IMPLEMENTATION OF SECURE DATA RETRIEVAL SYSTEM FOR DTN NETWORKS

Fatima Nilofar[1], P.Kumaraswamy[2]
[1]M.Tech in SE Dept, [2]Assistant Professor in CSE Dept, Coordinator,
SR ENGINEERING COLLEGE Warangal, ANDHRA PRADESH, INDIA

***Abstract:** In the sizable amount of outgrowing business setting every and everything depends on the opposite sources to transmit the info firmly and maintain the info furthermore within the regular medium. moveable nodes in military environments, for instance, a line or associate antagonistic space square measure liable to expertise the bear of irregular system network and frequent partitions. Disruption-tolerant network (DTN) innovations are becoming to be fruitful results that let remote device sent by officers to talk with each other and access the confidential data or secret information or summon reliably by abusing outside capability nodes or storage nodes. Thus a new methodology is introduced to supply self-made communication between one another furthermore as access the confidential information provided by some major authorities like commander or different superiors. The methodology is termed Disruption-Tolerant Network (DTN). This method provides economical situation for authorization policies and also the policies update for secure information retrieval in most difficult cases. The most promising crypto logic answer is introduced to regulate the access problems known as Cipher text Policy Attribute Based coding (CP-ABE). a number of the foremost difficult problems during this situation square measure the social control of authorization policies and also the policies update for secure information retrieval. Cipher text -policy attribute-based encryption (CP-ABE) may be a guaranteeing crypto logic accounts the proper to realize entrance management problems. However, the matter of applying CP-ABE in redistributed DTNs introduces many security and privacy challenges with relevancy the attribute revocation, key escrow, and coordination of attributes issued from different authorities. During this paper, we tend to propose a secure information retrieval theme exploitation CP-ABE for redistributed DTNs wherever multiple key authorities manage their attributes severally..We demonstrate the way to apply the proposed mechanism to soundly and proficiently wear down the classified data spread within the Interruption or disruption tolerant network.*

I. INTRODUCTION

Mobile In several Military network cases wireless devices connections that is followed by soldier could also be disconnected quickly by association jam, some surroundings factors and quality, in the main once they operate in hostile environments. to speak one another in these extreme networking environments Disruption- tolerant network (DTN) technologies ar resolution for the permit nodes. Once there's no any finish to finish association in between supply and destination combine and massage from supply node might assist intermediate node for a considerable amount of your time till the association would be eventually established. In military applications needed enlarged protection of confidential knowledge with access management methodology that are cryptographically enforced .several of the cases it's fascinating to produce completely different access service like knowledge access policies are outline over the user's attributes and roles, that are managed by the key authorities. as an example, in a disruption-tolerant military network, on the storage node commander might store confidential knowledge that is access by "Battalion A" United Nations agency ar taking part in "Region B." we tend to studies on DNA design for handle multiple problems and independently manage own attribute keys as DTN [10]. The attributes based mostly cryptography is promising approach that is fulfill the need of secure knowledge in DTNs. ABE options a by mistreatment access policies it's mechanism of modify access management over the encrypted knowledge and ascribed attributes among personal keys and cipher texts.

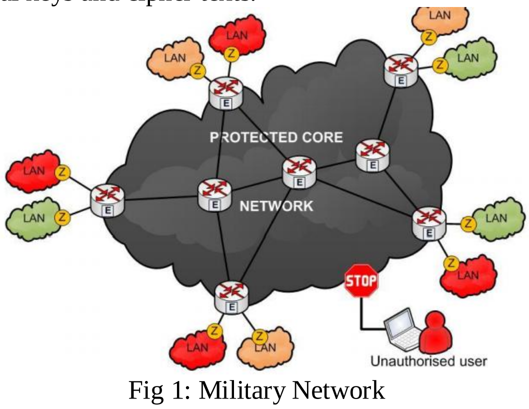


Fig 1: Military Network

one in every of the vital thing is cipher texts-policy ABE (CP-ABE) provided easier method of encrypted knowledge such the encrypted will delineate the attribute keys that to be want method by descriptor and convert into cipher text [13]. but the user will decipher the data on completely different method for security purpose. Hence, the matter of applying the ABE to DTNs introduces many security and privacy challenges. At some purpose some users might amendment their associate attributes like user amendment the region or some personal keys might be compromised, to form system secure key change for every attribute is critical. However, this issue is even tougher, particularly in ABE systems, since every attributes shared by every user as we tend to study multiple teams of users as attribute teams. This defines that revocation of attributes or any single user of attribute cluster will impact on alternative users in cluster. Another challenge is that the key written agreement drawback. In CP-ABE, generate personal key for user by key authorities by applying the authority's master keys to user associated set of attributes. Thus, by making attribute key, specific user will mistreatment key attribute decipher each cipher text. Key attributes once compromised by adversaries this is able to be doubtless threat to the info security or privacy particularly once the info is very sensitive. The every key authority having complete privilege for produce own attribute with own master secrets, the key written agreement is an inherent drawback in multiple authority system. A key generation methodology relies on signal passkey and it's the basic methodology uneven cryptography system because the attribute based mostly or identity-based cryptography protocols, removing escrow in single or multiple-authority CP-ABE could be a polar open drawback. The key written agreement is associate inherent drawback even within the multiple-authority systems as long as every key authority has the whole privilege to come up with their own attribute keys with their own master secrets. Since such a key generation mechanism supported the one master secret is that the basic methodology for many of the uneven cryptography systems such as the attribute- based mostly or identity-based cryptography protocols, removing written agreement in single or multiple-authority CP-ABE is a polar open drawback.

II. PROBLEM STATEMENT

The idea of Attribute primarily based coding (ABE) could be a guaranteeing approach that satisfies the stipulations for secure data recovery in DTNs. ABE characteristics a system that empowers a right to achieve entrance management over disorganized data utilizing access approaches and attributable qualities among personal keys and cipher texts. The difficulty of applying the ABE to DTNs presents a couple of security and protection challenges. Since a couple of purchasers could modification their connected qualities sooner or later (for instance, moving their district), or some personal keys could also be listed off, key repudiation (or redesign) for every one characteristic is prime keeping in mind the top goal to form frameworks secure. This infers that resignation of any property or any single consumer in a very characteristic gathering would influence alternate purchasers within the gathering. Case in purpose, if a consumer joins or leaves a attribute assemble, the connected characteristic key got to be modified and decentralized to the assorted components within the same gathering for retrograde or forward mystery. it's going to bring on bottleneck amid rekeying methodology or security corruption thanks to the windows of impotence if the past characteristic key's not overhauled quickly.

A. LIMITATION OF EXISTING FRAMEWORK:

- the difficulty of applying the ABE to DTNs presents a couple of security and protection challenges. Since a couple of purchasers could modification their connected properties sooner or later (for instance, moving their area), or some personal keys could also be bargained, key resignation (or upgrade) for every one attribute is prime with a particular finish goal to form frameworks secure.
- However, this issue is considerably a lot of difficult , significantly in ABE frameworks, since every one characteristic is probably imparted by completely different purchasers (hereafter, we tend to suggest to such a gathering of purchasers as a high quality gathering)
- Another take a look at is that the key written agreement issue. In CP-ABE, the key power creates personal keys of purchasers by applying the power's professional mystery keys to clients' connected set of properties.
- The last take a look at is that the coordination of traits issued from distinctive powers. At the purpose once varied powers administer and issue ascribes keys to purchasers freely with their professional mysteries, it's tough to characterize fine-grained access arrangements over traits issued from distinctive powers.

III. PROPOSED FRAMEWORK

In this paper, we have a tendency to propose a property primarily based secure info recovery plan utilizing CP-ABE for decentralized DTNs. The planned arrange emphasizes the attendant accomplishments. Initially, prompt property disclaimer upgrades retrogressive/forward mystery of secret information by decrease the windows of helplessness. Second, encryptors will characterize a fine-grained access strategy utilizing any monotone access structure underneath traits issued from any picked set of powers. Third, the key written agreement issue is decided by a while not written agreement key supplying convention that adventures the conventional for the decentralized DTN structural engineering. The key supplying convention produces and issues consumer mystery keys by activity a protected two-gathering processing (2pc) convention among the key powers with their own particular professional business executive facts. The 2pc convention deflects the key powers from obtaining any professional mystery knowledge of 1 another such none of them may turn out the whole set of consumer keys alone. Subsequently, shoppers don't seem to be required to utterly believe the dominant presences keeping in mind the top goal to secure their info to be imparted. the knowledge privacy and security may be cryptographically enforced against any inquisitive key powers or information warehousing hubs within the planned arrange.

A. PREFERENCES OF planned FRAMEWORK:

- knowledge secrecy: Unapproved shoppers World Health Organization do not have enough accreditations fulfilling the correct to achieve entrance approach ought to be prevented from about to the plain info within the stockpiling hub. Likewise, unapproved access from the stockpiling hub or key powers have to be compelled to be to boot averted.
- Collusion-safety: If completely different shoppers conspire, they'll have the capacity to unscramble a ciphertext by consolidating their characteristics in spite of the actual fact that every of the shoppers cannot decode the ciphertext

alone. • Backward and forward Mystery: within the setting of ABE, retrogressive mystery implies that any consumer World Health Organization involves hold a property (that fulfills the correct to achieve entrance arrangement) ought to be unbroken from about to the plaintext of the past information listed before he holds the characteristic. Then again, forward mystery implies that any consumer World Health Organization drops a characteristic have to be compelled to be unbroken from about to the plaintext of the consequent info listed once he drops the attribute, unless the other substantial properties that he's holding fulfill the correct to satisfy the policy.

IV. SYSTEM ARCHITECTURE

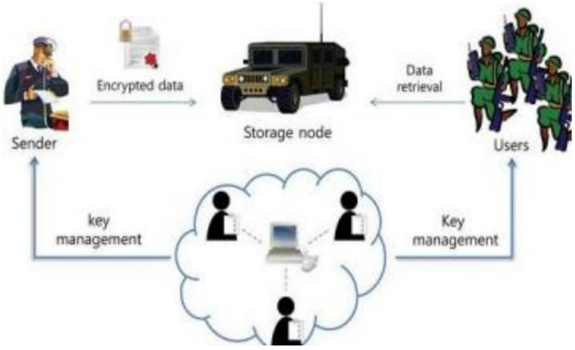


Fig 2: System Architecture

A. Implementation

Implementation 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 implementation stage involves careful planning, investigation of the existing system and it‟s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

i) Key Authorities
ii) Storage Nodes
iii) Sender
iv) User

i. 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.

ii. 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 semi-trusted that is honest-but-curious.

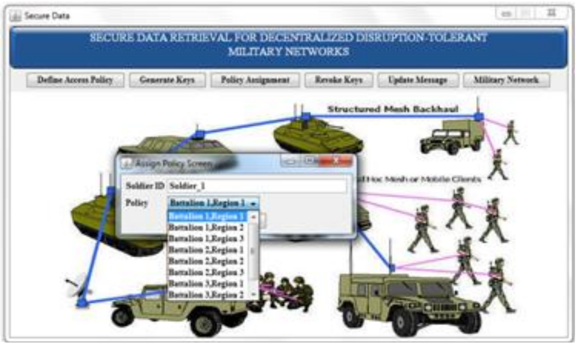
iii. Sender:

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.

iv. User:

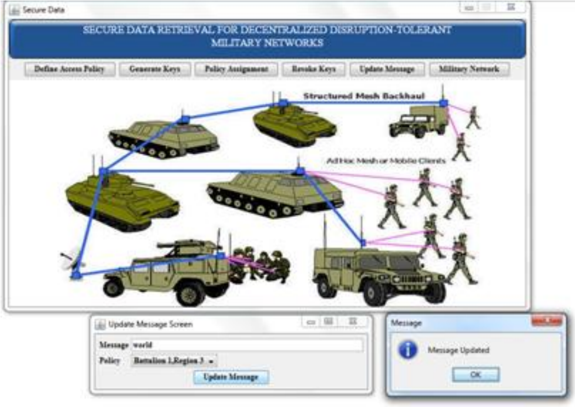
This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

V. EXPERIMENTAL RESULTS



Soldier ID Soldier_1
Policy Battalion 1,Region 1

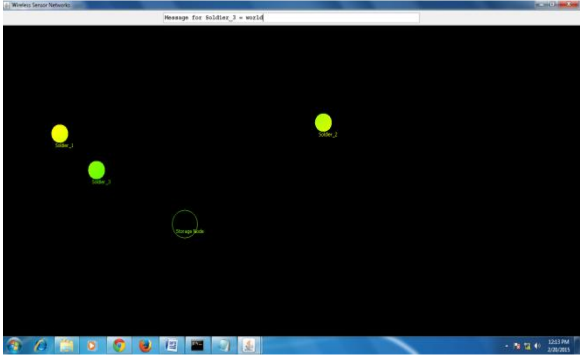
Fig 3: Policy assignment



Message world
Policy Battalion 1,Region 3

Message Updated

Fig 4: Updating a message ‘world for battalion 1 & region 3



Message for Soldier_3 = world

Fig 5: After updating the messages click on Military Network to see the network:

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 paper, 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 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] 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.

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

[9] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,”CryptologyePrint Archive: Rep. 2010/351, 2010.

[10] A. Sahai and B. Waters, “Fuzzy identity-basedencryption,” in Proc. Eurocrypt, 2005, pp. 457

[11] 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.

Fatima Nilofar Currently doing M.Tech in Software Engineering at SR Engineering College, Warangal, India. Research interests include Networks, Mobile Computing etc.,

P.Kumaraswamy is 10 years experienced Assistant Professor in the department Computer Science & Engineering, SR Engineering College, Warangal, India. Research interested area is Networks security etc.,.