sensor nodes, where maintaining low device cost is particularly crucial. Device keys in our systems are only a small constant number of group elements (in fact, just 3 group elements and 5 group elements respectively) from an elliptic-curve group of prime order. Furthermore, our schemes are public-key stateless broadcast encryption schemes1, and we work with stateless receivers. We achieve this small device key size without compromising on other critical parameters such as cipher text length {our cipher texts will consist of just O(r) group elements, where r is the number of revoked users. This is the same behavior as the previously best-known schemes for revocation. We also do not compromise on security: we obtain adaptive security in the standard model under the well-established d-BDH and decisional linear assumptions.

IV. STUDY OF KEY POLICY TECHNIQUES

Cryptographic key assumption:

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.



Attribute key assumption:

Group key distribution schemes has recently received a lot of attention from the researchers, as a method enabling large and dynamic groups of users to establish group keys over unreliable network for secure multicast communication. In such schemes, time is divided into epochs called sessions. At the beginning of each session, a Group Manager transmits some broadcast message, in order to provide a common key to each member of the group. Every user, belonging to the group, computes the group key using the message and some private information. The main property of the scheme is that, if some broadcast message gets lost, then users are still capable of recovering the group key for that session by using the message they received at the beginning of a previous session and the message they will receive at the beginning of a subsequent one, without requesting additional transmission from the Group Manager. This approach decreases the workload on the Group Manager and reduces network traffic as well as the risk of user exposure through traffic analysis.

Key distribution:

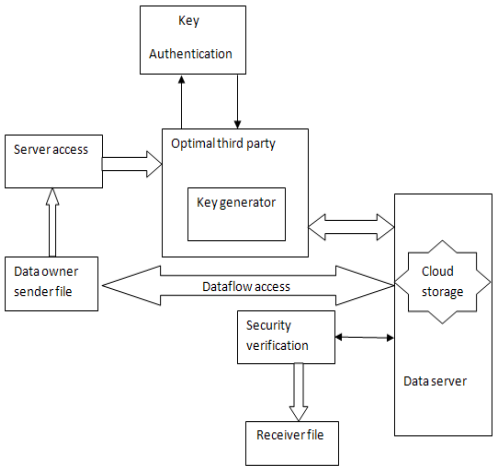
Common group key is frequently updated to ensure secure multicast communication. Group lifetime is dived into epochs called sessions; single key instance is valid only throughout one session. Group membership can change between consecutive sessions. At the beginning of

session j, GM distributes a new session key to nodes. Session duration is determined by the GM. It can vary over time, depending on security policy, group membership changes and nodes' behavior.

Session key changes have to be performed, with some predefined minimum frequency to protect the system from cryptanalysis attacks. Moreover, to effectively remove a node from multicast group, who is willing to leave, or is forced to leave, a new session must begin and nodes from shall start protecting group communication using a new , which is not accessible to Thus, the choice of session length is a tradeoff between key distribution cost in terms of communication and computational overhead, and the required security level.

Key issuing secured access:

Escrow-Free Key Issuing Protocol for CP-ABE and the TPA and the data-storing center are involved in the user key issuing protocol. In the protocol, a user is required to contact the two parties before getting a set of keys. The TPA is responsible for authenticating a user and issuing attribute keys to him if the user is entitled to the attributes. The secret key is generated through the secure protocol between the TPA and the data-storing center. They engage in the arithmetic secure protocol with master secret keys of their own, and issue independent key components to a user. Then, the user is able to generate the whole secret keys with the key components separately received from the two authorities. The secure protocol deters them from knowing each other's master secrets so that none of them can generate the whole secret keys of a user alone.



To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group, since otherwise revocation cannot take effect after all. This setting where the data-storing center knows the revocation list does not violate the security requirements, because it is only allowed to re encrypt the cipher texts and can by no means obtain any information about the attribute keys of users. Since the proposed scheme is built on, we recapitulate some definitions in to describe our construction in this section, such as access tree, encrypt, and decrypt algorithm definitions.

Security analysis

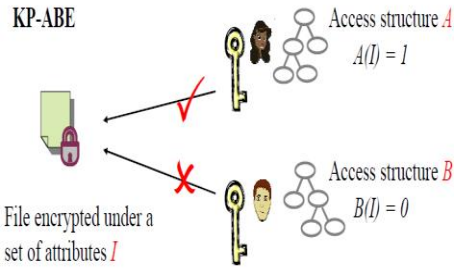
Security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely digital signature, message authentication code, and encryption,

in our system. The fraud can be repudiated only if the client can provide a different representation he knows of from the trusted authority (TA).

The enforcement of access policies and the support of policy updates are important challenging issues in the data sharing systems. In this study, we proposed a attribute based data sharing scheme to enforce a fine-grained data access control by exploiting the characteristic of the data sharing system. The proposed scheme features a key issuing mechanism that removes key escrow during the key generation. The user secret keys are generated through a secure two-party computation such that any curious key generation center or data-storing center cannot derive the private keys individually. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials. The proposed scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the cipher text policy attribute-based encryption. Therefore, the proposed scheme achieves more secure and fine-grained data access control in the data sharing system.

V. RESULTS AND DISCUSSION

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites on the cloud storage. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of re-encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE).



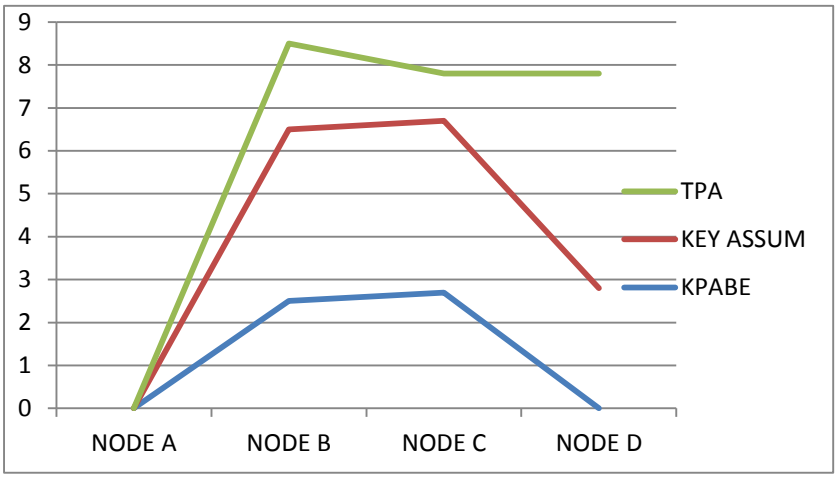
In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast re-encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Re-Encryption (HIBR). The proposed scheme is then built on this new CP-ABE variation by further integrating it into the proxy with KP-ABE reencryption for the user revocation. To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group which is related to TPA permission generated code, since otherwise revocation cannot take effect after all. This setting where the data-storing center knows the revocation list does not violate the security requirements, because it is only allowed to re encrypt the cipher texts with authentication and can by no means obtain any information about the attribute keys of users only accessed by valid users.

Advantage of Proposed System

The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data-storing center, and

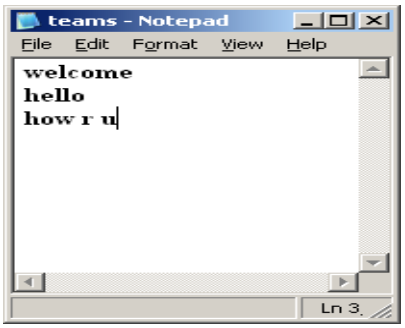
Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.

Comparison Chart



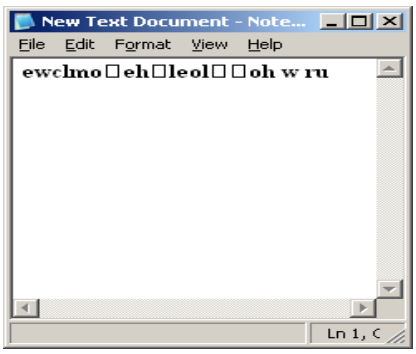
The client will generate keying materials via Keygen and FilePreProc, then upload the data to CSS. Different from previous schemes, the client will store a key instead of a network client server as metadata. Moreover, the client will authorize the TPA by sharing a value sig_{AUTH}. Verifiable Data Updating: the CSS performs the client's fine-grained update requests via Perform Update, then the client runs Verify Update to check whether CSS has performed the updates on both the data blocks and their corresponding authenticators (used for auditing) honestly. Challenge, Proof Generation and Verification: Describes how the integrity of the data stored on CSS is verified by TPA via GenChallenge, GenProof and Verify.

INPUT FILE
Encryption



OUTPUT FILE

Decryption



VI. CONCLUSION

In this study, we projected an attribute based data sharing scheme to enforce a KP-ABE standard data access control by exploiting the characteristic of the data sharing system. Thiskey policy algorithm provides a key issuing mechanism that removes key escrow during the key generation. The user secret keys are generated through a secure two-party computation such that any curious key generation center or data-storing center cannot derive the private keys individually. Thus, the algorithm enhances data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials with security. Its demonstrated that the resulting scheme is efficient and scalable to securely manage user data in the data sharing system and future to verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop:Routing for vehicle-based disruption tolerant networks," in Proc .IEEE INFOCOM, 2006, pp. 1–11.
[2] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp.1–6.
[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37–48.
[4] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policyattribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[5] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. Conf. File Storage Technol., 2003, pp. 29–42.
[7] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.
[8] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

Author's Details:

L.Gomathi received her BCA degree from Amman Arts & Science College, Chitode and MCA degree from Bharathidasan University, Trichy. She has completed his M.Phil at Periyar University, Salem. She is having 8 years of experience in collegiate teaching and She is the Assistant Professor of computer science and applications in Muthayammal college of Arts and Science, Rasipuram affiliated by Periyar University. Her main research interests include data mining, Network security.

D.Sangeetha received her B.Sc, degree in Muthayammal College of Arts and Science, Rasipuram, Periyar University, Salem (2007 - 2010) [TamilNadu (India). Then, did MCA degree in Muthayammal College of Arts and Science, Rasipuram, Periyar University, (2010-2012). She is the M.Phil Research Scholar of Muthayammal College of Arts and Science, Rasipuram. Periyar University, Salem. Her Area of interest is Networking.

