ISSN:0975-9646

Secure and Efficient Confidential Data Using Multiple Authorities in DTN

Ayinavalli Venkata Ramana[1], Pavithra Urjana[2]

[1]*Assistant Professor, Department of IT, GMRIT/JNTUK, India.*
[2]*M.C.A Student, Department of computer applications, GMRIT/JNTUK, India.*

Abstract: The Cipher text-policy Attribute Based Encryption for secure data retrieval in decentralized Disruption Tolerant Networks (DTNs). Here we are design multiple key authorities manage their attributes. Immediate attribute revocation enhances security in storage nodes. Key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized Disruption Tolerant Networks architecture proposed a decentralized approach. Previous techniques are not verifying the users effectively. Demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. Here we are design coordinates attributes verification after submission of each and every user. Finally the Disruption-tolerant network (DTN) technologies are provide the successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes.

Keywords: disruption tolerant network, confidentiality, CP-ABE, reliability, storage nodes information.

I. 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 suchthat data access policies are defined over user attributes or roles, which are control by the key authorities. For illustration, in 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.

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.

II.RELATED WORK:

In information retrieval we need to provide the security with attribute based encryption and revocation techniques (ABE). Two types of attribute based encryption techniques are available here.

1. Key policy attribute based encryption
2. Cipher text policy attribute based encryption

Key policy attribute based encryption works depends on key authorities. Key authorities verify the keys of information then provide the signal to decrypt the cipher text content. It does not depend on roles of user's. It's completely works depends on keys environment.

Cipher text policy attribute based encryption works depends of roles of users attributes. Select any file applies the number of attributes then converts into cipher text. Using this encryptions we can maintains the files as a confidential data.

The above two solutions are provide the attributes. These attributes are valid at specific time interval only. Again we generate the new keys and assign to number of users. Periodic attribute revocation is helpful to enhance the security.

Again design using attribute revocation techniques also security degradation problems are available. User may chance to change the attributes frequently. Automatically our system assigns the new keys. This approach we can call as a rekeying process. Using rekeying approach we can enhance the security in storage nodes. Here we observe the scalability issues.

Key authority periodically announces a key update material using unicast operation at each and every timeslot. Other users also must update the keys of information. It's very complex approach. This is solution is somewhat lack of efficiency and performance. Here some other problems are available like overhead.

In all approaches single trusted authority is available and generates the all private keys to users. These private keys of information are available under control master level. Numbers of levels are less to control the attackers. This is kind of issue we can call as a key escrow.

This problem is possible to solve with distributed key policy attribute based encryption technique. Distributed policy based attribute encryption design using multiple authorities. But here there is no centralized authority. There is no communication from one authority to another authority level.

Next decentralized attribute based encryption scheme design with multi authority network environment process. This policy works based on combined attributes content. Combined attributes results display in the form of Boolean expression. This Boolean expression format result also is not efficient to control attackers. This scheme also suffers with key escrow.

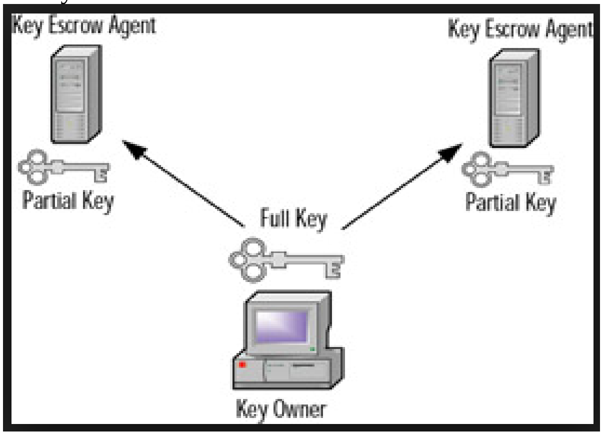

Fig1: Key Escrow Problem

III.PROBLEM STATEMENT

Here we can design the safeguard to enhance the quality on military networks. We suggest with this system to maintain the data as a safety in storage nodes or storage hubs. This system is secure against attackers. Here we arrange the attributes for user qualifications whether he is the user authorized or unauthorized. This system supplies the files as a scalable manner. It can control more amounts of failures. Using the number of attributes only we are gets the benefits in our implementation.

IV.PROPOSED SYSTEM ARCHITECTURE

In cipher text approach introduces the quality based encryption operations are performed in our implementation as a new feature. After user submission all attributes of information next to perform the encryption operation. Attributes are considered as assistance to perform the encryption operation. That's why it's quality encryption approach. Through these operations it's possible to get the scalability, reliability and enhance the security also in our implementation process.

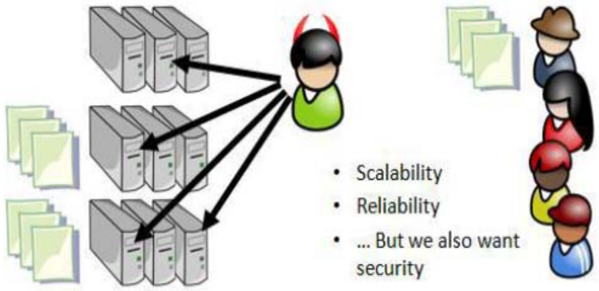

Fig2: Proposed system Architecture

One more new feature is designed that is called fine grained access control operation for each and every attribute group. Anyway our proposed scheme maintains the data as a confidential and efficient and secure. This system provides scalability, reliability and security services efficiently compare to all the previous approaches.

Functionalities of Framework:

1. Key authorities
2. Storage hub
3. Sender
4. User

Key Authorities:

These are key creation centers that create open/secrete parameters for cipher text policy attribute based encryption. Transmission of any content depends on different key authorities. Collect the attributes from neighborhood authorities next to allow the users to perform the operations and otherwise disallow the users.

Storage Hub:

Collect the information from sender store into hub and provide the files of information corresponding users. Storage hub works as a trusted authority.

Sender:

Organization users store the personal information and sensitive information in storage nodes. Storage node distributes the services, who need the services like different locations of users. Sender stores the data as an encrypted format. Encryption operation can perform after all attributes verification.

User:

User can fulfill the attributes of information then we can allow to accessing the information from storage hub. User can decrypt the information.

V.RESULTS AND DISCUSSION

Here using security requirements we prove the enhance security in our implementation. Using security requirements control collusion resistance attacks and increase the data confidentiality and also backward and forward secrecy.

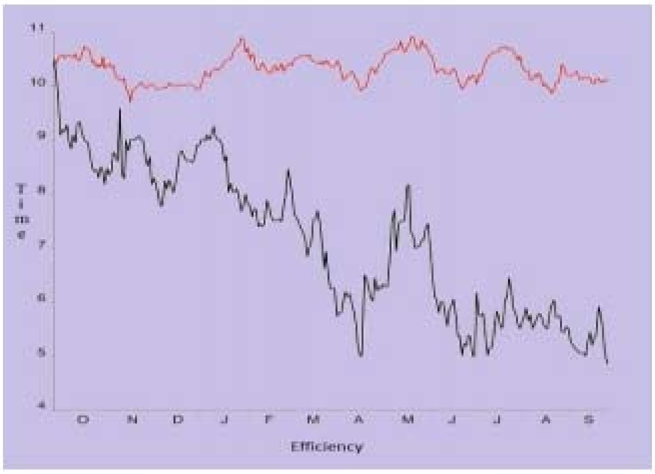

Fig 3: performance graph

VI.CONCLUSION

Using storage hubs we distribute the services to authorized users. CP-ABE provides the scalable and efficient cryptographic result content in our implementation process. Here using multiple authorities control the attackers in distributed disruption tolerant networks. Using inherent key approaches key escrow problem is resolve efficiently. Proposed mechanism manages the data confidential as a secure and efficient in our implementation process.

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] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in *Proc. IEEE MILCOM*, 2007, pp. 1–7.

[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 ciphertext-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 enforcement in 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.

[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. Comput. Commun. Security*, 2006, pp. 89–98.

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

[14] 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.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in *Proc. ASIACCS*, 2010, pp. 261–270.

[16] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attributebased systems,” in *Proc. ACMConf. Comput. Commun. Security*, 2006, pp. 99–112.