ISSN:0975-9646

Data Retrieval with Secure CP-ABE: A Review

Sharayu N. Bonde , Rahul Gaikwad

Computer Engineering Department
GF's Godavari College of Engineering, Jalgaon
Maharashtra, India

Abstract: Todays most popular used communication strategy is using wireless technology. Nodes in network communicate with each other accessing their confidential information using external storage nodes. Many applications require increased protection of confidential data including access control methods that are cryptographically enforced. The problem of cryptographic secure data retrieval from external storage is resolved by Ciphertext-policy attribute-based encryption (CP- ABE) methods. There are approaches using CP-ABE for wireless distributed network which are managing their attributes by multiple key authorities where data is stored centrally on server. The following paper is describing a methods demonstrating how to apply those method securely and efficiently for managing confidential information distributed over storage network

Keywords: DTN, Cryptography, storage network, ABE, CP-ABE.

1. INTRODUCTION

Cloud Storage is a model that treats the resources on the Internet as a unified entity, a cloud. Users use a service without being concerned about how computation is done and storage is managed. This method used to focus on designing a cloud storage system for robustness, privacy, and functionality. A cloud storage system is considered as a large scale distributed storage system that consists of many self-governing storage servers. Data robustness is a major obligation for storage systems. There are many proposals of storing data over storage servers. One way to present data robustness is to duplicate a message such that each storage server stores a copy of the message. It is robust because the message can be retrieved as long as one storage server survives.

Wireless DTN technologies are becoming popular solutions allowing nodes to communicate with each other in extreme networking areas [1],[2]. Mostly, when there is no end-to-end connection between a source and a destination hosts , the messages from the source node have to wait in the intermediate nodes for a substantial amount of time till the connection gets established.

Some technologies are proposed intermediate nodes in network [4-5] where data gets replicated in such a way that only authorized user nodes can access the necessary information quickly and efficiently. For many areas requiring increased protection on accessing confidential information including methods that are enforcing cryptography solutions.

Symmetric Key Cryptography (SKC) was invented to provide cryptographic basic solution where single key is used by source and destination hosts. The Public Key Cryptography (PKC) was proposed principally to overcome the limitation in ensuring secure group communications in the SKC based cryptosystems by using separate key as private key for user and public key for group authentication. However, the PKC based systems involve costly and complex public key authentication framework known as the public key infrastructure. Identity based Encryption (IBE) was proposed by Shamir[15] reducing complexity associated with the pure PKC based systems. The user chooses his name and network address as his public key instead of generating a random pair of public/secret keys and publishing one of these keys as in PKC based system. For multicasting a message to the users these two cryptosystems are complemented with fuzzy IBE where only the recipient whose attributes match defined on a set overlap distance metric can decrypt a message encrypted with the same identity.

The attribute-based encryption (ABE) concept [8],[9] is a method providing approach that fulfills the requirements for retrieving data securely in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and used attributes among private keys and cipher texts. ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). KPABE establishes a scheme in which attributes are attached to the ciphertext and a monotonic formula is attached with the secret key of user [5] where the encryptor gets only label a ciphertext with a set of attributes. The key authority chooses a policy for every other user determining which ciphertexts user can decrypt. He also issues the key to each user by attaching the policy into the user's key. The key of user can decrypt only kind of cipphertext which is determined by access structure associated with the secrete key of user. CP-ABE provides more power to the sender as compared to KP-ABE by using the approach of threshold secret sharing [6]. In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor where a key is created with respect to an attributes set for a user. CP-ABE is more appropriate to DTNs because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure by corresponding public keys or attributes . Thus, different users are allowed to decrypt different pieces of data per the security policy.

Now, in the real world, the attributes values of specific entity undergo periodic updates. For example, if we consider Harshal as a student at Knowledge city who stays at Address1. Then, the access restricts the identity of Harshal has the attributes {Name="Harshal"; Residence="Address1"; Institute="Knowledge city"}. Suppose, when Harshal is moved from Address1 to Address2, the respective attribute must also update. The basic CP-ABE and its variants enlisted support only the static attributes.

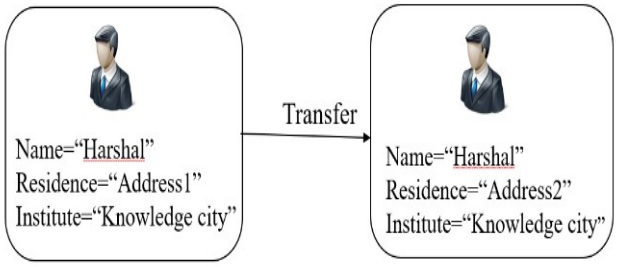

Fig. 1 Dynamic attribute Update

2. RELATED WORK

We briefly review CP-ABE method, storage systems, and integrity check functionality.

2.1 CP-ABE Method:

Definition 1 (Access Structure) :
Let {P1,P2,...,Pn} be a set of parties. The collection $A \subseteq 2\{P1,P2,...,Pn\}$ is monotone if $\forall B,C$: if $B \in A$ and $B \subseteq C$ then $C \in A$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of {P1,P2,...,Pn}, i.e., $A \subseteq 2\{P1,P2,...,Pn\}\backslash\{\emptyset\}$. The sets in A are called the authorized sets, and the sets not in A are called the unauthorized sets.

Attributes takes the role of parties. Hence, the authorized sets of attributes will be contained in the access structure A. However, we can realize general access structures using our techniques by having the no. of an attribute as a separate attribute altogether. Thus, the number of attributes in the system will be doubled.

Access Tree

1) Description: Let T be tree representing an access structure. Each non leaf node of the tree represents a threshold gate. If num_x is the number of children of a node x and k_x is its threshold value, then each leaf node of the tree is described by an attribute and a threshold value $0 \leq k_x \leq num_x$. It denotes the attribute associated with the leaf node x in the tree, $p(x)$ represents the parent of the node x in the tree. The children of every node are numbered from 1 to num. Number associated with the node returned by the function $index(x)$ returns such a number associated with the node x. The index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner.

2) Satisfying an Access Tree: Let be the T_x subtree of T rooted at the node x. If a set of attributes γ satisfies the access tree T_x, we denote it as $T_x(\gamma)$ (We compute $T_x(\gamma)$ recursively as follows. If x is a non leaf node, evaluate $T_x'(\gamma)$ for all children x' of node x. $T_x(\gamma)$ Returns 1 iff at least k_x children return 1

An ciphertext-policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Encrypt, KeyGen, , Decrypt and Delegate as described below.

Setup: This algorithm takes the implicit security parameter and outputs the public parameters PK and a master key MK.

Encrypt(PK,M,A): The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. The ciphertext implicitly contains A.

Key Generation(MK,S): The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

Decrypt(PK,CT,SK): The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

Delegate(SK, $\tilde{S}$): The delegate algorithm takes as input a secret key SK for some set of attributes S and a set $\tilde{S} \subseteq S$. It output a secret key $\widetilde{SK}$ for the set of attributes $\tilde{S}$

2.2 Storage Systems: At the early days, the Network-Attached Storage (NAS) and the Network File System (NFS) are used for extra storage devices over the network which will allows user to access the storage devices through network connection. Then forward improvements on scalability, robustness, efficiency, and security were proposed [10-12]. Here storage server can join or leave without control of a central authority. Hence, good scalability is offered by a decentralized architecture for storage systems. Robustness against server failures are provided via a simple method which creates replicas of each message and store them in different servers. As n replicas results in n times of expansion, this method is becomes expensive. One way to reduce the expansion rate is to use erasure codes to encode messages[13],[14]. A message is encoded as a codeword, which is a vector of symbols, and each storage server stores a codeword symbol. A storage server failure is modeled as an erasure error of the stored codeword symbol. Random linear codes support distributed encoding, means each codeword symbol is independently computed. To store a message of

k blocks , each storage server linearly combines the blocks with randomly chosen coefficients and stores the codeword symbol and coefficients. To retrieve the message, a user queries k storage servers for the stored codeword symbols and coefficients and solves the linear system. Some authors addressed robustness and confidentiality issues by presenting a secure decentralized erasure code for the networked storage system.

2.3 Integrity check : Most important functionality about cloud storage is the function of integrity checking. After a user stores data into the storage system, he no longer possesses the data at hand. The user may want to check whether the data are properly stored in storage servers. The concept of provable data possession and the notion of proof of storag are proposed. Nevertheless all of them consider the messages in the clear text form.

3. NETWORK ARCHITECTURE

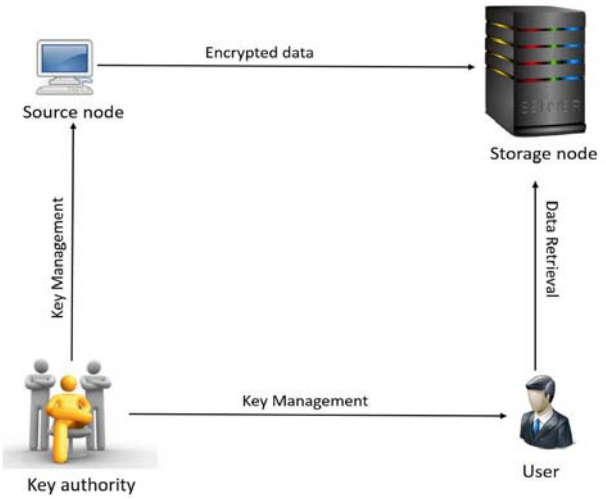

Fig 2. Network Architecture

3.1 System assumption:

Fig 1 show the network architecture. In the DTN network we can assume the following architecture of a network consisting of following components.

1) **Source node:** It has confidential information and wishes to store them into the external data storage node for sharing purpose and intending a reliable delivery to users in the extreme networking environments. Source node user defines (attribute based) access policy and before storing it to the storage node enforces it on its own data by encrypting the data under the policy.
2) **User**: This mobile node is a one who wants to access the data stored at the storage node. To decrypt the ciphertext and obtain the data, User have to posses set of attributes satisfying the access policy of the encrypted data defined by the source node, and is not revoked in any of the attributes .
3) **Server node:** This is an entity that stores data from source and provide corresponding access to users. This storage node may be static or mobile. It is assumed the storage node to be semi trusted, that is honest-but-curious.
4) **Key Authorities :** They are key generation centers responsible for generating public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. It is considered that key authorities are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Different attributes and issues corresponding attribute keys to users are managed by each local authority by granting differential access rights to individual users. The key authorities are assumed to be honest-but- curious. That means, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.

The key authorities should be deterred from accessing plaintext of the data in the storage node as they are semi-trusted; meanwhile, they should be still able to issue secret keys to users. The central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. Both of them don't knows each other's master secrets hence none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the central authority does not collude with the local authorities

3.2 Considered Security threat

1) **Data confidentiality**: Users those do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. Also the unauthorized access from the storage node or key authorities is also prevented. In the existing model, the multiple key authorities are semi trusted as well as the storage node even if they are honest. Hence, the plain data to be stored is kept secret from them as well as from unauthorized users.
2) **Collusion-resistance**: Though each of the users cannot decrypt the ciphertext alone, when multiple users collude, they will decrypt a ciphertext by combining their attributes. We also consider collusion attack among curious local authorities to derive users' keys. In CP-ABE model, rather than embedding secret sharing into user's private key, it is embedded into the ciphertext. The private keys of users are randomized with personalized random values selected by the such that they cannot be combined in the existing scheme.
3) **Backward and forward Secrecy:** It is a considerable scenario that users may change their attributes frequently, e.g., position or location move when considering these as attributes Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time, a ciphertext is encrypted with a policy that can be decrypted with a set of attributes (embedded in the users keys) for users with . After time , say , a user newly holds the attribute set . Even if the new user should be disallowed to decrypt

the ciphertext for the time instance, he can still decrypt the previous ciphertext until it is reencrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the encrypted data even if he does not hold the attribute any more until the next expiration time (forward secrecy). For example, when a user is disqualified with the attribute at time, he can still decrypt the ciphertext of the previous time instance unless the key of the user is expired and the ciphertext is reencrypted with the newly updated key that the user cannot obtain.

4) **Key escrow Problem**: Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information [16-18]. Hence, the most inherent problem is key escrow problem where the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. In CP-ABE, user secret key is generated by single personalized key and multiple attribute keys. It is uniquely determined for each user to prevent collusion attack among users with different attributes. The key generation protocol is composed of the two protocols. Personal key generation where The central authority and each local authority are involved in secret key generation. After setting up the personalized key component, each generates attribute keys for a user with a public parameter received from CA called attribute key generation protocols. Using this 2PC protocol key escrow problem is eliminated via none of authorities can determine the whole key of user independently.

4. CONCLUSIONS

Most popular used communication strategy is using wireless technology. CP-ABE is a secure and efficient cryptographic solution to the access control and secure data retrieval issues for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem, forward and backward secrecy and collusion resistance problem are resolved such that the guaranteed confidentiality of the stored data is achieved under the hostile environment where key authorities might be semi trusted or compromised. In future, the above method can be improved by the concept of multiple storage node for storing single data file

ACKNOWLEDGMENTS

The authors thank anonymous reviewers for their valuable. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies. This work was can be done in part of in our institution and support of all staff members.

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] S.RoyandM.Chuah,“Secure data retrieval based on ciphertext policy attribute-based encryption (CP- ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.

[4] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in Proc. IEEE MILCOM, 2007, pp. 1–7. s[

[5] Goyal V,Pandey O,Sahai A, et al. attribute based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on Computer and communications security. New York: ACM, 2006:89-98.

[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.

[8] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. Eurocrypt, 2005, pp. 457–473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf.Comput.Commun.Security,2006,pp.89–98.

[10] J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao, “Oceanstore: An Architecture for Global-Scale Persistent Storage,” Proc. Ninth Int’l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190201, 2000.

[11] P. Druschel and A. Rowstron, “PAST: A Large- Scale, Persistent Peer-to-Peer Storage Utility,” Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80, 2001.

[12 M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable Secure File Sharing on Untrusted Storage,” Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 2942, 2003.

[13] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, “Ubiquitous Access to Distributed Data in Large-Scale Sensor Networks through Decentralized Erasure Codes,” Proc. Fourth Int’l Symp. Information Processing in Sensor Networks (IPSN), pp. 111117, 2005.

[14] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, “Decentralized Erasure Codes for Distributed Networked Storage,” IEEE Trans. Information Theory, vol. 52, no. 6 pp. 2809-2816,June 2006.

[15] Shamir. Identity Based Cryptosystems and Signature Schemes. In Advances in Cryptology CCRYPTO, volume 196 of LNCS, pages 47- 53.Springer, 1984.

[16] L.CheungandC.Newport, “Provably secure ciphertext policy ABE,” in Proc. ACM Conf. Comput.Commun.Security,2007,pp.456–465.

[17] V.Goyal, A.Jain, O.Pandey, and A.Sahai, “ Bounded ciphertext policy attribute-based encryption,” in Proc.ICALP,2008,pp.579–591.

[18] X. Liang, Z. Cao, H. Lin, and D. Xing, “Provably secure and efficient bounded ciphertext policy attribute based encryption,” in Proc. ASIACCS, 2009, pp. 343–352