International Journal of Science Engineering and Advance Technology

Protected data retrieval System using CP-ABE for decentralized Tolerant Networks (DTNs) where many key authorities manage their attributes separately

V. Siva mallikarjunarao[1], K.Jhon Paul[2]
[1]M.Tech (SE), Nova College of Engineering and Technology, A.P., India.
[2]Associative Professor, Dept. of Computer Science & Engineering, Nova College of Engineering and Technology, A.P., India..

Abstract
The Hostile Military situations like war zone and antagonistic systems work in specially appointed mode and they endure confined system network. Arrangement of Disruption-tolerant systems (DTN) improves the network between remote gadgets conveyed by warriors in combat zone; this gives them to impart viably and offer the data unhesitatingly. Cipertext - arrangement trait based encryption (CP-ABE) is successful cryptographic method to get to control issues. Specially appointed system are decentralized and asset compelled systems, applying CP-ABE to such systems is a testing issue, thus it presents new security and protection issues identified with trait disavowal, coordination of qualities, and key escrow. This paper chiefly concentrate on a protected information accumulation system utilizing CP-ABE for specially appointed DTNs where more than one key power deals with their traits powerfully and freely. We investigated the proposed component and connected to the disturbance tolerant military system to get to the data safely.

Keywords : DTNs, CP-ABE, Ad hoc Network, Key Management.

I. Introduction

Military communication networks are decentralized associated by means of remote gadgets conveyed by warrior, because of some natural components, and portability they are separated, and stuck. To overcome scientists are finding new advances like Disruption-tolerant system (DTN), these systems permits hubs to impart in particular environment conditions [2]–[3]. In multi bounce specially appointed systems information ought to be sent by means of transitional hubs, the information ought to be put away at these hubs ought to be recovered safely until the association is set up in the middle of source and destination. A methodology of capacity of information at hubs which can be gotten to just by approved hubs was proposed by Chuah [4] and Roy [5]. Classification and uprightness ought to be kept up in military application by applying cryptographic methods [6]. Taking into account specially appointed system and antagonistic system highlights it is required to characterize new information approaches taking into account client properties and parts oversaw by distinctive key administration powers. Continuously DTNs can be utilized as a part of military correspondence where an administrator can store and forward the information to specific unit and the main determined brigade can recover the information safely later. In DTN structural planning show in fig 1 we can watch that numerous powers can issue and deal with their own quality key without concentrated power [7]. Next to numerous encryption procedures trait based encryption best suit for DTNs for secure information gathering. The primary element of ABE is it gives access control over information in light of access approaches and qualified characteristics among figure writings and client private keys [8]-[10]. CP-ABE is an adaptable methodology for encryption of information where encryptor characterizes the trait set which decryptor uses to decode the message. So in view of the security strategy distinctive clients are permitted to unscramble diverse bits of information [10].

The real issue with ABE is applying this instrument to DTNs which are decentralized, in the process it may prompt a few protection and security issues. In military systems because of portability of hubs (force from on area to other) may trade off clients private keys, the substitute to this is key renouncement for each characteristic through which it may accomplish security. The new issue is these keys ought to create at whatever point a hub moves starting with one district then onto the next. The other test is key escrow issue. Each key power has an expert mystery key through which all client information can be unscrambled, if there should be an occurrence of key power bargained by aggressors in military correspondence system. This will be not kidding risk for security and information secrecy. At

long last coordination of characteristics issues by diverse key authorities.

II. Related Work

There are two kinds of Attribute Based Encryption (ABE) to be specific Key-approach ABE(KP-ABE) and ciphertext-strategy (CP-ABE). The primary issue with KP-ABE is, just the encryptor gets the mark to figure content with some characteristic set and the key power keeps up some entrance arrangements which are inserted in key issues to the client. This key can be utilized by the beneficiary to unscramble the message. These parts are switched in CP-ABE, the cipertexts is scrambled with an entrance arrangement by encryptor and key is made by an arrangement of qualities. So CP-ABE is more adaptable for DTNs contrasted with KP-ABE [4][11].

Some work has done on CP-ABE and KP-ABE in regards to key disavowal component by andBoldyreva et al and Bethencourtet al [9]. In any case, their answer has a constrained legitimacy of keys and after termination date or time new testaments ought to be issues to substantial client. These intermittent trait recoverable ABE plans have two noteworthy issues.

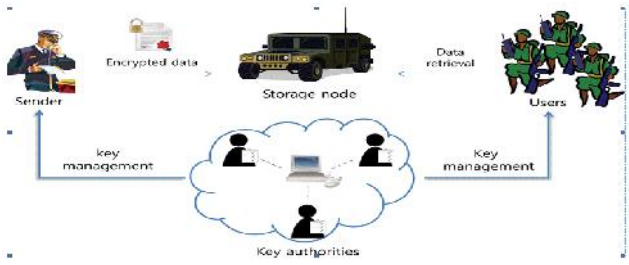
The main is issue with respect to security corruption i.e forward and in reverse mystery and the other is versatility problem.Golleet al.[12]proposed a client revocable KP-ABE instrument, the significant blemish of this plan is it works just if no of traits are half of the universe size.

Pursue et al proposed a disseminated KP-ABE that give answer for key escrow issue in multi power framework. The correspondence overhead of this is plan is O(N2) where N is the no of dominant presences in framework.

Huang et al. proposed a decentralized ABE scheme in multi authority environment. It achieved a combined access policy over attributes issued by various authorities by simple encryption algorithm.

III. System Architecture

The basic DTN architecture is define in Fig 1. Which can be used in DTNs based military network.



The system architecture shown in Fig. 1 has the following aspects.

3.1 Sender: This is where the data transmission begins with encryption of data in real time it may represent a commander who sends the data to its battalion located in different regions. Sender node is only responsible to encrypt the data using its own access policies.

3.2 Storage Node: It is intermediate node which stores the data and provide access to the data when the user is available. Storage node may be static or mobile. This node can also be compromised since it is a semi trusted.

3.3 Key Authorities: these powers produce the keys for both encryption and unscrambling in CP-ABE. It is a blend of focal and nearby powers. we have to accept that there is secure and solid information channel between both the powers amid beginning key era and sharing. The client imparts dto nearby power which approves client and issues credits to the clients. Clients get access based upon the client characteristic qualities.

3.4 Receiver/User beneficiary (warrior) hub can get to the data from the capacity hub (middle of the road hub) which is exchanged by sender hub (officer). Client need to fulfill all the entrance approach of scrambled information to unscramble the figure content.

3.5 Security Architecture: To achieve forward and backward secrecy, data confidentiality and collusion-resistance security architecture is defined as below.

3.6 Backward and forward Secrecy: in reverse mystery implies the client require just to get to the data subsequent to holding the quality issues by key power, the past information cannot be gotten to. Forward mystery implies once the client drops property he ought not have the capacity to get to the figure content until unless the characteristic he holding fulfill the key agreement.

3.7 Data confidentiality: there should be a mechanism where unauthorized users holding access policy should not access the cipher text. It should be prevented and for both user and key authorities.

3.8 Collusion-resistance: multiple users can combine their attributes in case of a single user cant decrypt the message. This may lead to collusion attack, so we need to implement a mechanism so that no two nodes can combine their attributes to decrypt the message.

3.9 Technical Terminology : We propose some basic definition regarding proposed scheme, mainly access structure to define definitions and bi linear map and its security requirements. [12][13]

3.10 Access Structure: Here we assume a set of parties {P1, P2, P3 …. Pn} and a is a monotone if

if⊆C and . where is a nonempty subset {P1, P2, P3….Pn}. so the in are authorized sets and set not in are unauthorized sets.

In proposed scheme the attributes take the role of parties. So an monotype structure is known as access structure.

Bilinear pairings: Let $_0$ and $_1$ be two multiplicative cyclic group of prime order of p. Let g be generator of $_{0.}$ A bilinear map is defines as e: $_0$ x $_{1\quad 1.}$ If e($P^{a,}$ Q^{b}) = e(P,Q)^{ab}for all P, Q $_0$ for all a, b $^{*}{}_{P.}$

IV. Proposed Scheme

The proposed procedure depends on multiauthority CP-ABE component for secure information gathering in DTNs. There are two key issuing powers' to be specific expert key power and neighborhood key issue power. Expert power issues the keys to nearby power and it to its client. The clients need to unscramble the information through characteristics issued by its concerned power. Scaliblity and security are accomplished in proposed plan with usage of element property overhaul. Taking into account first CP-ABE proposed by Bethencourtet al. [13]

Bethencourtet al. [9], a large portion of CP-ABE plans have been proposed [12]–[15]. Every one of these plans depend on Bethencourtet al's. plan, however neglected to accomplish the revelations and phrasing. Confirmations of those plans are investigated however relatively few mimicked. Proposed procedure is based Bethencourtet al's. development keeping in mind the end goal to improve the expressiveness. It has four modules as undernea

4.1 Access Tree :

- Description: For a tree be representing access structure. A threshold gate is maintained for every non leaf node. If a tree x has num_x no of children's then $k_x$is its threshold value then0 $k_x$$num_{x.}$ an attribute is defined for every leaf node and the threshold value is $k_{x\,=}$ 1.
- Fulfilling an Access Tree: Every tree is having a sub tree at some node. Let has a sub tree at node x which is $_{x.}$ we can calculate $_x$ () = 1. Where α is a set of attributes. We can compute $_x$(α) recursively.

4.2 Scheme Development:

To construct the system we need to undergo different steps as below.

4.2.1 **System setup:** In this phase every trusted initializer selects a bilinear map $_0$ which has a prime order of p with generator g based on security parameters. A universal one-way Hash function is selected.

4.2.2 **Central key authority:** It generates the public/private key pair and issues to the local key authorities.

4.2.3 **Local Key authorities:** After receiving the public/private key pair from CA key authority, it is transferred to concern user.

4.2.4 **Key Generation:** In existing approach CP-ABE it consist of multiple attribute keys and single personalized key. To overcome the collusion attack different and unique personalized key is generated for every user. A separate approach for generation of personal key is composed in proposed solution.

Personal/unique Key Generation Protocol:

The personal key authority and local key authority are responsible in generation of personal key for a user.

Algorithm Unique key generation:

Step 1: CA communicates with user and authenticates it. Every user is assigned with a unique random exponent with respect to every local authority. With the above values it generates $r_{t\ value}$ for every local authority L1, L2, L3…..Ln L. This $r_{t\ value}$ is unique and secret to the user.

Step 2: Local authority Li randomly picks and computes T value and sends it to CA.

Step 3: CA then computes M value and sends it to the Li.

Step 4: Li results a unique key component Fi and sends it to the user Ut.
User then computes its personal key for encryption.

Attribute Key: Attribute keys are generated by the local authority Li once the unique key component is generated.

Algorithm for attribute generation:

Step 1: CA picks a random value and generates attribute r' and sends it to Li and user.

Step 2: Li takes set of attributes generated by CA and generates keys for user and transfer rj to each user.

- Encryption: when a sender wishes to send some private information to the recipient he chooses a fitting encryption calculation and uses the characteristics produced by the focal power and issued by neighborhood power.

- Decrypt: When collector gets the ciper content Cp from capacity hub it utilizes the characteristic M created by neighborhood power Li and uses its remarkable key and unscrambles the

figure tectcp to plaintext. A productive decoding calculation is utilized by decryp

Revocation: whenever a key is changed by the user then all the local authorities should be updated with the newly assigned key which is generated by the CA. problem with this mechanism is that it may generate more overhead in terms of computation and communication cost. The alternate to this problem is to re-encrypt the attribute value and validate it and share it with local authorities and user.

V. Analysis:

The proposed technique is compared with the existing CP-ABE schemes and it shows that the poposed algorithm is dynamic in terms of all the phases of Cp-Abe than others.

Table 1 comparative analysis of CP-ABE for DTN with other approaches.

Scheme	Authority	Revocation	Expressiveness
BSW	Single	Periodic	---
HV	Multiple	Periodic	AND
RC	Multiple	immediate	AND
proposed	Multiple	immediate	Any monotone Access structure

Efficiency: The table II provides the comparison cost of various computations like

VI. Conclusion

DTN based correspondence systems are turning out to be more prominent specially appointed systems and are being sent in military applications to permits remote impromptu gadget to convey proficiently. Data ought to be dependably transmitted between the sender and recipient, so key administration assumes an essential part in giving information classification and security. CP-ABE based arrangements are extremely adaptable contrasted with other cryptographic methodologies. In this paper we proposed an effective and adaptable CP-ABE based methodology which can be utilized for secure information gathering as a part of military correspondence arranges that work on DTN advancements.

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. 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.

5. 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.

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

7. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473.

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

9.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.

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

11. S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput.Surv., vol. 35, no. 3, pp. 309–329, 2003.

12. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.

13. V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591.

14. X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in Proc. ASIACCS, 2009, pp. 343–352.

ISSN 2321-6905

Mrs.V.Siva mallikarjuna rao is a student of NOVA College of Engineering & Technology, Vegavaram, Jangareddy gudem. Presently He is pursuing His M.Tech [Software Engineering] from this college and he received her B.Tech from Sri Sarathi college of engineering and technology(SSIET), affiliated to JNT University, Kakinada in the year 2006. His area of interest includes Computer Networks and Object oriented Programming languages and information security, all current trends and techniques in Computer Science.

Mrs.K.Jhon Paul, well known Author and excellent teacher Received M.Tech (CSE) from JNT University, Kakinada.He is working as Associative Professor in Department of Computer science and Engineering , NOVA college of Engineering and Technology. He has 7 years of teaching experience in this college. To His credit couple of publications both national and international conferences /journals . His area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other advances in computer Applications.