SECURE DATA TRANSFER WITH DISRUPTION TOLERANT NETWORK TECHNOLOGY IN MILITARY APPLICATION

Dr. A.Satyanarayana[1], Dr. JVN Ramesh[2]
[1,2]Siddartha Institute of Technology and Sciences

Abstract

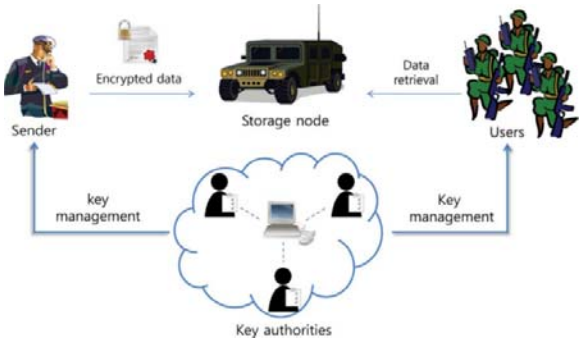
This paper presents about a communication system which communicates the information from source to destination in a secure manner. In a normal communication system that may effect by the intermittent network connectivity and authentication problem. Such problems can be avoided by disruption tolerant network (DTN) technologies. This system had successfully launched in military communication. In this communication the soldiers required the confidential information or reliable information in a successful manner in between two wireless devices. The most challenging issues in this scenario are the authorization policies and secure data retrieval. The cipher text policy attribute based encryption (CP-ABE) is a cryptographic resolver for above the issues. However the issues of CP-ABE in decentralized DTH, introduces in several security systems. In this paper, we proposed secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.

Keywords: disruption tolerant network, cipher text policy, security systems , decentralized DTH

Introduction

The key expert chooses a policy for each user that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key. The immediate key revocation can be done by revoking users using ABE that supports negative clauses. 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. Since some users may change their associated attributes at some point or some private keys might be compromised, key revocation 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

- First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability
- Second, encryptions can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities.
- Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture



- The concept of attribute-based encryption (ABE) is a promising Approach that fulfils the requirements for secure data retrieval in DTNs.
- The problem of applying the ABE to DTNs introduces several securities and privacy challenges.

- 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.

Cipher text-policy ABE make available a well-organized means of encrypting data with the intention that attribute set was described that needs to possess with the purpose of decrypting cipher-text. The key escrow intricacy is resolved by means of an escrow-free key issuing procedure that exploits feature of decentralized disruption-tolerant network construction. Attribute-based encryption features a method that facilitates an access control above encrypted data by means of access policies and recognized attributes between private keys and ciphertexts. Cipher textpolicy ABE provides an efficient means of encrypting data with the intention that attribute set was described that decryptor needs to possess with the purpose of decrypting cipher-text. Different users are authorized to decrypt dissimilar pieces of data for each security policy

A. Related Work

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the en-cryptor 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 ciphertexts 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 encryptors such as a commander to choose an access policy on attributes and to encrypt confi-dential data under the access structure via encrypting with the corresponding public keys or attributes [4], [7], [15].

1) Attribute Revocation: Bethencourt *et al.* [13] andBoldyreva*et al.* [16] 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 dis-tribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes [8], [13], [16], [17] have two main problems.

The first problem is the security degradation in terms of the backward and forward secrecy [18]. It is a considerable sce-nario that users such as soldiers may change their attributes fre-quently, e.g., position or location move when considering these as attributes [4], [9]. Then, a user who newly holds the attribute might be able to access the previous data encrypted before heobtains the attribute until the data is reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time t_i , a ciphertext$C$ is encrypted with a policy that can be decrypted with a set of attributes a_i (embedded in the users keys) for users with a_i . After time t_i , say t_j , a user newly holds the attribute set a_i . Even if the new user should be disallowed to decrypt the ciphertext$C$ for the time instance t_i , he can still decrypt the previous ciphertext$C$ until it is reencrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the en-crypted 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 a_i at time t_j , he can still decrypt the ciphertext$C$ of the previous time instance t_i unless the key of the user is expired and the ciphertext is reencrypted 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 pe-riodically announces a key update material by unicast at each time- slot so that all of the nonrevoked users can update their keys. This results in the "1-affects-n" problem, which means that the update of a single attribute affects the whole nonrevoked users who share the attribute [19]. This could be a bottleneck for both the key authority and all nonrevoked 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 perfor-mance. This scheme will pose overhead $O(R)$ group elements[1]

additively to the size of the ciphertext and $O(\log M)$ multi-plicatively to the size of private key over the original CP-ABE scheme of Bethencourt*et al.* [13], where M is the maximum size of revoked attributes set R. 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 ciphertext is ex-actly half of the universe size.

2) Key Escrow: Most of the existing ABE schemes are con-structed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information [11], [13], [14], [21]–[23]. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext 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 multiauthority 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 ap-proach is the performance degradation. Since there is no cen-tralized 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 $O(N_2)$commu-nication overhead on the system setup and the rekeying phases

B. Contribution

In this paper, we propose an attribute-based secure data re-trieval scheme using CP-ABE for decentralized DTNs. The pro-posed scheme features the following achievements. First, imme-diate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is re-solved by an escrow -free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by per-forming a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC pro-tocol deters the key authorities from obtaining any master secret information of each other such that none of them could gen-erate the whole set of user keys alone. Thus, users are not re-quired to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be crypto-graphically enforced against any curious key authorities or data storage nodes in the proposed scheme.

C. Revocation

We observed that it is impossible to revoke specific attribute keys of a user without rekeying the whole set of key components of the user in ABE key structure since the whole key set of a user is bound with the same random value in order to prevent any collusion attack. Therefore, revoking a single attribute in the system requires all users who share the attribute to update all their key components even if the other attributes of them are still valid. This seems very inefficient and may cause severe overhead in terms of the computation and communication cost, especially in large-scaled DTNs.

For example, suppose that a user u_t is qualified with l dif-ferent attributes. Then, all l attribute keys of the user u_t are gen-erated with the same random number r_t in the ABE key archi-tecture. When an attribute of the user is required to be revoked ($l-1$ other attribute keys of the user are still valid), the other valid $l-1$ keys should be updated with another new r_t that is different from r_t and delivered to the user. Unless the other $l-1$ keys are updated, the attribute key that is to be revoked could be used as a valid key until their updates since it is still bound with the same r_t . Therefore, in order to revoke a single attribute key of a user, $O(l)$ keys of the user need to be updated. If n users are sharing the attribute, then total $O(nl)$ keys need to be updated in order to revoke just a single attribute in the system

D. Key Update

When a user comes to hold or drop an attribute, the corre-sponding key should be updated to prevent the user from ac-cessing the previous or subsequent encrypted data for backward or forward secrecy, respectively.

The key update procedure is launched by sending a join or leave request for some attribute group from a user who wants to hold or drop the attribute to the corresponding authority. On receipt of the membership change request for some attribute groups, it notifies the storage node of the event. Without loss of generality, suppose there is any membership change in G_i (e.g., a user comes to hold or drop an attribute λ_i at some time instance). Then, the update procedure progresses as follows.

1) The storage node selects a random $s \in Z_*$ and a K_i, which is different from the previous attribute group

TABLE I
EXPRESSIVENESS, KEY ESCROW, AND REVOCATION ANALYSIS

Scheme	Authority	Expressiveness	Key Escrow	Revocation
BSW [13]	single	–	yes	periodic attribute revocation
HV [9]	multiple	AND	yes	periodic attribute revocation
RC [4]	multiple	AND	yes	immediate system-level user revocation
Proposed	multiple	any monotone access structure	no	immediate attribute-level user revocation

ANALYSIS

In this section, we fi rst analyze and compare the efficiency of the proposed scheme to the previous multiauthority CP-ABE schemes in theoretical aspects. Then, the efficiency of the proposed scheme is demonstrated in the network simulation in terms of the communication cost. We also discuss its efficiency when implemented with specific parameters and compare these results to those obtained by the other schemes.

Table I shows the authority architecture, logic expressive-ness of access structure that can be defined under different dis-joint sets of attributes (managed by different authorities), key escrow, and revocation granularity of each CP-ABE scheme. In the proposed scheme, the logic can be very expressive as in the single authority system like BSW [13] such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [9] and RC [4] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, attributes of users can be revoked at any time even before the expiration time that might be set to the attribute. This enhances security of the stored data by re-ducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each at-tribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the ser-vice in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the ac-cess policy defined in the ciphertext. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities.

Table II summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the key authority or the storage node needs to send to update nonrevoked users' keys for an attribute. Private key size represents the storage cost re-quired for each user to store attribute keys or KEKs. Public key size represents the size of the system public parameters. In this comparison, the access tree is constructed with attributes of m different authorities except in BSW of which total size is equal to that of the single access tree in BSW. As shown in Table II, the proposed scheme needs rekeying message (Hdr) size of at most $(n-l)\log \frac{n}{C}$ to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its ciphertext size is linear to the number of revoked users in the system since the user revocation mes-sage is included in the ciphertext. The proposed scheme requires a user to store $\log m$ more KEKs than BSW. However, it has an effect on reducing the rekeying message size. The proposed scheme is as efficient as the basic BSW in terms of the ciphertext size while realizing more secure immediate rekeying in multi-authority systems.

References

[1] https://www.google.co.in/imgres?imgurl= http://blogs.shephertz.com/wp-content /uploads/2013/08/connection-resiliency. jpg&imgrefurl =http: //blogs .shephertz. com/ 2013/08/27/connection-resiliency-support-to-recover-from-intermittent-connection-errors/&h=312 &w=330 & tbnid=ssJnx4mMNmpr4M:&docid=T3S8 x6HQ6nK5EM&hl=en&eia6rVsniHseKu ATxsaCoDw&tbm=isch&ved=0ahUKEwi Jw5r10s_KAhVHBY4KHfEYCPUQMwhc KDkwOQ

[2] https://www.google.co.in/imgres?imgurl= http://i.stack.imgur.com/W1IMx.png&img refurl=http://security.stackexchange.com/ questions/24620/what-is-the-role-of-radius-server-and-active-directory-to-increase-the-security&h=173&w=552&tbnid=4RQ63 7jengz8GM:&docid=A4s924ZztUwMbM &hl=en&ei=p7CrVoKxOYfvugT-6ryIAg&tbm=isch&ved=0ahUKEwjCoLr C1M_KAhWHt44KHX41DyEQMwgbKA AwAA

[3] https://www.google.co.in/imgres?imgurl= http://www.nasa.gov/sites/default/files/im ages/

[4] 509835main_DTN_DemonstrationPhasin g.png&imgrefurl=https://www.nasa.gov/c ontent/disruption-tolerant networking&h =244& w=330 & tbnid =E3B34boaZwe4jM:&docid=qDfV59FX 7U5AyM&hl=en&ei=ca6rVqPXO8P_ugS -xqfIDw &tbm =isch&ve d=0ahU KEwjj08q00s_KAhXDv44KHT7jCfkQMw gnKAwwDA

[5] Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014

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

[7] 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] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Medi-atedciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[9] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryp-tion," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[10] D. Huang and M. Verma, "ASPE: Attribute-based secure policy en-forcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp.1526–1535, 2009.

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

[12] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc.Eurocrypt*, 2005, pp. 457–473.

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

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[15] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput.Commun. Security*, 2007, pp. 195–203.

[16] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

[17] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Se-curity*, 2008, pp. 417–426.

[18] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 99–112.