International Journal of Current Research in Multidisciplinary (IJCRM)
ISSN: 2456-0979
www.ijcrm.com Volume 1 Issue 2 ǁ June. 2016 ǁ PP 21-25

Improving Privacy and Security in Decentralized Cipher text-Policy Attribute-Based Encryption

G.Balachandar[1], M.Umapathy[2]
[1](Computer Science and Engineering ,TheKavery Engineering College,Salem,TamilNadu)
[2](Assistant Professor ,Computer Science and Engineering ,The Kavery Engineering College,Salem,TamilNadu)

Abstract :
In from multiple authorities with them knowing his/her attributes and furthermore, a central authority is required. Notably, a user's identity information can be extracted from his/her some sensitive attributes. Hence, existing PPMA-ABE schemes cannot fully protect users' privacy as multiple authorities can collaborate to identify a user by collecting and analyzing his attributes. Moreover, cipher text-policy ABE (CP-ABE) is a more efficient public-key encryption, where the encrypt or can select flexible access structures to encrypt messages. Therefore, a challenging and important work is to construct a PPMA-ABE scheme where there is no necessity of having the central authority and furthermore, both the identifiers and the attributes can be protected to be known by the authorities. In this paper, a privacy-preserving decentralized CP-ABE (PPDCP-ABE) is proposed to reduce the trust on the central authority and protect users' privacy. In our PPDCP-ABE scheme, each authority can work independently without any collaboration to initial the system and issue secret keys to users. Furthermore, a user can obtain secret keys from multiple authorities without them knowing anything about his global identifier and attributes. Previous privacy-preserving multiauthority attribute-based encryption (PPMA-ABE) schemes, a user can acquire secret keys

I. Introduction

Existing System : Our scheme is constructed in the standard model, while the existing DCP-ABE scheme was designed in the random oracle model. The existing scheme. Since sensitive attributes can also reveal the users' identities, existing schemes cannot provide a full solution to protect users' privacy in MA-ABE schemes. We exploit the set-membership proof technique. For each attribute, the authority specifies an un forgeable authentication tag such that a user can prove in zero knowledge that the attribute for which he is possessing a secret key is monitored by the authority.

Proposed System: The proposed PPDCP-ABE scheme can provide stronger privacy protection compared to the previous PPMA-ABE schemes where only the GID is protected. Proposed a distributed CP-ABE scheme. This scheme was proven to be secure in the generic group, instead of reducing to a complexity assumption. In this scheme, a central authority is required to generate the global key and issue secret keys to users. A fully secure multi-authority CP-ABE (MACP-ABE) scheme in the standard model was proposed. This scheme was based on the previous CP-ABE scheme. In this scheme, there are multiple central authorities and attribute authorities.

Advantage

- The central authorities distribute identity related keys to users, while the attribute authorities distribute attribute-related keys to users.
- Prior to possessing attribute keys from the attribute authorities, the user must obtain secret keys from the multiple central authorities.
- In this scheme, multiple authorities can work independently without any collaboration.

Drawback of these papers (future work)

- This scheme not effective result for key encryption processes.
- Need for more privacy.
- Need for new method for security enhancement
- This key process is centralized authority using here. But key static process using there.
- We need change the random key process.

- We must using AES 256bit key process. This is high level bit encryptions.
- Need for time limit for key process.
- Find the internal packet missing problem.
- Trace out the missing packet

II. Literature survey

Improving privacy and security in decentralized ciphertext-policy attribute-based encryption : Attribute-based Encryption Sahai and Waters introduced the first attribute-based encryption (ABE) where both the ciphertext and the secret key are labelled with a set of attributes. A user can decrypt a ciphertext if and only if there is a match between the attributes listed in the ciphertext and the attributes held by him. ABE schemes can be classified into two types: key-policy ABE (KPABE) and ciphertext-policy ABE (CP-ABE). KP-ABE. In a KP-ABE scheme, the ciphertext is associated with a set of attributes, while an access structure is embedded in the secret keys CP-ABE. In a CP-ABE scheme, an access structure is embedded in the ciphertext, while the secret keys are associated with a set of attributes.

Multi-Authority Attribute-based Encryption : In the seminal work, Sahai and Waters left an open problem, namely how to construct an ABE scheme where the secret keys can be extracted from multiple authorities so that users can reduce the trust on the central authority. Chase answered this question affirmatively by proposing an MAABE scheme. As mentioned in, the technical hurdle in constructing an MA-ABE scheme is to resist the collusion attacks. To overcome this hurdle, all secret keys of a user are tied to his GID. In [10], multiple authorities must interact to initialize the system, and a central authority is required. Lin et al. proposed an MA-ABE scheme where the central authority is not required. This scheme was derived fromthe distributed key generation (DKG) protocol and the joint zero secret sharing (JZSS) protocol. To initialize the system, the multiple authorities must collaboratively execute the DKG protocol and the JZSS protocol twice and k times, respectively, where k is the degree of the polynomial selected by each authority. Each authority must keep k+2 secret keys. Furthermore, this scheme is k-resilient, namely the scheme is secure if and only if the number of the compromised users is no more than k, and k must be fixed in the setup stage. Muller et al. [20] proposed a distributed CP-ABE scheme.

This scheme was proven to be secure in the generic group [4], instead of reducing to a complexity assumption. In this scheme, a central authority is required to generate the global key and issue secret keys to users. A fully secure multi-authority CP-ABE (MACP-ABE) scheme in the standard model was proposed by Liu et al.[21]. This scheme was based on the previous CP-ABE scheme [8]. In this scheme, there are multiple central authorities and attribute authorities. The central authorities distribute identity related keys to users, while the attribute authorities distribute attribute-related keys to users. Prior to possessing attribute keys from the attribute authorities, the user must obtain secret keys from the multiple central authorities. This scheme was constructed in the bilinear group with Composite order (N = p1p2p3). Lekwo and Waters [11] proposed a new MA-ABE schemecalled decentralizing CP-ABE (DCP-ABE) scheme. This scheme improved the previous MA-ABE schemes that require collaborations among multiple authorities to initial the system.In this scheme, no cooperation between the multiple authorities is required in the setup stage and the key generation stage, and a central authority is not required. Notably, an authority in this scheme can join or leave the system dynamically without the need to reinitialize the system. The scheme was constructed in the bilinear group with composite order (N = p1p2p3), and achieved full (adaptive) security in the random oracle model. Furthermore, they also proposed two methods to create a prime order group variant of their scheme. Nevertheless, the authorities can collect a user's attributes by tracing his GID. Chase and Chow first proposed [12] a privacy-preserving MA-ABE (PPMA-ABE) scheme which improved the previous scheme [10] and removed the need of a central authority.In previous MA-ABE schemes, to obtain the corresponding secret keys, a user must submit his GID to each authority.

Hence, multiple authorities can collaborate to collect the user's attributes by his GID. In Chase and Chow provided an anonymous key issuing protocol for the GID by using the 2-party secure computing technique. As a result, a group of authorities cannot collaborate to collect the users attributes by tracing his GID. Nevertheless, the multiple authorities must cooperate to initial the system. Meanwhile, each pair of authorities must execute the 2-party key exchange protocol to share the seeds of the selected pseudorandom functions (PRFs) [22]. This scheme is N −2 tolerant, namely the scheme is secure if and only if the number of the compromised authorities is no more than N − 2, where N is the number of the authorities in the system. The authorities cannot know any information about the user's GID, but they can know the user's attributes. Chase and Chow [12] also left an open challenging research problem on how to construct a PPMA-ABE scheme without the need of cooperation's among authorities. Li [15] proposed a MACP-ABE scheme with accountability. In this scheme, the anonymous key issuing protocol [12] was employed. Specifically, a user can be identified when he shared His secret keys with others. Likewise, the multiple authorities must cooperate to initialize the system. Recently, a privacy-preserving decentralized KP-ABE (PPDKP-ABE) scheme was proposed by Han et al. . In this scheme, multiple authorities can work independently without any collaboration. Especially, a user can obtain secret keys from multiple authorities without releasing anything about his GID to them, and the central authority is not required. Qian et al. Proposed a privacy-preserving decentralized CPABE (PPDCP-ABE) scheme where simple access structures can be implemented. Nevertheless, similar to that in the authorities in these schemes can also collect the user's attributes. C. Anonymous Credential In an anonymous credential system [23], a user can obtain a credential from an issuer, which includes the user's pseudonym and attributes. By using it, the user can convince a third party that he obtains a credential containing the given pseudonym and attributes without releasing any other information. In a multiple-show credential system [24], a credential can be demonstrated an arbitrary number of times, and cannot be linked to each other. Therefore, when constructing our PPDCP-ABE, we assume that each user has obtained an anonymous credential including his GID and attributes. Then, he can convince the multiple authorities that he has a GID and holds the corresponding attributes by using the anonymous credential technique.

Multi-Processor Architectural Support for Protecting Virtual Machine Privacy in Untrusted Cloud Environment : Cloud computing is revolutionizing the information technology, ranging from personal to enterprise to government computing. While cloud computing can provide computational and storage resources on demand and at a low cost, it creates new security/privacy problems. This is fundamentally caused by the separation of resource users (i.e., cloud tenants) from resource owners (i.e., cloud providers).New threats and concerns include: (i) failures in ensuring separation between tenants in terms of storage and memory;(ii) subversion of hypervisor or Virtual Machine Monitor (VMM) [1]; (iii) attacks launched from one Virtual Machine (VM) against the host platform or the other located VMs on the same platform [2, 3]; (iv) eavesdropping a tenant's VM contents by a compromised VMM, untrusted resource owners, or malicious insiders. These threats have caused a large degree of reluctance in adopting the cloud paradigm [4,5]. According to a survey of more than 500 global executives and IT managers in 17 countries [6], 20% executives trust their internal systems over the cloud due to concerns about security threats and loss of control over data and systems. Indeed, many data centre customers demand their services to be hosted by dedicated servers that are physically isolated from other customers' servers. This would ruin, to a large extent, the merits of cloud computing that are essentially based on virtualization and sharing of physical resources.

Access control and secure data retrieval based on ciphertext policy attribute-based encryption in decentralized DTNS : Now days many computing devices e.g. PDAs, smart-phones, sensors have wireless interfaces and hence can form ad hoc networks. Wireless adhoc networks allow nodes to communicate with one another without relying on any fixed infrastructure. These rapidly deployable networks are very useful in several scenarios e.g. [1] military network environments, connections of wireless devices carried by soldiers may be temporarily disconnected by environmental factors, jamming and mobility, especially when they operate in terrestrial environments. Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme terrestrial environments [2]-[4]. 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. For storage and replicate the data storage node is introduced [5][6]where authorized mobile nodes can access the necessary information quickly. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced [7], [8]. 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. Multiple key authorities manage their attribute independently in DTN [9], [10].

The concept of attribute-based encryption (ABE) [11]–[14] is a promising approach that fulfils 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 ciphertexts. Especially, ciphertexts-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext [13].Thus, different users are allowed to decrypt different pieces of data per the security policy. 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 attributes 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 associatedattribute 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 of vulnerability if the previous attribute key is not updated immediately.
One more challenging issue is Key escrow problems ,CP-ABE, authority's master secret key is used to generates private keys of users associated set of attributes. So, 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 multipleauthority 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 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.

ABE comes in two flavors called key-policy ABE (KP-ABE)andciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes. The key authority chooses a policy for each user that determines which ciphertexts he can decrypt and issues the key to each user by embedding the policy into the user’s key. However the roles of the cipher texts and keys are reversed in CP-ABE. In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptorssuch as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes [4], [7], [15] location of node tracked to reduce overhead [18].

Effective Data Retrieval in Disruption Tolerant Networks Using Cipher Text Policy-Attribute Based Encryption : The Disruption tolerant networks [1] has many application such as space environment and terrestrial environment in which terrestrial environment mainly concerned with IntermittentlyConnected Networks(ICNs) and frequency partitions(FPs), where ICNs doesn’t prevent communication between the disconnected areas and FPs doesn’t allow for resource allocation. The terrestrial environment of DTN is envisioned for Under Water Networks (UMNs), Pocket Switched Networks (PSNs), Vehicular Ad-hoc Networks (VANETs) and Airborne Networks (ANs). UMNs are deployed to perform collaborative monitoring tasks over an oceanographic area. The characteristics of UMNs are transmission loss, noise, multipath, high delay and delay variance and doppler spread PSN is a new communication paradigm for mobile devices. It takes advantage of every communication opportunity, and the physical mobility of the devices, in order to transport data to destinations. VANET uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. ANs are proposed network in which all nodes would be located in aircraft. The network is intended for use in aviation communications, navigation, and surveillance (CNS) and would also be useful to businesses, private Internet users, and government agencies, especially the military. The attribute-based encryption is a promising approach for encryption and decryption using public key encryption (PKE), Identity based encryption (IDE), Fuzzy identity based encryption (Fuzzy-IDE), Cipher-text policy or key policy attribute based encryption (CP-ABE or KP-ABE) [2], [8]. The concept of attribute-based encryption (ABE) [4],[7] provides access policies and described attributes among private keys and Cipher text.
The major difference between CP-ABE and KP-ABE in Cipher text–policy ABE [2], [5], access policy is associated in the Cipher text and in key-policy ABE access policy is associated with the private key.

Cipher Text - Policy Attribute based Encryption for Secure Data Retrieval in Disruption Tolerant Military Networks (DTN) : The Cipher text - policy Attribute Based Encryption for secure data retrieval in decentralized Disruption Tolerant Networks (DTNs) where multiple key authorities manage their attributes independently. Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Key escrow problem is resolved by an escrow-free key issuing g protocol that exploits the characteristic of the decentralized Disruption Tolerant Networks architecture proposed a decentralized approach; their technique does not authenticate users. Demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption - tolerant military network. Finally the Disruption - tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes.

III. Future enhancements

As a future work, such a structure synergistically combines the inherent advantages and overcome the disadvantages of the Privacy and secures new enhancements of server authentication and network security enhancement. Two party computational protocol which is used to deliver attribute keys for each users. The organization of attributes difficult is decided by avoiding the grouping of users to access same data in dissimilar position by the various key that can be provided by key authority. The inherent key escrow problem is determined such that the secrecy of the stored information's is certain even under the aggressive environment where key authorities might be not cooperated by providing escrow free key

References

[1] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. Au, "PPDCPABE: Privacy-preserving decentralized ciphertext-policy attribute-based encryption," in Computer Security (Lecture Notes in Computer Science), vol. 8713. Cham, Switzerland: Springer-Verlag, 2014, pp. 73–90.

[2] P. Bichsel, J. Camenisch, T. Groß, and V. Shoup, "Anonymous credentials on a standard Java Card," in Proc. ACM Conf. CCS, 2009, pp. 600–610.

[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494.Heidelberg, Germany: Springer-Verlag, 2005, pp. 457–473.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. SP, May 2007, pp. 321–334.

[5] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. CCS, 2007, pp. 456–465.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. CCS, 2006, pp. 89–98.

[7] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. 14th ACM Conf. CCS, 2007, pp. 195–203.

[8] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical)inner product encryption," in Advances in Cryptology (Lecture Notesin Computer Science), vol. 6110. Heidelberg, Germany: Springer-Verlag, 2010, pp. 62–91.

[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571. Heidelberg, Germany: Springer-Verlag, 2011, pp. 53–70.

[10] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography (Lecture Notes in Computer Science), vol. 4392. Heidelberg, Germany: Springer-Verlag, 2007, pp. 515–534.

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6632. Heidelberg, Germany: Springer-Verlag, 2011, pp. 568–588.

[12] M. Chase and S. S. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proc. 16th ACM Conf. CCS, 2009, pp. 121–130.

[13] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[14] H. Qian, J. Li, and Y. Zhang, "Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure," in Information and Communications Security (Lecture Notes in Computer Science), vol. 8233. Heidelberg, Germany: Springer-Verlag,2013, pp. 363–372.

[15] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in Proc. 6th ASIACCS, 2011,pp. 386–390.

[16] J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6056. Heidelberg, Germany: Springer-Verlag, 2010, pp. 19–34.

[17] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," in Progress in Cryptology (Lecture Notes in Computer Science), vol. 5365. Heidelberg, Germany: Springer-Verlag, 2008, pp. 426–436.