Comparitive Study on Secure Data Retrieval Framework for Military Networks

C Krithina Thimmaiah
PG Student, CSE Dept
Cambridge Institute of Technology
Bangalore, India.
E-mail: krithina.thimmaiah@gmail.com

Sandeep Kumar
Associate Prof. and HOD, ISE Dept
Cambridge Institute of Technology
Bangalore, India.
E-mail: hod.ise@citech.edu.in

Abstract— In the immensely colossal 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 conventional medium. Portable nodes in military environments, for example, a front line or an antagonistic area are prone to experience the undergo of eccentric system network and frequent partitions. Disruption-tolerant network (DTN) innovations are getting to be fruitful results that sanction remote contrivance conveyed by officers to verbalize with one another and access the confidential data or secret data or summon dependably by abusing outside capacity nodes or storage nodes. Thus an incipient methodology is introduced to provide prosperous communication between each other as well as access the confidential information provided by some major ascendant entities like commander or other superiors. The methodology is called Disruption-Tolerant Network (DTN). This system provides efficient scenario for sanction 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 Predicated Encryption (CP-ABE). Some of the most challenging issues in this scenario are the enforcement of sanction policies and the policies update for secure data retrieval. Ciphertext - policy attribute-predicated encryption (CP-ABE) is a assuring cryptographic answer for the right to gain ingress control issues. However, the quandary 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 ascendant entities. In this paper, we propose a secure data retrieval scheme utilizing CP-ABE for decentralized DTNs where multiple key ascendant entities manage their attributes independently..We demonstrate how to apply the proposed mechanism to safely and proficiently deal with the relegated information dispersed in the Interruption or disruption tolerant network

Keywords — *Disruption-tolerant network(DTN), Ciper text Policy Attribute Predicated Encryption (CP-ABE), Encryption.*

*****

I. INTRODUCTION

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

In the above scenarios, a terminus-to-end path between a source and a destination pair may not always subsist where the links between intermediate nodes may be opportunistic ,predictably connectable, or periodically connected. To sanction nodes to communicate with each other in these extreme networking environments, Disruption-tolerant network (DTN) technologies are becoming prosperous solutions that sanction nodes to communicate with each other [1]-[3].Typically ,when there is no terminus-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 duration until the connection would be eventually established. After the connection is eventually established, the message is distributed to the destination node.

Roy and Chuah introduced storage nodes in DTNs where data is stored or replicated such that only sanctioned mobile nodes can access the obligatory information expeditiously and efficiently. A requisite in some security-critical applications is to design an access control system to bulwark 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 afore being stored in storage nodes, and the decryption keys are distributed only to sanctioned users. In such approaches, flexibility and granularity of content access control relies heavily on the underlying cryptographic primitives being utilized. It is hard to balance between the intricacy of key management and the granularity of access control utilizing any solutions that are predicated on the conventional pair sapient 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 ascendant entities issue and manage their own attribute keys independently as a decentralized DTN. In this paper, we describe a CP-ABE

predicated encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each utilizer is associated with a set of attributes predicated on which the user‟s private key is engendered. 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 finegrained access control to each content object but additionally more sophisticated access control antics. Ciphertextpolicy attribute-predicated encryption (CP-ABE) is a assuring cryptographic answer for the right to gain ingress control issues. In any case, the issue of applying CP-ABE in decentralized DTNs presents a few securities and bulwark challenges as to the property disavowal, key escrow, and coordination of characteristics issued from distinctive potencies.

II. SYSTEM-DESIGN

i. Subsisting System: The conception of Attribute predicated encryption (ABE) [6]- [9] is a ensuring approach that gratifies the prerequisites for secure information recuperation in DTNs. ABE characteristics a system that empowers a right to gain ingression 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 bulwark challenges. Since a few clients may transmute their cognate 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 terminus goal to make frameworks secure. This infers that renouncement of any property or any single client in a characteristic amassing would influence alternate clients in the accumulation. Case inpoint, if a client joins or leaves a trait assemble, the cognate characteristic key ought to be transmuted and redistributed to the sundry components in the same amassing for retrograde or forward mystery. It may establish bottleneck amid rekeying method or security corruption because of the windows of powerlessness if the past characteristic key is not overhauled expeditiously.

.i.Limitation of subsisting system: i) The issue of applying the ABE to DTNs presents a few security and auspice challenges. Since a few clients may transmute their cognate 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 categorical end goal to make frameworks secure. ii) However, this issue is significantly more onerous, particularly in ABE frameworks, since each one characteristic is possibly imparted by

different clients (hereafter, we allude to such an accumulation of clients as a quality amassing) iii) Another test is the key escrow issue. In CP-ABE, the key power engenders private keys of clients by applying the puissance's expert mystery keys to clients' cognate set of properties. iv) The last test is the coordination of traits issued from distinctive potencies. At the point when sundry powers oversee and issue ascribes keys to clients liberatingly with their expert mysteries, it is tricky to characterize fine-grained access arrangements over traits issued from distinctive potencies.

III. PROPOSED SYSTEM

In this paper, we propose an attribute-predicated secure data retrieval scheme utilizing CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances rearward/forward secrecy of confidential data by reducing the windows of susceptibility. Second, encryptors can define a finegrained access policy utilizing any monotone access structure under attributes issued from any culled set of ascendant entities. Third, the key escrow quandary is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol engenders and issues utilizer secret keys by performing a secure twoparty computation (2PC) protocol among the key ascendant entities with their own master secrets. The 2PC protocol deters the key ascendant entities from obtaining any master secret information of each other such that none of them could engender the whole set of utilizer keys alone. Thus, users are not required to plenarily trust the ascendant entities in order to bulwark their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key ascendant entities or data storage nodes in the proposed scheme.

ii.iAdvantages: i) Data confidentiality: Unauthorized users who do not have enough credentials satiating the access policy should be deterred from accessing the plain data in the storage node. In integration, unauthorized access from the storage node or key ascendant entities should be additionally averted. ii) Collusion-resistance: If multiple users collude, they may be able to decrypt a ciphertext by cumulating their attributes even if each of the users cannot decrypt the ciphertext alone. iii)Rearward and forward Secrecy: In the context of ABE, rearward secrecy betokens that any utilizer who comes to hold an attribute (that slakes the access policy) should be obviated from accessing the plaintext of the anterior data exchanged afore he holds the attribute. On the other hand, forwardpolicy and enforcing it on its own data by encrypting the data under the policy afore 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 utilizer possesses a set of attributes gratifying 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 ascendant entities 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 scarcely contradictory requisite, the central ascendancy and the local ascendant entities 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 obviates them from kenning each other‟s master secrets so that none of them can engender the whole set of secret keys of users individually. Thus, we take a posit that the central ascendancy does not collude with the local ascendant entities (otherwise, they can conjecture the secret keys of every utilizer by sharing their master secrets).

IV. FUNCTIONING OF SYSTEM

: Key Powes: They are key era focuses that engender open/mystery parameters for CP-ABE. The key powers comprise of a focal power and numerous neighborhood potencies. We accept that there are secure and dependable correspondence channels between a focal power and every neighborhood power amid the commencement 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 plausibly 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 adscititiously expect the capacity hub to be semiassumed that is fair yet inquisitive. 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 astounding systems administration situations. A sender is in charge of characterizing (characteristic predicated) access arrangement and sanctioning it all solitary information

secrecy denotes that any utilizer who drops an attribute should be obviated from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satiate the access policy.

ii.ii.Challenges: The quandary 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 ascendant entities.

V. SYSTEM ARCHITECTURE

The fig1 shows the general architecture of secure data retrieval in a disruption-tolerant military networks. As shown in fig1 the architecture consists of the following four system entities.

1) Key Authorities: This entity generate public and secret keys for CP-ABE.the key owner has the central authority and multiple local authorities.
2) Storage node: This is an entity which act as an storage for the data from senders and provide corresponding authorization to user. It can be mobile or static[4], [5].
3) Sender: This is an entity who have secrete messages and data and stores them in an storage node for data sharing
4) User: This is a mobile node which access the data which is stored at storage node. If user provides attributes that satisfy the policy of the cipher text by the sender, then he will be able to decrypt the cipher text and obtain the original data

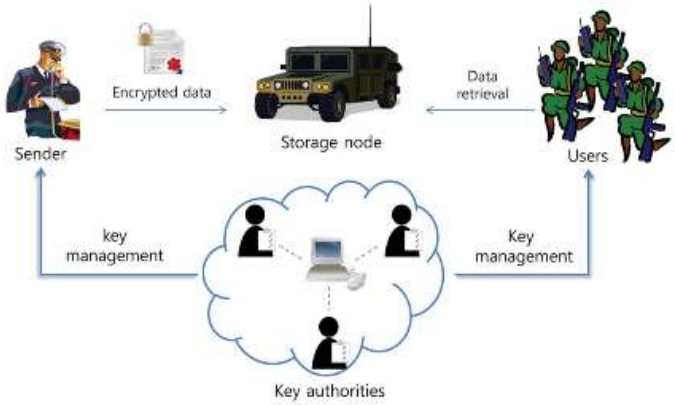

Fig. 1. Architecture of secure data retrieval in a disruption-tolerant military network.

VI. LITERATURE SURVEY

Literature survey is the most consequential step in software development process. Afore developing the implement it is obligatory to determine the time factor, economy n company vigor. Once these things r gratified, then next steps is to determine which operating system and language can be utilized for developing the implement. Once the programmers start building the implement the programmers need lot of external support. This fortification can be obtained from senior programmers, from book or from websites. Afore building the system the above consideration r taken into account for developing the proposed system.

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CPABE). In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes. The key ascendancy culls a policy for each utilizer that determines which ciphertexts he can decrypt and issues the key to each utilizer by embedding the policy into the

user‟s key. However, the roles of the ciphertexts and keys are inverted in CP-ABE. In CP-ABE, the ciphertext is encrypted with an access policy culled by an encryptor, but a key is simply engendered with deference to an attributes set. CP-ABE is more congruous to DTNs than KP-ABE because it enables encryptors such as a commander to cull an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes.

VII. CONCLUSION

DTN technology are being used in military which allow wireless devices to communicate with each other and access confidential information by exploiting external storage nodes. CP-ABE is a efficient method to access control and secure data retrieval issue .In this paper we introduce secure and efficient frame work using CP-ABE for decentralized DTN where different key authorities will be able to manage there attributes independently. The inherent key ESCROW problem is solved by providing confidentiality to the data stored under the hostile environment where key authorities might be not be fully trusted.

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 design for sparse ad hoc networks with mobile nodes,” in Proc. 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] A. Sahai and B. Waters, “Fuzzy identity-basedencryption,” in Proc.Eurocrypt, 2005, pp. 457–473.

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

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

[9] 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.