IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

UNDERSTANDING THE DIFFERENT VULNERABILITY METHODS OF ATTACKS IN SECURE DATA

S.Padmaja*, Mrs.J.Uma Maheswari
* Assistant Professor, School of Computing Sciences, Vels University, Pallavaram,Chennai-600117.
M.Phil Scholar, Vels University, Pallavaram, Chennai-600117.

ABSTRACT

Cipher text-policy attribute based encryption (CPABE) provides an encrypted access control mechanism for broadcasting messages. Basically, a sender encrypts a message with an access control policy tree which is logically composed of attributes; receivers are able to decrypt the message when their attributes satisfy the policy tree. A user's attributes stand for the properties that he current has. It is required for a user to keep his attributes up-to-date. However, this is not easy in CP-ABE because whenever one attribute changes, the entire private key, which is based on all the attributes, must be changed. In this paper, we introduce fading function, which renders attributes ”dynamic” and allows us to update each one of them separately. We study how choosing fading rate for fading function affects the efficiency and security. We also compare our design with CP-ABE and find our scheme performs significantly better under certain circumstance.

KEYWORDS: Network, Vulnerable attacks, CP-ABE and Encryption, DTN, MAC.

INTRODUCTION

Attribute-Based Encryption (ABE) systems use attributes for encryption and decryption of the data. Sahai and Waters proposed an attribute based encryption scheme [5] in 2005. The proposed scheme depends on a single authority for maintaining attributes. A single authority
System has the following drawbacks.

□□All attributes of the system are managed by the single authority; Failure or corruption of the authority affects the whole system.

i. Another drawback of a single authority system is the “Key Escrow” problem.
ii. Private keys are distributed by the single
Authority so that the single authority can decrypt any cipher text in the system. Chase [3] proposed a multi-authority attribute-based encryption system to overcome the drawbacks of a single authority attribute-based system. The proposed system uses a central authority (CA) and multiple attribute authorities (AAs). The problem with the Chase multi authority attribute-based encryption system is that the CA can decrypt every cipher text which reduces the user privacy and confidentiality of user data. Chase and Chow [4] proposed a multi-authority attribute based encryption scheme without the central authority.

CRYPTOGRAPHIC HASH FUNCTION (Algorithm)

A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data is often called the message, and the hash value is often called the message digest or simply the digest. The ideal cryptographic hash function has four main properties: it is easy to compute the hash value for any given message it is infeasible to generate a message that has a given hash it is infeasible to modify a message without changing the hash it is infeasible to find two different messages with the same hash. Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for more general functions with rather different properties and purposes.

NOVEL KEY (ALGORITHM)

Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols. Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling; key scheduling typically refers to the internal handling of key material within the operation of a cipher. The key generation algorithm used here produces a very strong key which is very difficult to guess even with exhaustive search. The process of key generation is as given below:

1. Extract the main features of EEG wave.
2. To reduce the bandwidth compresses the EEG wave using SPIHT algorithm.
3. Pass the non-zero output of this block to the pseudo random binary sequence generator.
4. The output of PRBSG is the key kn.
5. Take mod 8 of the key generated to get a decimal value ranging from 0 to 7.

Then, the user computes for all its attributes key components and finally obtains its whole secret key set as where. During the key generation phase using the 2PC protocol, the proposed scheme (especially 2PC protocol) requires messages additively to the key issuing overhead in the previous multi authority ABE schemes in terms of the communication cost, where is number of key authorities the user is associated with, and is the bit size of an element in . However, it is important to note that the 2PC protocol is done only once during the initial key generation phase for each user. Therefore, it is negligible compared to the communication overhead for encryption or key update, which could be much more frequently performed in the DTNs. (The detailed communication cost will be analyzed in Section V-A.) and Social Networks.

NETWORK ARCHITECTURE

In this section, we describe the DTN architecture and define the security model.

System Description and Assumptions

Fig. 1 shows the architecture of the DTN. As shown in Fig. 1,the architecture consists of the following system entities.

*1) **Key Authorities***: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities Consist of a central authority and multiple local authorities. We 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.

2) ***Storage node:*** This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [1], [2]. Similar to the previous schemes, we also assume the storage node to be semi trusted, that is Honest-but-curious.

3) ***Sender:*** This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node 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.

4) 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. Since the key authorities are semi-trusted, they should be deterred from accessing

plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users. In order to realize this somewhat contradictory requirement, 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. The 2PC protocol prevents them from knowing each other's master secrets so that 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 (otherwise, they can guess the secret keys of every user by sharing their master secrets).

CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data re- trivial issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes indepen- dently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be com- promised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demon- state how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the dis-ruption-tolerant military network.

REFERENCES

[1] W.Baga, R. Molva and S.Crosta. "Policy based encryption schemes from bilinear pairings". In ASIACCS, page 368, 2006.

[2] Bethencourt, A.Sahai, and B.Waters. "Cipher text-Policy-attribute- based encryption in IEEE symphosium on security and privacy, pages321-334,2007.

[3] M.Chase. "Multi-authority attribute based encryption". In TCC, pages 515-534, 2007.

[4] M.Chase and S.Chow. "Improving privacy and security in multi-authority attribute- based encryption". In ACM conference on computer and communications security, pages 121-130,2009.

[5] A.Sahai and B.Waters, "Fuzzy Identity based encryption", In: Advances in cryptology, vol 3494 of LNCS, pp. 457-473, 2005.