ATTRIBUTE-BASED SECURE DATA RETRIEVAL SCHEME USING CP-ABE

M.Baby[1], T.Brindha[2], A.Dhivya[3], B.Gnanamozhi[4]

[1,2,3,4] *Information Technology, Panimalar Engineering College, (India)*

ABSTRACT

Mobile nodes in military environments such as a battlefield or a hostile region suffer from intermittent network connections and frequent partitions. Disruption-tolerant network (DTN) technologies are best solutions that allow wireless devices carried by soldiers to communicate and access the confidential information or command reliably by exploiting external nodes. Cipher text-policy attribute-based encryption (CP-ABE) is a cryptographic solution to the access control issues. The problem of applying CP-ABE in decentralized DTNs generates several security and privacy issues with attribute updation, key escrow problem, and attribute coordination issued from different key authorities. We propose a attribute based secure data retrieval scheme for decentralized DTNs where multiple key authorities manage their attributes separately. In this paper,we are proposing CP-ABE using MD5 algorithm and two channels are required for secure data retrieval. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

I. INTRODUCTION

In several military networks,wire-less devices gets disconnected due to jamming, environmental factors, and changes in position, mainly when they operate in remote environments. Disruption-tolerant network (DTN) technologies are best solutions that allow nodes to communicate with each other in extreme networking environments. When there is no end-to-end connection, 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 and Chuah 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. In many scenarios, it is desirable to provide differentiated access services such that data access policies are defined over user attributes.The key authorities will manage these data access policies. For instance, in a Disruption-tolerant military network, a sender may store confidential information at a intermediate node, which must be accessed by "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. We refer 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. ABE enables an access control over encrypted data using access policies and ascribed

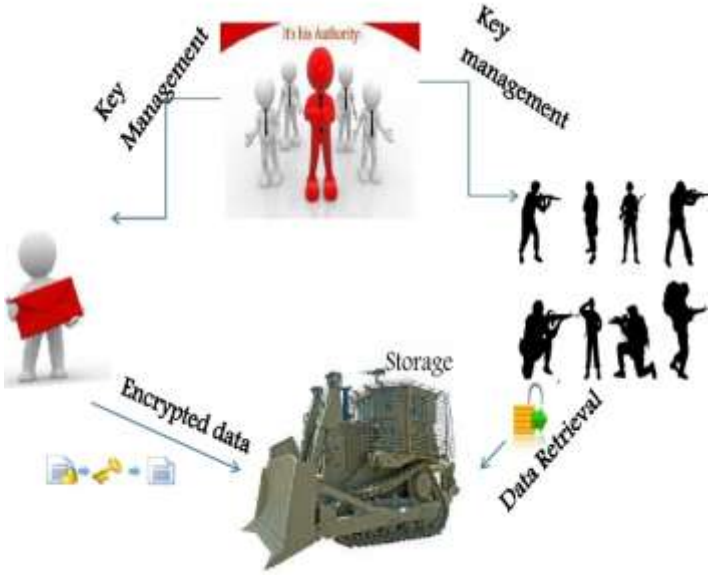
attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to de-crypt the cipher text . Thus, different users are allowed to decrypt different pieces of data per the security policy.

However, the problem of applying the ABE to DTNs introduces several security and privacy issues. Since users may change their associated attributes at some point (for ex-ample, mobility), 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 more challenging, mainly in ABE, since each attribute is conceivably shared by multiple users (we refer to such a collection of users as an attributes). This shows that attribute revocation or any single user in an attribute group would affect the other users in the group. For instance, if a member joins or leaves an attribute group, the corresponding attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may cause problem during rekeying procedure, or degrade the security due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow . In CP-ABE, the key authority provides private keys by applying the authority's master secret keys to members' associated set of at-tributes. Thus, the key authority can dechiper every cipher text to specific users by generating their attribute keys. If the key authority is compromised by hackers when deployed in the remote environments, this could be a main threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an main problem in the multiple-authority systems as long as each key authority has the whole access to generate their own attribute keys with their own master secrets. Since the key generation mechanism based on the single master secret is the basic method for the asymmetric encryption systems such as the attribute-based or identity-based encryption rules, removal of key escrow in single or multiple-authority CP-ABE is a pivotal open problem.

The last issue is the coordination of attributes issued from different key authorities. When multiple key authorities manage and issue attributes keys to users with their own master secrets, which is very difficult to define fine-grained access policies over attributes issued from different key authorities. For instance,the attributes "role 1" and "region 1" are man-aged by the authority X, and "role 2" and "region 2" are man-aged by the authority Y.It is impossible to produce 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 invented. Because, the fact that the different authorities generate their own attribute keys using their own independent and separate master secret keys. Hence, general access policies, such as " -out-of- " logic, cannot be expressed in the previous methods, which is a very practical and commonly required access policy logic.

II. NETWORK ARCHITECTURE



2.1 System Description and Assumptions

1)Key Authorities: Key authorities are key generation centers that generate public/secret parameters for CP-ABE. The key authorities contain a central authority and many local authorities. We take that there are secure and reliable communication channels between a central authority and every local authority during the initial key setup and generation phase. Each local authority maintains different attributes and provides associate attribute keys to members. They allow different access rights to each users based on the members' attributes. The key authorities are assumed to be honest. ie, they will execute the assigned tasks in the node, therefore they would learn information of encrypted contents as much as possible.

2)Storage node: Storage node is an entity that stores data from senders and provide access to members. It may be dynamic or static. Similar to the previous schemes, we also assume the storage node 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 unreadable data explain by the commander, and is not revoked, then decrypt the ciphertext and obtain the data.

III. SYSTEM ANALYSIS

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

IV. EXISTING SYSTEM

In several military networks,wire-less devices gets disconnected due to jamming, environmental factors, and changes in position, mainly when they operate in remote environments. Disruption-tolerant network (DTN) technologies are best solutions that allow nodes to communicate with each other in extreme networking environments. When there is no end-to-end connection, 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 and Chuah 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. In many scenarios, it is desirable to provide differentiated access services such that data access policies are defined over user attributes.The key authorities will manage these data access policies. For instance, in a Disruption-tolerant military network, a sender may store confidential information at a intermediate node, which must be accessed by "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. We refer DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

4.1 Disadvantages of Existing System

1. No Proper Encryption Schema is implemented.
2. security degradation.
3. Key escrow.

V. PROPOSED SYSTEM

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval. ABE 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 encryptor defines the attribute set that the decryptor needs to possess in order to de-crypt the cipher text . 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 issues. Since users may change their associated attributes at some point (for ex-ample, mobility), 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 more challenging, mainly in ABE, since each attribute is conceivably shared by multiple users (we refer to such a collection of users as an attributes). This shows that attribute revocation or any single user in an attribute group would affect the other users in the group. For instance, if a member joins or leaves an attribute group, the corresponding attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may cause problem during rekeying procedure, or degrade the security due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow . In CP-ABE, the key authority provides private keys by applying the authority's master secret keys to members' associated set of at-tributes. Thus, the key authority can dechiper every cipher text to specific users by generating their attribute keys. If the key authority is compromised by hackers when deployed in the remote environments, this could be a main threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an main problem in the multiple-authority systems as long as each key authority has the whole access to generate their own attribute keys with their own master secrets. Since the key generation mechanism based on the single master secret is the basic method for the asymmetric encryption systems such as the attribute-based or identity-based encryption rules, removal of key escrow in single or multiple-authority CP-ABE is a pivotal open problem.

5.1 Authentication

This module helps to send the message safely from a commander to the soldier in the war field. They both should set a secret Key word for sending and receiving the message safely. Without that keyword the message cannot be read by the soldier.

5.2 Sending Message

When a commander is sending message to his soldier in war field he needs to set a secret key which is known to him and his soldier alone. So, when he sends a message to him the soldier should enter the secret key word and then only the message will be displayed.

5.3 Encryption

Encryption is a process of converting a message, called the Plaintext, into an unreadable message, called the Cipher text. This is usually accomplished using a secret Encryption Key and a cryptographic Cipher. It helps to avoid eaves dropping when the message is sent.

5.4 Receiver

When a soldier is receiving message from his commander in war field , he should enter the secret key and after decryption ,then the message will be displayed.

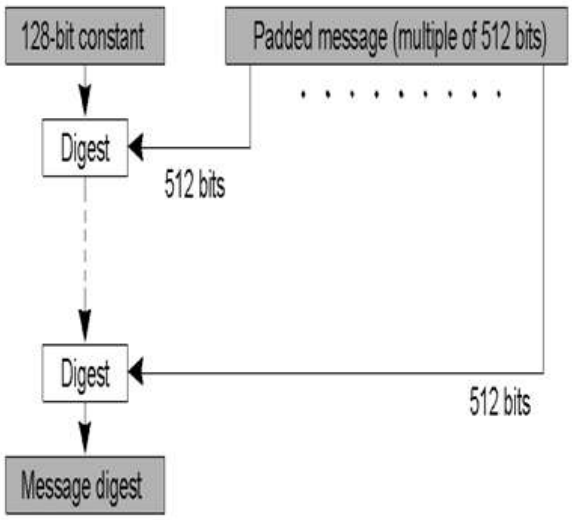
5.4.1 Advantages of Proposed System

1. Data Transmission without any interruption.
2. Secure transmission of data between nodes.

VI. METHODOLOGY

MD5 algorithm was introduced by Professor Ronald L. Rivest in 1991.MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input …The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA."

6.1 MD5 Algorithm Structure



Step1 Append padding bits

The input message is "padded" so that its length (in bits) equals to 448 mod 512. Padding is performed, if the length of the message is already 448 mod 512. The input message is "padded" so that its length (in bits) equals to 448 mod 512. Padding is performed, if the length of the message is already 448 mod 512.

Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448 mod 512.The appending bits are atleast one bit and at most 512 bits

.**Step2. Append length**

A 64-bit representation of the message length is appended to the result of previous step. If the message length is greater than 2^64, only the low-order 64 bits will be used. The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message has length that is an exact multiple of 16 (32-bit) words.A 64-bit representation of the length of the message is appended to the result of previous step. If the message length is greater than 2^64, only the low-order 64 bits will be used.

The resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. The input message has the length that is an exact multiple of 16 (32-bit) words.

Step3. Initialize MD buffer

A four-word buffer (A, B, C, D) is used to compute the MD.A, B, C, D is a 32-bit register. These registers are used to the values in hexadecimal. The low-order bytes are arranged first.

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

Step 4. Process message in 16-word blocks

Four functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

F (X, Y, Z) = XY or not (X) Z

G (X, Y, Z) = XZ or Y not (Z)

H (X, Y, Z) = X xor Y xor Z

I (X, Y, Z) = Y xor (X or not (Z))

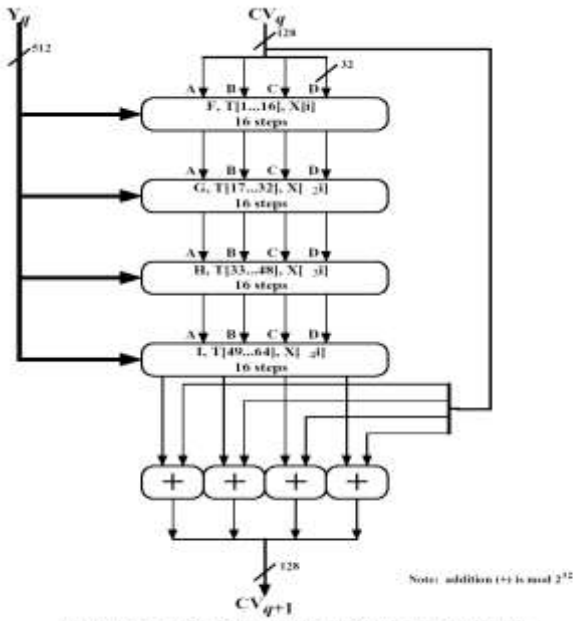


Figure 9.2 MD5 Processing of a Single 512-bit Block (MD5 Compression Function)

After processing of all 512 bit blocks, a 128 bit message digest is produced, which is a function of all the bits of your message.

The operations of the Functions F, G, H, I can be expressed as follows:

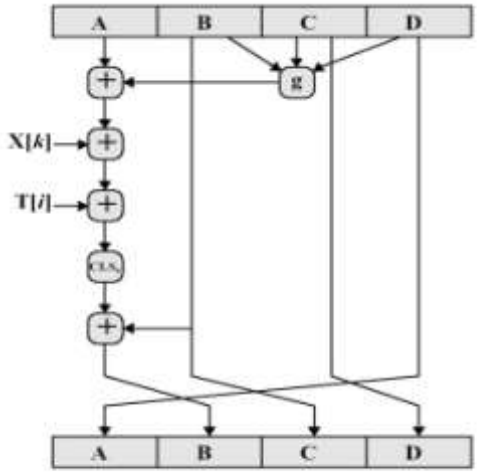


Figure 9.3 Elementary MD5 Operation (single step)

VII. 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 retrieval 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 independently. 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 demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

VIII. ACKNOWLEDGEMENT

First and foremost, we record our sincere thanks to Almighty GOD and our beloved parents who provided us this chance during our tenure in college. We are grateful to our college & **Dr. K. Mani, M.E, PhD**,our beloved principal. We are also thankful to **Mrs. M. Helda Mercy, M.E, PhD** Head of the Department of Information Technology for providing the necessary facilities during the execution of our project work. We also thank for her valuable suggestions, advice, guidance and constructive ideas in each and every step, which was indeed a great need towards the successful completion of the project.

This project would not have been a success without my Internal guide. So, I would extend my deep sense of gratitude to my Internal guide **Mrs. D. Karunkuzhali, Professor**, for the effort she took in guiding me in all the stages of completion of my project work.

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,” inProc. IEEE MILCOM, 2006, pp. 1–6.

[3] M.M.B.Tariq,M.Ammar,andE.Zequra,“Mesage ferry route de-sign for sparse ad hoc networks with mobile nodes,” inProc. ACM MobiHoc, 2006, pp. 37–48.

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

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

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable securefile sharing on untrusted storage,” inProc. Conf. File Storage Technol., 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Medi-ated ciphertext-policy attribute-based encryption and its application,” inProc. WISA, 2009, LNCS 5932, pp. 309–323.

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

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

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

[11] Sahai and B. Waters, "Fuzzy identity-based encryption," inProc. Eurocrypt, 2005, pp. 457–473.

[12] V.Goyal, O.Pandey, A.Sahai,and B. Waters, "Attribute-based en-cryption forfine-grained accesscontrol of encrypted data," inProc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

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

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

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