International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Quick and Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

A. Vineth[1], John Deva Prasanna[2]

[1]Department of computer science and engineering, Hindustan University Padur Chennai, India

[2]Department of Computer Science and Engineering, Hindustan University Padur Chennai, India

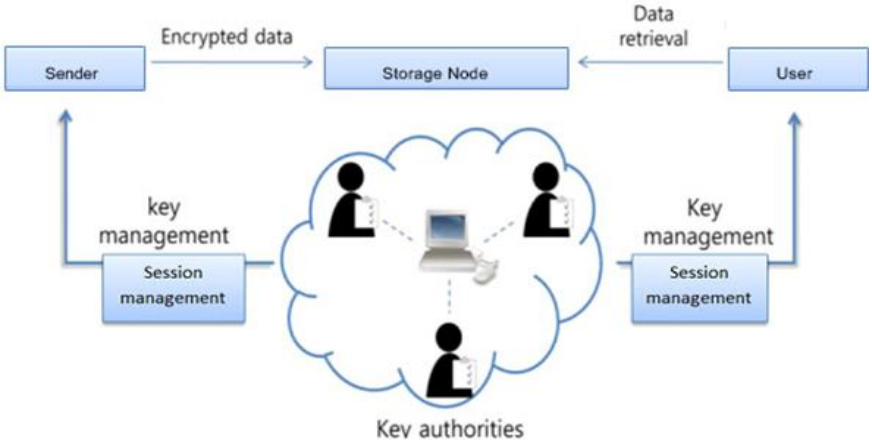
Abstract: ***The DTN technology is the famous technology which used in the military network it is differ from the normal peer to peer network it is having the storage network if the connection is not establish it will store in the storage node the after the connection is establish then it transfer to the receiver to make it secure ABE CP is used in which the transfer data is encrypted in which the key is required to decrypt, for that key manager is set up as it is a decentralized network multiple key authority are decentralized new bundle protocol is used for its efficiency and make it as traffic free session management is used in which we are having fast and secure data transfer.***

Keywords: Attribute-based encryption (ABE), Disruption-tolerant network (DTN), Multiauthority, Secure-data retrieval, Session management, Bundle protocol, Access control

1. Introduction

In Military security, is an important issue and in which lot of secret information and stuff are transfer, and for the secrecy we are cryptographically enforced it and in which the commander for the group is act as the key authority in before that the every person in the mission is need register in the portal for them a specific user id and password is given and by that they can termite the information for the ever user they are having the specific communication device and from that device they can send information in which for them for the specific region specific key authority are there and they can get the key form them and as it is military environment the DTN technology is used and it useful even when the frequency is not there if the soldier in the region 1 need to send the information he get the key form his key authority and send the information to the storage node and form that required information can be able to take by the user from the storage node

Then the last challenge is the coordination of the key authority and the soldiers who are holding account in that and in which previous the key escrow problem is there and now it is reduced in which all the key authorities are not able to view the key and in which for the particular key authority can see their own group members and remaining cannot view and in which if the old existing user remove account form the group and that will be intimated to the key authority and the account is expired the unauthorized user not able to view are go in that



For security purpose the encryption policy is maintain in this for which we are using the CP-ABE encryption technique the encryption is different it is based on the attribute base and in which the needed information that are taken and that are encrypted form by getting the key from the authority and for the group of the members the individual authority is there and in which the key up date is there in the same algorithm is used are the new algorithm is used and in which the CP is stands for the cipher text and as it is the attribute based encryption the encryption that is different for the individual attribute and make it is secure the member form the group is removed his unique id is removed and if the new member is joined means the same id is not given it is different from frequent

2. Related Work

In CP-ABE, is taken for the encryption policy and in the

transferred data is taken to this step but a key is simply created with respect to an attributes set. CPABE is more appropriate to DTNs than KP-ABE because it enables encryptions such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes ABE comes in two flavors called key-policy ABE (KP-ABE) and cipher text-policy ABE(CPABE).In KP-ABE, the encrypted only gets to label a cipher text with a set of attributes. The each user is having the different policy from the key authority that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key.

1) Key Escrow
The secret information that are encrypted for the key of the single master and he is the one is having the all the power and the master can view the key when generating Thus the key escrow problem is following such that the key authority can decrypt every cipher text addressed to users in the same group generating their secret keys at any time.

2) Attribute Revocation
Key evocation mechanisms in CP-ABE and KP-ABE, respectively. The solutions are to relate to each attribute expiration the date or time and distribute a new set of the keys to real users after that it expiration. The periodic attribute revocable schemes have two main problems. The first and fore most problem is the security issue in terms of the Back ward and forward secrecy. It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g., position or location move when considering that.

3) Revocation
The keys of a user without rekeying the whole set of key components of the user in ABE key structure since the whole key set of a user is bound with the same random value in order to prevent any collusion attack. Therefore, revoking a single attribute in the system requires all users who share the attribute to update all their key components even if the other attributes of them are still valid. This seems very inefficient and may cause severe overhead in terms of the computation and communication cost, especially in large-scaled DTNs Shows the authority architecture, logic expressiveness of access structure that can be defined under different dis joint sets of attributes managed by different authorities, key escrow, and revocation granularity of each CP-ABE scheme. In the previous scheme the logic can be very expressive that the same BSW single authority such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV the schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done as to the BSW in the immediate way it taken. Therefore, the user of the attribute is revokes that at any time even before the expiration time.

4) Efficiency of encryption
In addition, the proposed scheme realizes more fine-grained user revocation for each at- tribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the cipher text. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities. Table summarizes the efficiency comparison results among CP-ABE Schemes. As shown in Table the proposed scheme needs rekeying message size of at most to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its cipher text size is linear to the number of revoked users in the system since the user revocation message is included in the cipher text. The proposed scheme requires a user to store more KEKs

5). Key Updating
If the single key is used we can't be to secure more we need the key updating the same algorithm and a new algorithm is used for the updating of the key and it is mandatory

3. System Description and Assumptions

1)Key authorities
The Center authority is the key authority and he is having multiple authority and all of decentralized and in which the particular group is need the key then he is going to get the key from his authority from his communication device already he is having the user name and the password and the key is one time generation and it generated for the one time and after that the encrypt data which is stored in the storage node then the user need the information he need to decrypt for that he get the key from the key authority and form that key decrypt and he take the necessary information.

2) Storage node
As it is the DTN network the storage node is needed, because it end to end connection the signal is not there, for that it is used and in which both the sender and user are in the use and in the data are encrypted and stored because all the data are highly sensitive date and the encryption is taken for the multiply time by the same and the different algorithm and by this the collision loss is fully reduced and we are having the strong security based encryption system

3) Sender
The sender send the important things and information for his communication device to store in the storage node and make it secure he get the key from the authority and form that key he can store the important things and information

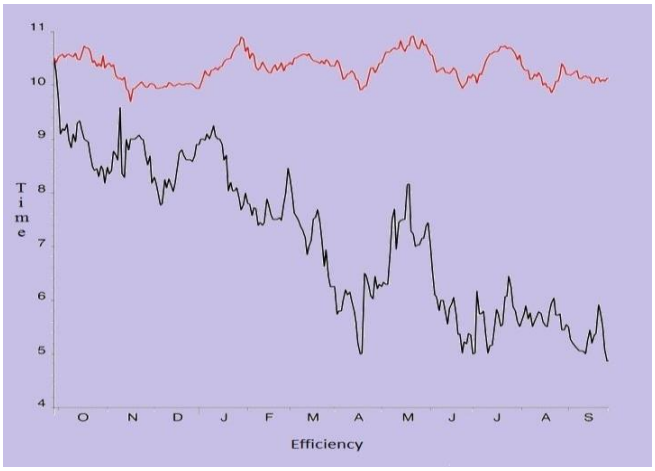
4) Receiver
The receiver who is away from the sender and he is in another near location and he need the confidential information and important message he need to get it from the storage node for that he need the decryption key so that he need to get the decryption key from the key authority after that getting key using that he receive the information and after that the acknowledgement which is received to the authority the key which is generate by one time after that it is not valid.

5) CP-ABE Method
In Cipher text Policy Attribute based Encryption scheme, the encryption can fix the policy, which 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 cipher. In our method in which the access policy not be sent along with the cipher text, by which we are able to preserve the privacy of the encryption the encryption which is the attribute based and in which it is difference from attribute. In which multiple times of the encryption may be done and by the same algorithm and by the different algorithm.

6) Session management
Session management in the many data owners going to upload the data in storage node before the they get key for the key authorities to make it encrypt likewise many data owner approach the Key authorities it will to traffic so we using the session management It maintain certain session timing after that it reject the connection and go for the another user by the same it will be in user download the data.

4. Proposed Scheme

The bundle protocol is used in the proposed scheme it is used to send application data across the DTN network basically the DTN is used in the delay tolerant network and it is also known as the delay disruption tolerant network in which the data is bundled together and that are stored in the storage node and some of the uses are
1) Use of the delay tolerant network
2) Bundles fragmentation in vehicular delay
3) Transport layer protocols



In which many technique is used and they are Internet engineering task force, Delay tolerant network architecture bundle protocol specification, Transmission control protocol, Transmission layer OSI model, User data gram protocol are used, It is new technique and it is used in the space research and it is used to increase the efficiency of the data transfer

The session management is used to reduce the traffic and in which the many user are waiting for receiving the key from the key authority and it creates the traffic for that we are using the session management and in it waiting for the particular waiting time and after the waiting time is reached the session is finished and it connects the next user. We use the session management for the both the key authority for the sender and for the receiver in both side the traffic will be taken

5. Conclusion

In military area the DTN technology is now booming because the network is secure and efficient and in which the session management is used to reduce the traffic and the new bundle protocol is used for the efficiency of the network the DTN technology is used because as it is the military environment signal is may or may not be in which we are having the collusion loss and to overcome that we are using the technology and in which previous the store and forward technique is used and in which less packet that be transmitted and the it is less efficient, to overcome that bundle protocol is used and it booming now a days and it is using in the space and the for the disaster management in which the routers is used to transmit the signals for the security CP-ABE technique is used

Reference

[1] J.Burgess, B.Gallagher, D.Jensen, and B.N.Levine, "Maxprop:Routing for vehicle-based disruption tolerant networks," in Proc.IEEE INFOCOM, 2006,
[2] M.Chuah and P.Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006
[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 Mobic, 2006
[4] S.Roy and M.Chuah, "Secure data retrieval based on cipher text 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
[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
[7] L.Ibraimi,M.Petkovic,S.Nikova,P.Hartel, and W.Jonker, "Mediated cipher text-policy attribute-based encryption and its application in Proc. WISA, 2009, LNCS 5932
[8] N.Chen, M.Gerla, D.Huang, and X.Hong,"Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption,"inProc. Ad Hoc Network. Workshop, 2010
[9] D.Huang and M.Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," Ad Hoc Network., vol. 7, no. 8,2009.
[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,
[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. Computer. Commun. Security, 2006
[13] J.Bethencourt, A.Sahai, and B.Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symposia. Security Privacy, 2007
[14] R.Ostrovsky,A.Sahai,B.Waters, "Attribute-based encryption with non- monotonic access structures," in Proc. ACM Conf. Computer.Commun. Security, 2007
[15] S.Yu,C.Wang,K.Ren,W.Lou, "Attribute base data sharing",ASIACCS, 2012
[16] A.Boldyreva,V.Goyal, and V.Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Compute. Commun. Security,2008
[17] S.Rafaeli and V.Gouda, "A Survey of Key management for secure group communication",2013