International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Security Evaluation Of Pattern Classifiers Under Attack

[1] B Soundarya [2] Sai Manogna, [3] Prasad B
[1]II/IV, [2][3]Associate Professor
[1][2][3] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM) Hyderabad
[1] beldesoundarya@gmail.com[2] manognasai@gmail.com [3]bprasad@gmail.com

Abstract **Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. 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. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.**

Keywords: **Disruption-tolerant network, Cipher text-policy, Attribute based encryption**

I. INTRODUCTION

In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. 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.DTN architecture may be referred as 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 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, ciphertext-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. 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 attribute is 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 associated attribute 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.

II. SYSTEM ANALYSIS

2.1 Existing System

The idea of Attribute based encryption (ABE) is a guaranteeing approach that satisfies the prerequisites for secure information recovery in DTNs. ABE characteristics a system that empowers a right to

gain entrance control over scrambled information utilizing access approaches and credited qualities among private keys and ciphertexts. The issue of applying the ABE to DTNs presents a few security and protection challenges. Since a few clients may change their related qualities sooner or later (for instance, moving their district), or some private keys may be traded off, key repudiation (or redesign) for each one characteristic is fundamental keeping in mind the end goal to make frameworks secure. This infers that renouncement of any property or any single client in a characteristic gathering would influence alternate clients in the gathering. Case inpoint, if a client joins or leaves a trait assemble, the related characteristic key ought to be changed and redistributed to the various parts in the same gathering for retrograde or forward mystery. It may bring about bottleneck amid rekeying method or security corruption because of the windows of powerlessness if the past characteristic key is not overhauled quickly.

2.2 Limitation of existing system

The issue of applying the ABE to DTNs presents a few security and protection challenges. Since a few clients may change their related properties sooner or later (for instance, moving their area), or some private keys may be bargained, key renouncement (or upgrade) for each one trait is fundamental with a specific end goal to make frameworks secure. However, this issue is significantly more troublesome, particularly in ABE frameworks, since each one characteristic is possibly imparted by different clients (hereafter, we allude to such a gathering of clients as a quality gathering). Another test is the key escrow issue. In CP-ABE, the key power creates private keys of clients by applying the power's expert mystery keys to clients' related set of properties. iv) The last test is the coordination of traits issued from distinctive powers. At the point when various powers oversee and issue ascribes keys to clients freely with their expert mysteries, it is tricky to characterize fine-grained access arrangements over traits issued from distinctive powers.

2.3 Proposed System

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate 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 resolved 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 performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

2.4 Advantages

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 cipher text by combining their attributes even if each of the users cannot decrypt the cipher text 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.

2.5 Challenges

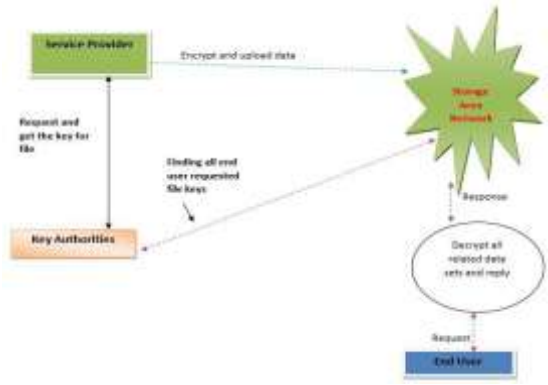

Fig 1: Overall Design of the system

The problem of applying CP-ABE in decentralized disruption tolerant networks introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities.

III. SYSTEM DESIGN

System design is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The system design stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

***Modules Description*:**
Modules description consists of KeyAuthorities, Storage Nodes, Sender, User, CP-ABE Method

A. 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.

B. Storage Nodes

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 semitrusted, that is honest-but-curious.

C. 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 (attributebased) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

D. Users

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 ciphertext 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).

E. CP-ABE Method

In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor. This techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

IV. FUNCTIONING OF THE SYSTEM

4.1 Key Powers

They are key era focuses that create open/mystery parameters for CP-ABE. The key powers comprise of a focal power and numerous neighbourhood powers. We accept that there are secure and dependable correspondence channels between a focal power and

every neighbourhood power amid the starting key setup and era stage. Every neighbourhood power oversees diverse characteristics and issues relating credit keys to clients. They give differential access rights to individual clients focused around the clients' traits. The key powers are thought frankly however inquisitive. That is, they will sincerely execute the allotted undertakings in the framework; nonetheless they might want to learn data of scrambled substance however much as could reasonably be expected. Storage Nodes: This is a substance that stores information from senders and give comparing access to clients. It might be portable or static. Like the past plans, we additionally expect the capacity hub to be semi assumed that is fair yet inquisitive.

4.2 Sender

This is an element who claims private messages or information (e.g., a commandant) and wishes to store them into the outer information stockpiling hub for simplicity of imparting or for dependable conveyance to clients in the amazing systems administration situations. A sender is in charge of characterizing (characteristic based) access arrangement and authorizing it all alone information by scrambling the information under the strategy before putting away it to the stockpiling hub.

4.3 Clients

This is a versatile hub that needs to get to the information put away at the stockpiling hub (e.g., a fighter). In the event that a client has a set of properties fulfilling the right to gain entrance approach of the encoded information characterized by the sender, and is not disavowed in any of the qualities, then he will have the capacity to decode the ciphertext and get the information. CP-ABE Policy: In Ciphertext Approach Quality based Encryption plot, the encryptors can alter the arrangement, who can decode the scrambled message. The strategy could be structured with the assistance of characteristics. In CP-ABE, access arrangement is sent alongside the ciphertext. We propose a system in which the right to gain entrance approach require not be sent alongside the ciphertext, by which we have the capacity safeguard the security of the encryptor. This methods encoded information might be kept classified regardless of the fact that the stockpiling server is untrusted; besides, our techniques are secure against intrigue assaults. Past Characteristic Based Encryption frameworks utilized credits to portray the encoded information and incorporated arrangements with client's keys; while in our framework ascribes are utilized to depict a client's qualifications, and a gathering encoding information decides an arrangement for who can unscramble.

V. IMPLEMENTATION

Fig 2: Registration

Fig 3: Input

Fig 4: Message

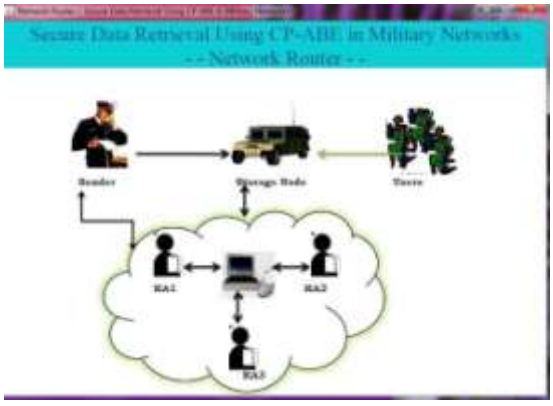

Fig 5: Network Router

Fig 2,3,4 allows new user to register into the system which asks to provide IP address and shows a confirmation window that the registration was successful.

Fig 6: Sender

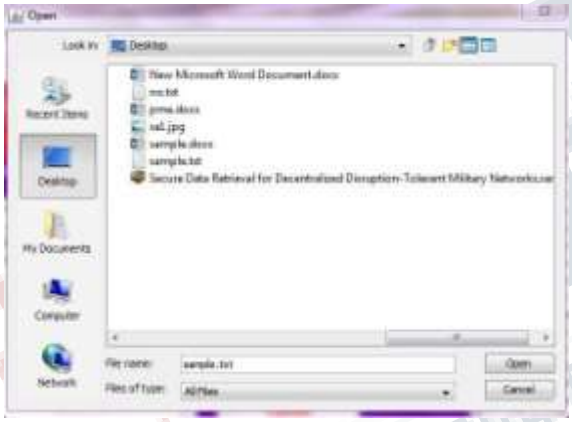

Fig 7: Browsing of a File

Fig 6,7,8 windows allows sender to browse and select the files from the desired locations.

Fig 8: Window showing the file after browsing it from the desired location

Fig 9 shows the browsed message is encrypted using the encryption techniques.

Fig 9: Encryption of message

Fig 10: IP address Input

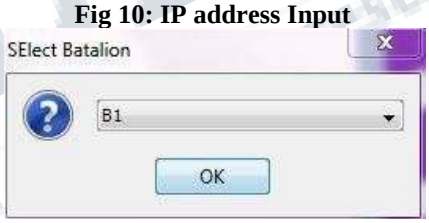

Fig 11 : Selection of Batalion

Fig 12 : selection of Region

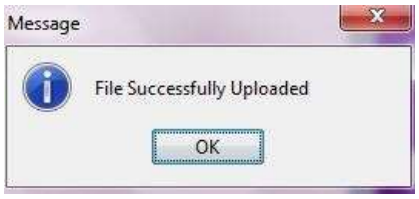

Fig 13: Message showing the successful upload of file

Fig 10,11,12,13shows the windows which asks for storage node's IP address to upload the files and also the windows asking to select battalion and region.

After selection showing the successful upload message.

Fig 14: Key Authority Window

Fig 15: Window that shows the privileges

Fig 16: Window the shows the keys

Fig 14,15,16,17 Windows showing the key authorities where the users, privilages and keys of each user can be viewed.

Fig 18,19 shows the end user can log into his personal account and view the message by providing the user name and password.

Fig 20, 21 shoes the window which provides the access to the required user and also a message showing the successful granting of access.

Fig 17: Storage Nodes.

Fig 18: End User Login

Fig 19: After logging into the End user window

Fig 20: Access Priviliges

Fig 21: Window showing the granted access to the user

Fig 22: End user

Fig 23: End user receiving the message successfully

Fig 22, 23 shoes the end user can receive files by providing the secret key.

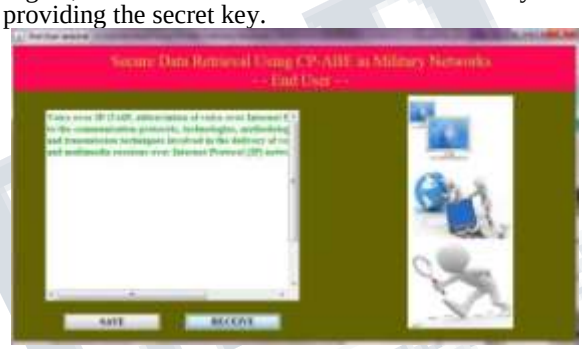

Fig 24: End user after receiving the file and viewing it

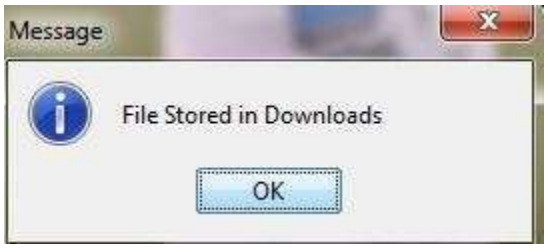

Fig 25: After clicking SAVE button the file is stored in the downloads

Fig 24,25 shows the end user can view and download the files required.

VI. 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 project, 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 compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We also provide security in storage node in which the data in the storage node can be retrieved securely and efficiently. We also use some standard key generation algorithms in key authorities for generating the key.

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," in Proc. IEEE MILCOM, 2006, pp. 1–6.

[**3]** M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37–48.

[4] S. Roy andM. 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," in Proc. IEEE MILCOM, 2007, pp. 1–7

[6] 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.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in Proc. 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 encryption," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement 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] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473.

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

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334. 38

[14] 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.

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