INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

Secure Data Retrieval in a Networks using Asymmetric Cryptography with Regeneration of key

T.Pradebha#1, **G.** Rajeswari*2

#1. PG Scholar, Surya Group of Institutions ,Vikkravandi, Villupuram- Dist.

#1 debhathirumal@gmail.com

**2. AP (Sr.G)/CSE,Surya Group of Institutions ,Vikkravandi, Villupuram- Dist.*

**2 rajilaxman.1980@gmail.com*

ABSTRACT

Asymmetric cryptography is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature. Here we propose the concept of dynamic creation of key for each individual user. Each user has there ownkey to decrypt the data. The key belongs to one user can't used by other one to decrypt. This is applicable for corresponding file too.

Index Terms—Access control, Data forwarding, Asymmetric Key Encryption, Secure Data Retrieval.

I. INTRODUCTION:

In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments [1]–[3]. Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. Roy [4] and Chuah [5] introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles, which are managed by the key authorities. For example, in a disruption-tolerant. military network, a commander may store confidential information at a storage node, which should be accessed by members of "Battalion 1" who are participating in "Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing current location of moving soldiers). We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encrypt or defines the attribute set that the decrypt or needs to possess in order to decrypt the cipher text [13]. Thus, different users are allowed to decrypt different pieces of data per the security policy.

ISSN : 2454-9924

However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a collection of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure, or security degradation due to the windows ofvulnerability if the previousattribute key is not updated immediately.

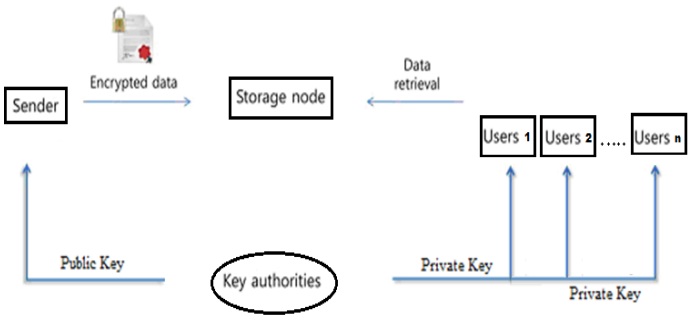
Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys.

If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute-based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities. For example, suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and "region 2" are managed by the authority B. Then, it is impossible to generate an access policy (("role 1" OR "role 2") AND ("region 1" or "region 2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented.

This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as " -out-of- " logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

2. THE SYSTEM ARCHITECTURE:



KEY AUTHORITIES

Key generation centers that generate public/secret parameters.The key authorities consist of a central authority and multiple local authorities. Assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase.Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.

STORAGE NODE

This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar we also assume the storage node to be semi- trusted, that is honest-but-curious.

SENDER

This is an entity who owns confidential messages or data and wishes to store them into the external data storage node

ISSN : 2454-9924

for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

USER

This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier).If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the cipher text and obtain the data.

3. BACKGROUND & RELATED WORKS

A. Attribute Revocation

Bethencourt et al. [13] and Boldyreva et al. first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy [18]. It is a considerable scenario that users such as soldiers 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 re encrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time, a cipher text 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 cipher text for the time instance, he can still decrypt the previous cipher text until it is re encrypted 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 cipher text of the previous time instance unless the key of the user is expired and the cipher text is re encrypted with the newly updated key that the user cannot obtain. We call this uncontrolled period of time windows of vulnerability.

The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the non revoked users can update their keys. This results in the "1-affects- " problem, which means that the update of a single attribute affects the whole non revoked users who share the attribute. This could be a bottleneck for both the key authority and all non revoked users.

The immediate key revocation can be done by revoking users using ABE that supports negative clauses [4], [14]. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance. This scheme will pose overhead group elements1

Additively to the size of the cipher text and multiplicatively to the size of private key over the original CP-ABE scheme of Beth encourt et al. [13], where is the maximum size of revoked attributes set .Golle et al. [20] also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a cipher text is exactly half of the universe size.

B. Key Escrow

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. Thus, the key escrow problem is inherent such that the key authority can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. Chase et al. [24] presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute

authorities should communicate with each other in the system to generate a user's secret key. This results in communication overhead on the system setup and the rekeying phases and requires each user to store additional

ISSN : 2454-9924

auxiliary key. The group elements mean those in the pairing operation group, not the user
group. Since the computation in ABE schemes is done in the pairing operation group, the group elements in the manuscript mean group elements in the pairing group. Components besides the attributes keys, where is the number of authorities in the system.

C. Decentralized ABE

Huang et al. [9] and Roy et al. [4] proposed decentralized CP ABE schemes in the multi authority network environment.They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages of this approach are efficiency and expressiveness of access policy. For example, when a commander encrypts a secret mission to soldiers under the policy ("Battalion 1" AND ("Region 2" OR 'Region 3")), it cannot be expressed when each "Region" attribute is managed by different authorities, since simply multi encrypting approaches can by no means express any general " -out-of- " logics (e.g., OR, that is 1-out-of-). For example, let be the key authorities, and be attributes sets they independently manage, respectively. Then, the only access policy expressed with is , which can be achieved by encrypting a message with by , and then encrypting the resulting cipher text with by (where is the cipher text encrypted under), and then encrypting resulting cipher text with by , and so on, until this multi encryption generates the final cipher text . Thus, the access logic should be only AND, and they require iterative encryption operations where is the number of attribute authorities. Therefore, they are somewhat restricted in terms of expressiveness of the access policy and require computation and storage costs. Chase [25] and Lewkoet al. [10] proposed multi authority KP-ABE and CP-ABE schemes, respectively. However, their schemes also suffer from the key escrow problem like the prior decentralized schemes.

4. CONCLUSION:

An authenticated key exchange protocols that are designed to address the above issues. We show that our protocols are capable of reducing up to approximately 54% of the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness.

It is capable of reducing up to approximately 80% of the workload of the metadata server. TLS protocol with key exchange algorithm is designed to establish a secure connection between a client and a server communicating over an insecure channel and reducing the burden of the server. This is achieved by keeping key authority system and storage nodes in two different paths. Over an insecure channel, a public key is generated along with the corresponding private key and provide to number of users individually. The Key provided is assorted of other keys for each user.

5.REFERENCE

1. C. Adams. The simple public-key GSS-API mechanism (SPKM). The Internet Engineering Task Force (IETF), RFC 2025, Oct 1996.

2. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Communications of the ACM, 53(4):50–58. ACM Press, Apr 2010.

3. M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Advances in Cryptology – Proceedings of EUROCRYPT, pages 139–155. Springer LNCS 1807, May 2000.

4.Amazon simple storage service (Amazon S3). http://aws.amazon.com/ s3/.

5.Zhong hi,chengwang,siqianyang,changjunjiang,and Ivan Stojmenovic,fellow,IEEE:"Space-crossing:community-based data forwarding in mobile social networks under the hybrid communication architecture":DOI 10.1109/TWC.2015.

6.G.Nandi and A.Das, " A survey on using data mining techniques for online social network analysis"international journal of computer science issues,vol 10,nov 2013.

7.G.T.Prabavathi and V.Thiagarasu,"Overlapping community detection algorithm in dynamic networks: An overview"(IJETCAS-13-585)2013

8.ZongqingLu,YonggangWen and GuohongCao,"Community detection in weighted networks: algorithm and applications"IEEEjan 2013.

9.P.Hui,J.Crowcroft, and E.Yoneki, "Bubble rap:social based forwarding in delay tolerant networks":a social network perspective,in ACM Mobihoc 2008.

10.B.Chen, J.Xiang,K.Hu and Y.Tang ,Enhancing betwenness algorithm for detecting community in complex networks," modern physics letters B,Vol.28,no.09,

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924