International Journal of Research in Advent Technology, Vol.5, Issue 3, March 2017
E-ISSN: 2321-9637
Available online at www.ijrat.org

Secure Data Retrieval using CP-ABE for Decentralized DTN

Ku. Dhanshree K. Bhure[1], Prof. Pawan Mundhare[2]
Department of computer Networking[1,2], Student[1],Assistant Professor[2]
Email: dhanshree2101@gmail.com[1] ,pmundhare@gmail.com[2]

Abstract-Portable nodes in military environments, for example, as in battlefield or an unfriendly area are prone to experience the under go of irregular system network and frequent partitions. Interruption tolerant network (ITN) innovations are getting to be fruitful results that permit remote device conveyed by officers to speak with one another and access the secret data or summon dependably by abusing outside capacity nodes. Possibly the most solid issues in this situation are the necessity of approval arrangements and the strategies redesign for secure information recovery. This paper considers an attribute-based secure data retrieval scheme using CP-ABE for ITNs where multiple key authorities manage their attributes independently. Immediate attribute repeal enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Key escrow problem is resolved by an escrow-free key issuing protocol that utilizes the characteristic of the decentralized ITN architecture proposed a decentralized approach; their technique does not authenticate users. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the Interruption-tolerant military network.

Index Term- Access-control, Attribute-based encryption (ABE), Interruption-tolerant Network (ITN), Multiauthority, Secure Data Retrieval.**1.**

1. INTRODUCTION

In military system environment, associations of remote gadgets conveyed by officers may be briefly detached by sticking, ecological variables, and versatility, particularly when they work in hostile environments. Interruption tolerant system (DTN) technologies are becoming favorably result that authorize nodes to communicate with each other in these immensely networking environments. [1]–[3].Naturally, when there is no limit to-end attachment between a source and a destination pair, the messages from the source node may need to wait in the middle nodes for a considerable amount of time until the connection would be finally established. Roy [4] and Chuah [5] presented capacity hubs in ITNs where information is put away or duplicated such that just approved movable hubs can get to the essential data rapidly and completely. Innumerable military applications require enlarge security of private information including access control procedure that are cryptographically implemented. In many cases, it is sensible to provide discriminate access services such that data access policies are defined over user attributes or roles, which are control by the key authorities. For illustration, in a Interruption-tolerant military network, a commander may store classified data at a stockpiling hub, which ought to be gotten to by parts of "Legion 1" who are partaking in "District 2." It is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions, which could be frequently changed (e.g., the attribute representing current location of moving soldiers) [4], [8], [9].We suggest to this ITN construction where various powers issue and deal with their trait keys freely as a decentralized ITN [10]. The idea of attribute based encryption (ABE) [11]–[14] is an encouraging approach that satisfies the necessities for secure information recovery in ITN.ABE characteristics an instrument that authorize a right to gain approach control over scrambled information utilizing access approaches and attributed qualities among private keys and cipher text. Mostly, cipher text-policy ABE (CP-ABE) provides a expandable way of encrypting data such that the encryptors defines the attribute set that the decrypted needs to possess in order to decrypt the cipher text [13]. Thus, dissimilar users are allowed to decrypt dissimilar pieces of data according to the security policy.On the other hand, the ABE to ITN presents a few security and protection challenges. Since a small number of clients may change their related qualities eventually (for instance, moving their area), or some private keys might be compromised, key repeal (or update) for each attribute is necessary in order to make systems secure. This involves that repeal of any attribute or any single user in an attribute group would affect the other users in the group. For illustration, if a user add or quit an attribute group, the related attribute key should be changed and reconstruct to all the other members in the same group for backward or forward secrecy. It may result in congestion during rekeying procedure or security humiliation due to the windows of powerlessness if the previous attribute key is not updated immediately. An additional problem is the key escrow problem. In CP-ABE, the key authority produce private keys of users by exercise the authority's master secret keys to users' associated set of attributes. In this manner, the key control can decode each cipher text

tended to particular clients by producing their attribute keys. If the key authority is damage by opponent when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an built-in problem even in the various-authority systems as long as each key authority has the whole right to generate their own attribute keys with their own master secrets. The final problem is the coordination of attributes issued from dissimilar authorities.

2. RELATED WORKS

ABE comes in two savor called key-policy ABE (KP-.ABE) and Cipher text policy attribute-based encryption. In KP-ABE the encryptors just gets to name a cipher text with a set of attributes. The key power picks an approach for each one client that figures out which cipher text he can unscramble and issues the way to every client by inserting the strategy into the client's key. The key authority chooses a policy for each user that decides which cipher text he can decrypt and issues the key to each user by embedding the policy into the user's key.. In CP-ABE, the cipher text is encrypted with an access policy chosen by an encryptors, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors 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 [4], [7].

1) Attribute Repeal: Bettencourt et al. [13] and Boldyreva et al. [16] first suggested key repeal structure in CP-ABE and KP-ABE. Their results are to adjoin to each attribute an termination date (or time) and spread a new set of keys to valid users after the termination. The regularly property revocable ABE plans [8], [13], have two primary issues. The first problem is the security humiliation in terms of the backward and forward confidentiality. It is a trustworthy situation that clients, for example, fighters may change their qualities frequently, e.g., position or area move when considering these as characteristics [4], [9].Then, a user who just envelop the attribute might be able to access the foregoing data encrypted before he obtains the attribute until the data is re-encrypted with the newly updated attribute keys by periodic rekeying (backward confidentiality).

2) Key Escrow: Most of the live ABE schemes are build on the architecture where a single trusted authority has the power to create the whole private keys of users with its master secret statistics [11], [13]. Thus, the key escrow problem is built-in such that the key authority can decrypt every cipher text approach to users in the system by creating their secret keys at any time. Chase et al. introduce a distributed KP-ABE scheme that solves the key escrow problem in a Multiauthority system.

3. EXISITING FRAMEWORK

The scheme of Attribute based encryption (ABE) is a promise approach that fulfills the requirement for secure information recovery in ITNs. ABE characteristics a system that permit a right to gain entrance control over scrambled information utilizing access approaches and credited qualities among private keys and cipher text. The issue of applying the ABE to ITNs 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 in point, 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**.**

4. PROPOSED FRAMEWORK

In this paper, we suggest an attribute-based secure data recovery scheme utilizing CP-ABE for decentralized ITNs. The proposed plan features the following attainment. Firstly, immediate attribute repeal enhances backward/forward secrecy of confidential data by reducing the windows of helplessness. Second, encryptors can characterize a fine-grained access strategy utilizing any similarity access structure under feature issued from any chosen set of power. Third, the key escrow problem is resolved by a without escrow key issuing protocol that utilize the feature of the decentralized DTN structural engineering. The key issuing deals create and issues user secret keys by performing a reliable two-party processing (2PC) protocol among the key power with their own master secrets. The 2PC protocol intercept the key power from obtaining any master confidential information of each other such that none of them could create the whole set of user keys alone. Eventually, user are not needed to entirely believe the dominant presences keeping in mind the end goal to confidential their information to be convey. The information confidentiality and security might be cryptographically imposed against any disquisitive key power or information storage hubs in

the proposed scheme.

4.1 Ciphertext Policy Attribute based Encryption

A cipher text policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Key Generation, Encryption and Decryption.

Setup: The setup calculation takes no info other than the understood security parameter. It yields general society parameters PK and an expert key MK.

Key Generation (MK, S): The key era calculation takes as information the expert key MK and an arrangement of properties S that depict the key. It yields a private key SK.

Encrypt (PK, A, M): The encryption calculation takes as information of general parameters PK, a message M, and an entrance structure An over the universe of qualities. The calculation will encode M and produce a ciphertext CT such that lone a client that has an arrangement of qualities that fulfills the entrance structure will have the capacity to unscramble the message. Accept that the ciphertext verifiably contains A.

Decrypt(PK,CT,SK): The unscrambling calculation takes as information in general parameters PK, a ciphertext CT, which contains an entrance arrangement An, and a private key SK, which is a private key for a set S of traits. On the off chance that the set S of traits fulfills the entrance structure A then the calculation will decode the ciphertext and return a message M.

4.2 AES Algorithm

4.2.1 AEC Cipher :

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
Begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state, w[0, Nb-1])
  for round=1 to Nr-1
      SubBytes(state)
      ShiftRows(state)
      MixColumns(state)
      AddRoundKey(state, w[round*Nb, round+1)*Nb-1])
  end for
  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1)
  Out = state
End
```

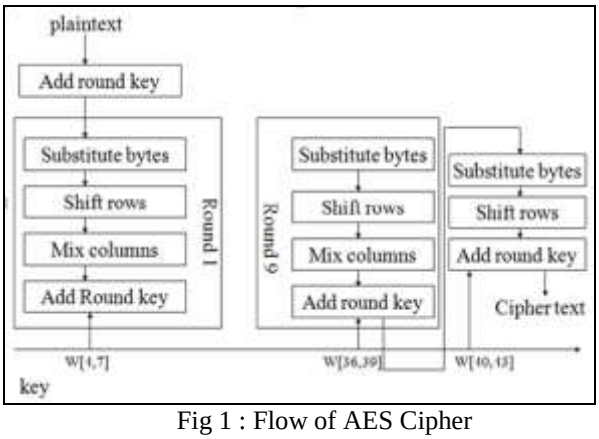

Fig 1 : Flow of AES Cipher

4.4.2 AEC Inverse Cipher :

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
Begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1)
  for round=1 to Nr-1
      InvShiftRows(state)
      InvSubBytes(state)
      AddRoundKey(state, w[round*Nb, round+1)*Nb-1])
      InvMixColumns(state)
  end for
  InvShiftRows(state)
  InvSubBytes(state)
  AddRoundKey(state, w[0, Nb-1])
  Out = state
```

End

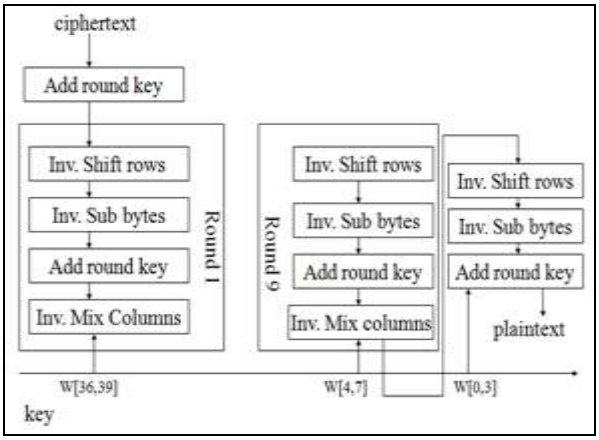

Fig 2 : Flow of AES Inverse Cipher

5. IMPLEMENTATION DETAIL

Implementation encompasses all the processes involved in getting new software or hardware operating properly in its environment, including installation, configuration, and running, testing, and making necessary changes. As such, implementation is the action that must follow any preliminary thinking in order for something to actually happen. Following models helps to get precise model of our project:

Fig 3: Browse the file to send

Fig 4 : Send the given file

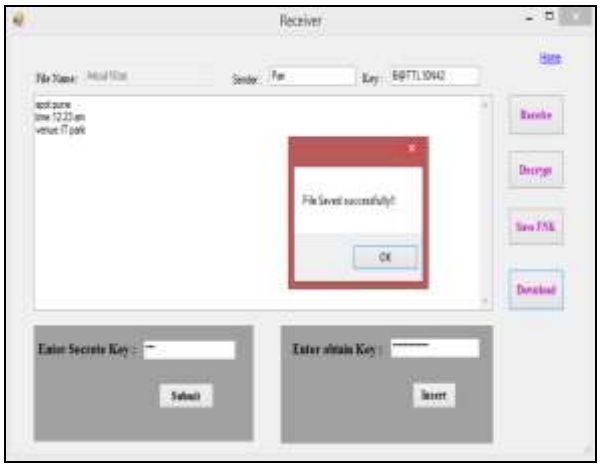

Fig 5 : Receiver Decryption process by entering obtain key

6. RESULT

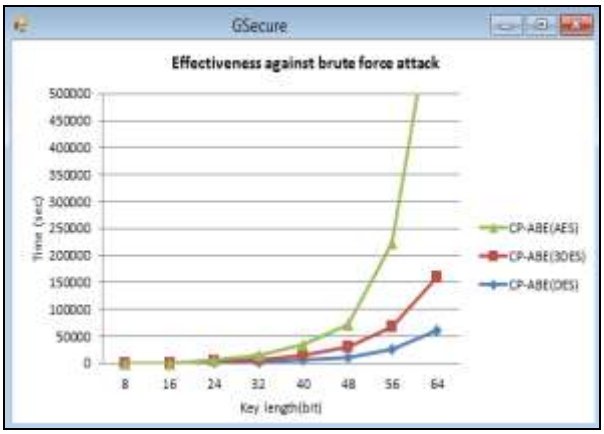

Fig 6 : Comparison: Effectiveness against brute force attack graph.

7. CONCULSION

DTN technologies are becoming successful result in military applications that permit wireless devices to communicate with each other and access the private information accurately by utilize external storage nodes. CP-ABE is a scalable cryptographic result to the access control and reliable data retrieval issues. In this paper, we proposed an efficient and reliable data retrieval procedure using CP-ABE for decentralized ITNs where various key authorities supervise their attributes separately. In addition, the fine-grained key revocation can be done for each attribute group. We determine how to apply the suggest mechanism to securely and efficiently manage the confidential data distributed in the interruption- 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. ACMMobiHoc, 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.17.

[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 cipher text-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 enforcementin 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.[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc.Eurocrypt, 2005, pp. 457–473.

[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.

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