International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 5; Issue: 6; June-2016

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in Disruption Tolerant Military Network

Manjunath Danki[1], Jyothi Patil[2]
[1]PG Student, Department of Computer Science and Engineering,
[2]Professor, Department of Computer Science and Engineering,
Poojya Doddappa Appa College of Engineering, Kalaburagi, Karnataka, India

***Abstract*— In the large number of outgrowing commercial environment each and everything depends on the other sources to transmit the data securely and maintain the data as well in the regular medium. Portable nodes in military environments, for example, a front line or an antagonistic area are prone to experience the undergo of irregular system network and frequent partitions. Disruption-tolerant network (DTN) innovations are getting to be fruitful results that permit remote device conveyed by officers to speak with one another and access the confidential data or secret data or summon dependably by abusing outside capacity nodes or storage nodes. Thus a new methodology is introduced to provide successful communication between each other as well as access the confidential information provided by some major authorities like commander or other superiors. The methodology is called Disruption-Tolerant Network (DTN). This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases. The most promising cryptographic solution is introduced to control the access issues called Cipher text Policy Attribute Based Encryption (CP-ABE). Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext -policy attribute-based encryption (CP-ABE) is a guaranteeing cryptographic answer for the right to gain entrance 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 safely and proficiently deal with the classified information dispersed in the Interruption or disruption tolerant network .**

***Keywords*— Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.**

I. INTRODUCTION

The design of the current Internet service models is based on a few assumptions such as (a) the existence of an end to-end path between a source and destination pair, and (b) low round-trip latency between any node pair. However, these assumptions do not hold in some emerging networks. Some examples are: (i) battlefield ad-hoc networks in which wireless devices carried by soldiers operate in hostile environments where jamming, environmental factors and mobility may cause temporary disconnections, and (ii) vehicular ad-hoc networks where buses are equipped with wireless modems and have intermittent RF connectivity with one another.

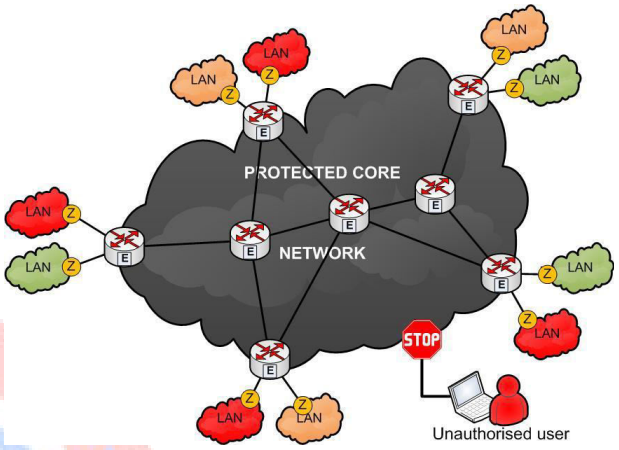

Fig.1. Military Networks

In the above scenarios, an end-to-end path between a source and a destination pair may not always exist where the links between intermediate nodes may be opportunistic ,predictably connectable, or periodically connected. To allow nodes to communicate with each other in these extreme networking environments, Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other. 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. After the connection is eventually established, the message is delivered to the destination node.

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. A requirement in some security-critical applications is to design an access control system to protect the confidential data stored in the storage nodes or contents of the confidential messages routed through the network. As an example, in a battlefield DTN, a storage node may have some confidential information which should be accessed only by a member of „Battalion 6" or a participant in „Mission 3". Several current solutions follow the traditional cryptographic-based approach

where the contents are encrypted before being stored in storage nodes, and the decryption keys are distributed only to authorized users. In such approaches, flexibility and granularity of content access control relies heavily on the underlying cryptographic primitives being used. It is hard to balance between the complexity of key management and the granularity of access control using any solutions that are based on the conventional pair wise key or group key primitives. Thus, we still need to design a scalable solution that can provide fine-grain access control. That is a DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

In this paper, we describe a CP-ABE based encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each user is associated with a set of attributes based on which the user‟s private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt. Our scheme can provide not only fine-grained access control to each content object but also more sophisticated access control antics. Ciphertext-policy attribute-based encryption (CP-ABE) is a guaranteeing cryptographic answer for the right to gain entrance control issues. In any case, the issue of applying CP-ABE in decentralized DTNs presents a few securities and protection challenges as to the property disavowal, key escrow, and coordination of characteristics issued from distinctive powers.

II. Related Work

ABE comes in two flavors called key-policy ABE (KP-ABE) and Ciphertextpolicy attribute-based encryption. In KP-ABE, the encryptor just gets to name a ciphertext with a set of attributes. the key power picks an approach for each one client that figures out which ciphertexts he can unscramble and issues the way to every client by inserting the strategy into the client's key. However, the parts of the ciphertexts and keys are turned around in CP-ABE.in CP-ABE, the ciphertext is encoded with a right to gain entrance arrangement picked by an encryptor, however a key is just made concerning a qualities set. CP-ABE is more proper to DTNs than KP-ABE in light of the fact that it empowers encryptors, for example, an officer to pick a right to gain entrance arrangement on credits and to encode secret information under the right to gain entrance structure by means of encoding with the comparing open keys or properties [4], [7], [15].

1) *Trait Disavowal*: Bettencourt et al. [16] initially recommended key disavowal instruments in CP-ABE and KP-ABE, individually. Their answers are to affix to each one characteristic a termination date (or time) and disperse another set of keys to substantial clients after the close. The occasional property revocable ABE plans [8], [13], [16], [17] have two primary issues. The principal issue is the security corruption regarding the retrograde and forward mystery [18]. It is a respectable situation that clients, for example, fighters may change their qualities frequently,e.g., position or area move when considering these as characteristics [4], [9]. At that point, a client who recently holds the credit may have the capacity to get to the past information encoded before he gets the quality until the information is re- encrypted with the recently upgraded characteristic keys by occasional rekeying (regressive secrecy).for sample, expect that at a time, a ciphertext is scrambled with an approach that might be unscrambled with a set of qualities (implanted in the clients keys) for clients with . After time, say, a client recently holds the quality set. Regardless of the possibility that the new client ought to be refused to decode the ciphertext for the time example, he can at present unscramble the past ciphertext until it is re-encrypted with the recently upgraded quality keys. Then again, a renounced client would in any case have the capacity to get to the scrambled information regardless of the possibility that he doesn't hold the quality any more until the following lapse time.

III. System Design

i. 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.

- **Limitation of existing system:**

i) 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.

ii) 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) iii) 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.

ii. 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.

- **Advantages:**

i) 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. ii) 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.

iii)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.

- **Challenges:**

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.

IV. SYSTEM ARCHITECTURE

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

Fig.2 shows the architecture of the DTN. As shown in Fig.2 the architecture consists of the following system entities.

1) 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.

2) 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

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) 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).

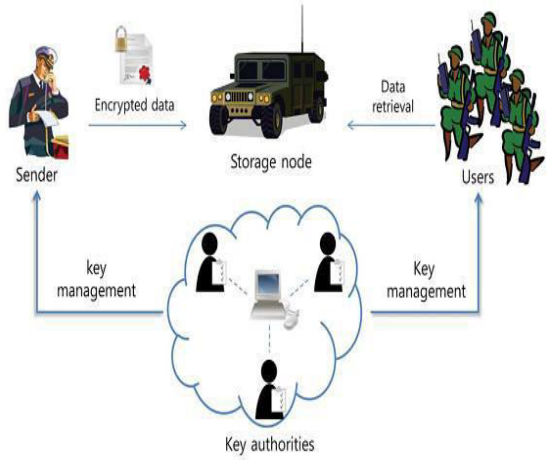

Fig.2 System Architecture

V. FUNCTIONING OF SYSTEM

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 neighborhood powers. We accept that there are secure and dependable correspondence channels between a focal power and every neighborhood power amid the starting key setup and era stage. Every neighborhood 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.

Sender: This is an element which 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.

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.

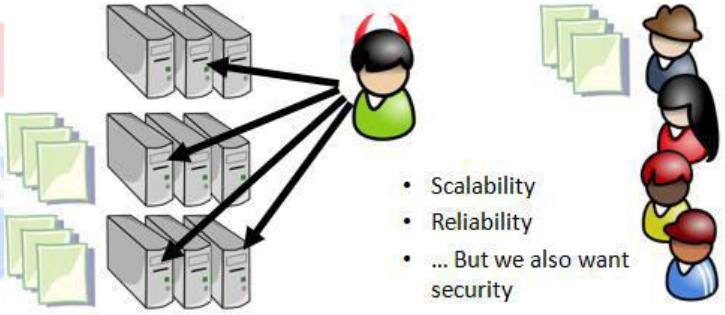

Fig.3Remote File Storage: Interesting Challenges

So one factor we have a tendency to do all time is store our files on remote servers. There are varieties of reasons why we have a tendency to do this. we have a tendency to might want to supply scalable access to our files to others victimization further resources on the market elsewhere.-- we have a tendency to might want a lot of dependability just in case of failures. During this case we have a tendency to might want to duplicate our files totally different information centers or with different organizations. However we would like security. We have a tendency to could have needs on World Health Organization will access that files. The fascinating factor is, there's a tension between security and therefore the alternative properties. The lot of we have a tendency to replicate our files, the lot of we have a tendency to introduce potential points of compromise and therefore the lot of trust we have a tendency to need. It's this tension that makes this type of drawback fascinating, and provides a context within which CP-ABE is also helpful.

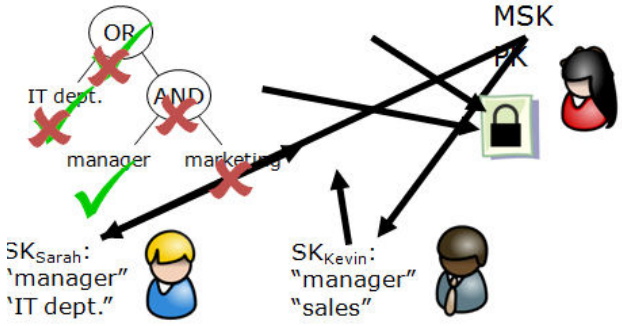

Fig.4 Access Control via Cp ABE

Point out that attributes of secret key are mathematically incorporated into the key itself, after file is encrypted; say we put it on the server. Explain that now; the policy checking happens "inside the crypto". That is, nobody explicitly evaluates the policies and makes an access decision. Instead, if the policy is satisfied, decryption will just work, otherwise it won't.

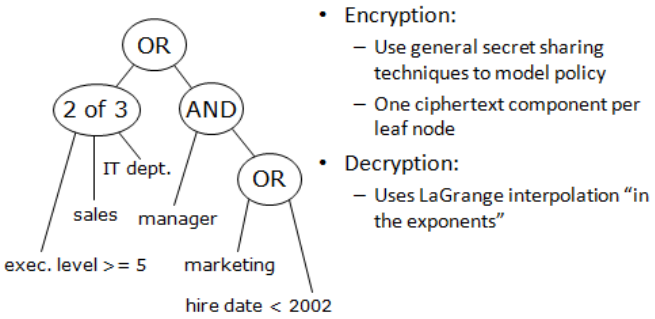

Fig 5 Highlights from Our Scheme: Encryption and Decryption

VI. CONCLUSIONS

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

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.