ISSN 23499842(Online), Volume 1, Special Issue 2(ICITET 15), March 2015
International Journal of Innovative Trends and Emerging Technologies

DECENTRALISED DISRUPTION TOLERANT MILITARY NETWORK FOR RETRIEVAL OF DATA

PARTHIBAN V[1] PRAVEEN KUMAR J[2] RAMPRASANTH R[3] SRIRAM K[4] SARAVANAN A[5] LALITHA R[6]
[1, 2, 3 ,4]UG [Scholar], [5,6]Professor, [1, 2, 3 ,4,5]Department of Computer Science and Engineering,
[1, 2, 3 ,4,5,6]Rajalakshmi Institute of Technology, Chennai, India
[1]parthibanpr143@gmail.com, [2] jpraveenjpkr@gmail.com,
[3]ramprasanth.r.400@gmail.com,[4]ram29483@gmail.com

Abstract— Disruption Tolerant network(DTN) technologies are becoming successful solutions that allow wireless devices carried by soldier to communicate with each other and access the confidential information or commands reliably by exploiting external storage node. The DTN technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. The source and a destination pair has no end to end connections between them, the messages which belong to the source node may need to wait in intermediate nodes for substantial amount of time until the connection would be eventually established. Ciphertext policy ABE(Attribute Based Encryption) provides a scalable way of encrypting data such that encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Digital signature is generated by key authorities which compares the major attributes of the files during decryption process. Signature verification is done to improve the security level.

KEYWORDS: Ciphertext policy ABE , DTN , Digital signature , Signature verification.

I. INTRODUCTION

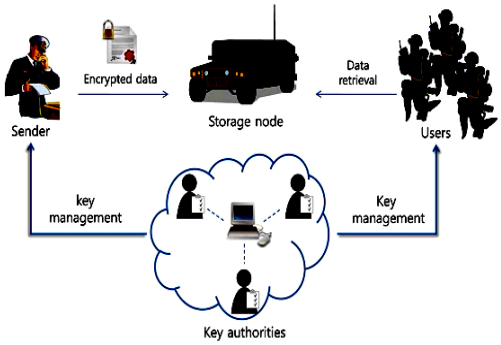
DTN(Disruption Tolerant Network) is designed to provide communication in the most unstable and stressed environments, where the network is subjected to frequent and long lasting disruptions. In this project, ABE (Attribute Based Encryption) algorithm is suggested by using public key encryption , in which the secret key of the user and cipher text depends on the attributes such as location . ABE features a mechanism that enables access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

A. Related Work

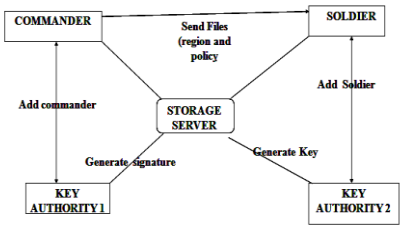
Delay tolerant network is a kind of network architecture in which no continuous path exist between source and destination. DTNs architecture [3] consists of sensor mobile nodes carried by human beings [4], [5], vehicles [6], [7], etc. In military applications, sensor nodes may be implemented in hostile environments such as battlefields to monitor the activities of enemy forces. In these situation, sensor networks may suffer different types of malicious attacks. P. Yang suggested that [2] "Performance Evaluations of Data-Centric Information Retrieval Schemes for DTNs" his paper explores how a content-based information retrieval system can be designed for DTNs. In this paper not much work has been done on designing schemes that provide efficient information access in such challenging network scenarios. S. Roy, M. Chuah suggested that [1]" Secure Data Retrieval Based on Cipher text Policy Attribute-Based Encryption (CP-ABE) System for the DTNs " in this paper Disruption Tolerant Network (DTN) technologies are designed to enable nodes in stressed and unstable environments to communicate with one another. Here, the level of security is low due to lack of digital signature verification. Huang and Roy 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.

II. ARCHITECTURE

Existing Architecture



Proposed Workflow



A. System Description and Assumptions

The architecture consists of the following system entities.

1) Key Authorities: They are key generation centres 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.

2) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. 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.

B. Threat Model and Security Requirements

Data confidentiality**:** Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

Collusion-resistance**:** If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone.

Backward and forward Secrecy**:** In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

III. Proposed Scheme

This paper work proposes the Cipher text-Policy ABE (CP-ABE) which provides a scalable way of encrypting data . The encryptor defines the attribute set that the descriptor needs to possess in order to decrypt the cipher text. Provides three tier security.

Signature verification is done to improve the security level. The master public/private key pair is given by .

1)Local Key Authorities : The master public/private key pair is given by,

2) Key Generation: The proposed key generation protocol is composed of the personal key generation followed by the attribute key generation protocols and a digital signature. It exploits arithmetic secure 2PC protocol to eliminate the key escrow problem such that none of the authorities can determine the whole key components of users individually.

Personal Key Generation: The central authority and each local authority are involved in the following protocol. For brevity, the knowledge of proofs are omitted below.

1) When authenticates a user , it selects random exponents for every local authority and sets . This value is a personalized and unique secret to the user, which should be consistent for any further attribute additions to the user. Then, and each engage in a secure 2PC protocol, where 's private input is , and 's private input is . The secure 2PC protocol returns a private output to . This can be done via a general secure 2PC protocol for a simple arithmetic computation. Alternatively, we can do this more efficiently using the construction in.

2) randomly picks . Then, it computes and sends it.

3) then computes and sends it.

4) outputs a personalized key component and sends it to the user securely. Then, the user computes its personal key component .

3) Data Encryption: When a sender wants to deliver its confidential data , the user defines the tree access structure over the universe of attributes , encrypts the data under to enforce attribute-based access control on the data, and stores it into the storage node. The encryption algorithm chooses a polynomial for each node in the tree . These polynomials are chosen in a top down manner, starting from the root node .

4) Data Decryption: When a user receives the ciphertext from the storage node, the user decrypts the ciphertext with its secret key. The algorithm performs in a recursive way. We first define a recursive algorithm that takes as inputs a ciphertext, a private key , which is associated with a set of attributes, and a node from the tree .

It outputs a group element of or . Without loss of generality, we suppose that a user performs the decryption algorithm. If is a leaf node, then define as follows. If , then (1) If , we define. We now consider the recursive case when is a non- leaf node. The algorithm then proceeds as follows. For all nodes that are children of , it calls and stores the output as . Let be an arbitrary -sized set of child nodes such that . If no such set exists, then the node was not satisfied and the function returns . Otherwise, we compute where (2) and return the result. The decryption algorithm begins by calling the function on the root node of the access tree. We observe that if the tree is satisfied by for all . When we set, the algorithm 0decrypts the ciphertext by computing .

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 is qualified with different attributes.

D. Key Update

When a user comes to hold or drop an attribute, the corresponding key should be updated to prevent the user from accessing 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.

IV. SECURITY

Data confidentiality**:** Unauthorized access from the storage node or key authorities should also be prevented.

Collusion-resistance**:** If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone.

Backward and forward Secrecy**:** In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute.

V.EXPERIMENTAL-SETUP

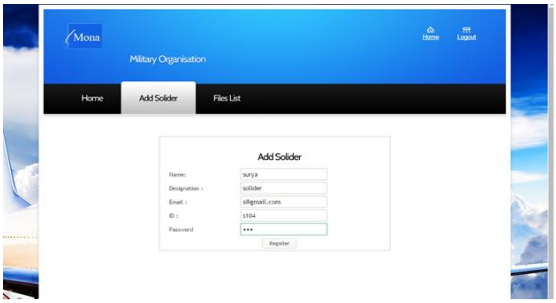


fig1:Adding soldiers

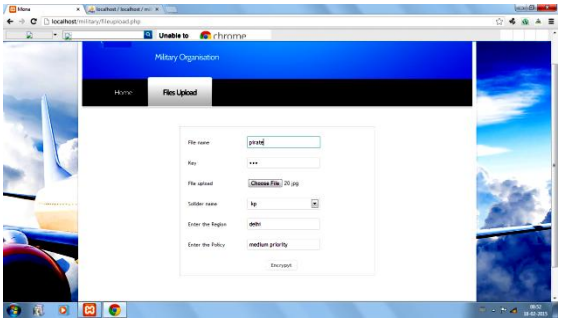


fig2: uploading file

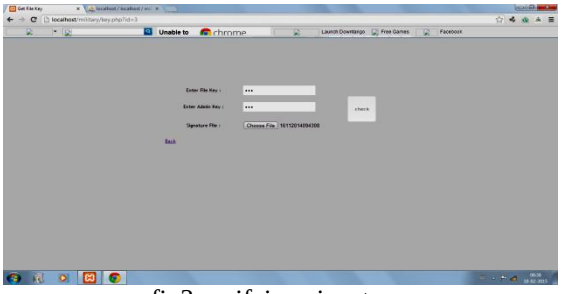


fig3:verifying signature.

VI. CONCLUSION

To secure the file transaction in military networks in this paper by providing a 3-tier security system using a public key, private key and a signature.

By using this digital signature verification, it eliminates hacker interruption as it will prevent the hacker from gaining access to the file even if the signature file is compromised

REFERENCES

[1] “Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks” IEEE transactions on networking accessed 2014

[2]"Evaluations of Data-Centric Information Retrieval Schemes for DTNs" in 2007 by P. Yang.

[3] K Fall,” A Delay-Tolerant Network Architecture for Challenged Internets”,Proc. ACM SIGCOMM ,pp.27-34,2003

[4] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, “Pocket Switched Networks and Human Mobility in Conference Environments,” Proc. ACM SIGCOMM, 2005.

[5] M. Motani, V. Srinivasan, and P. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. MobiCom, pp. 243-257, 2005.
[6] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006
[7] Qinghua Li, Wei Gao, Sencun Zhu, Guohong Cao " A routing protocol for socially selfish Delay Tolerant network" June 23 2011
[8] "The Pairing-Based Cryptography Library," Accessed Aug. 2010 [Online].
Available: http://crypto.stanford.edu/pbc/
[9] "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," by N. Chen, M. Gerla, D. Huang, and X. Hong in Proc. Ad Hoc Netw. Workshop, 2010
[10] "Attribute based data sharing with attribute revocation," by S. Yu, C. Wang, K. Ren, and W. Lou in Proc. ASIACCS, 2010, pp. 261–270.
[11] "Mediated ciphertext-policy attribute-based encryption and its application," by L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker in Proc. WISA, 2009, LNCS 5932, pp. 309–323.
[12] "Decentralizing attribute-based encryption," by A. Lewko and B. Waters Cryptology ePrint Archive: Rep. 2010/351, 2010.