iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IX **Month of publication:** September 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Improved Scalability and Security on Data Retrieval for Decentralized DTN'S Using CP-ABE Algorithm

G.Gayathri[1], A.K.Puneeth Kumar[2]
[1]M.Tech CSE Student, [2]Asso.Prof, ResearchScholar
Dept of CSE, SEAGI, Tirupati,

Abstract: ***Mobile Nodes in some challenging network scenarios suffer from intermittent connectivity and frequent divisions, for example in battleground if the network failure occurs then there is a chance to lose the data. Many of the networks are failed to recover the data that was lost. The DTN technology is the famous technology which is used in the military network. It permits devices which are wireless and supports by peoples in a military to interact with each other. In this technology the data will be transferred from sender to receiver through intermediate nodes. So, as we are using intermediate nodes there are issues related to data security. Some of the challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. In this paper, we suggest a secure data retrieval scheme based on the Cipher text Policy Attributed-Based Encryption (CP-ABE) algorithm. In Cipher text Policy Attribute-Based Encryption (CP-ABE), a user secret key is merged with a set of attributes, and the cipher text is related with an access policy over attributes. In decentralized DTNs multiple key authorities manage their attributes without depending on others. We illustrate how to apply the proposed mechanism to safely and proficiently deal with the classified information dispersed in the Interruption or disruption tolerant network.***

Keywords: ***Access-control, Attribute-based encryption (ABE), Disruption-tolerant Network (DTN), Multi authority, Secure Data Retrieval.***

I. INTRODUCTION

In numerous military system situations, associations of remote gadgets carried by soldiers are disconnecting temporarily, because of unfavorable environmental situations. Disruption tolerant system (DTN) innovations are getting to be successful arrangements that permit hubs to communicate with one another in these compelling system administration situations [1]-[3]. Usually, when there is no path exists in between a source and a destination combine, the messages from the source hub may need to hold up in the middle of the road hubs for a significant measure of time until the association would be inevitably settled. Roy [4] and Chuah [5] presented capacity hubs in DTNs where information is put away or reproduced such that just approved versatile hubs can get to the vital data rapidly and productively. In general military applications require more insurance of secret information including access control systems that are cryptographically upheld. Most of the time, it is necessary to give separated access administrations such that information access strategies are characterized over client characters or roles, that are overseen by the key authorities. Case in point, in an interruption tolerant military network, an administrator may store a secret data at a stockpiling hub, which have to be gotten to by individuals from "Region 1" who is participating in "Region 2." For this situation, it is a sensible suspicion that numerous key powers are liable to deal with their own particular element properties for fighters in their conveyed locales or echelons, which could be frequently changed [4] [8], [9]. The Disruption Tolerant Network structural planning where many powers issue and deal with their own quality keys freely as a decentralized DTN. The idea of characteristic based encryption (ABE) is a guaranteeing approach that satisfies the necessities for secure information recovery in DTNs. ABE characteristics an instrument that authorizes a right to gain entrance control over twisted information utilizing access strategies and attributed qualities among private keys and cipher texts. The Cipher Text policy Attribute based encryption algorithm gives a versatile method for encoding information such that the sender characterizes the characteristic set that the receiver needs to have to decode the cipher text. Therefore, different clients are permitted to decode different bits of information in the security strategy. It may causes in restricted access during the time that when we are changing the key or security weakening due to the windows of susceptibility if the previous attribute key is not updated immediately. The key escrow problem is another major

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

thing. In the Attribute based encryption the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. So that's why, the key authority can decrypt any cipher text forwarded to specific users by generating their attribute keys. The final challenge is the coordination of attributes issued from multiple authorities. It is very difficult to define good access schemes over attributes issued from several authorities, when several authorities manage and issue attributes and keys to users independently with their own master keys. For example, suppose that attributes "role 1" and "region2" are managed by the authority B, and "role 2" and "region 1" are managed by the authority A. In this situation it is not possible to produce an access policy (("role 1" OR "role 2") AND ("region 1" or "region 2")) in the previous strategies because the OR logic between attributes issued from different authorities cannot be implemented. Why, because the fact that the dissimilar authorities generate their own attribute keys using their own master secret keys that are autonomous and individual. So that's why, general access policies cannot be articulated in the existing schemes, which is a extremely practical and usually required access policy logic.

II. NETWORK ARCHITECHTURE

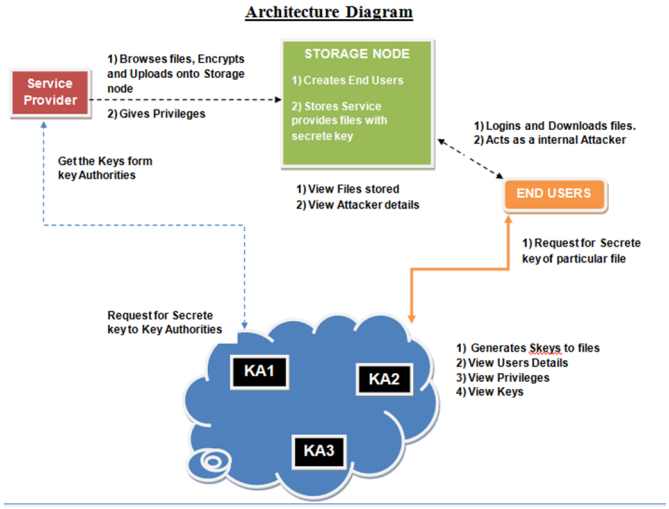


Fig 1: Disruption tolerance network architecture diagram

A. Key Authorities

They are the key generation centers that generate public or secret parameters for CP-ABE. The key authorities consist of central authority and multiple local authorities. There are secure and reliable communication channels between a central authority and each local authority. Each local authority manages different attributes and issues corresponding attribute keys to users.

B. Storage Node

This entity stores data from senders and provide corresponding access to users. It may be mobile or fixed.

C. Sender

This entity owns confidential data and wishes to store them into the external data storage node. A sender is responsible for defining access policy and encrypts the data under the policy before storing it to the storage node.

D. Receiver

This is a mobile node that wants to access the data stored at the storage node. If a user owns a set of attributes satisfying the access policy of the encrypted data then he will be able to decrypt the ciphertext and obtain the data.

III. EXISTING FRAMEWORK

In KP-ABE, the encryptor only gets to label a cipher text with a group of attributes. The key power chooses a policy for each user that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key. On the other hand, the roles of the cipher texts and keys are altered in CP-ABE. In CP-ABE, the cipher text is encrypted with an access

policy chosen by an encryptor, but a key is purely created with respect to an attributes set. CP-ABE is more suitable to DTNs than KP-ABE because it enables encryptors such as a commander to choose access guidelines on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes.

A. Disadvantages Of Existing Framework

The trouble of applying the ABE to DTNs introduces numerous security and privacy challenges. Because some users may change their associated attributes at some point (for example, moving their province), or a number of private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even more hard, particularly in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a collection of users as an attribute group)

Another challenge is the key escrow problem. In CP-ABE, the key power generates private keys of users by applying the authority's master secret keys to users' associated set of attributes.

The last challenge is the coordination of attributes issued from different authorities. When several authorities manage and issue attributes keys to users independently with their own master secrets, it is extremely hard to describe fine-grained access policies over attributes issued from different authorities.

IV. PROPOSED SYSTEM

In this section, we provide a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local power issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central power. Each attribute key of a user can be updated individually and immediately. Therefore, the scalability and security can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Bethencourt et al, dozens of CP-ABE strategies have been proposed. The successive CP-ABE schemes are mostly motivated by more rigorous security proof in the usual model. However, most of the schemes failed to achieve the expressiveness of the Bethencourt et al.'s scheme, which reports an competent system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic formula over attributes. Hence, in this segment, we develop a variation of the CP-ABE algorithm partially based on (but not limited to) Bethencourt et al.'s construction in order to improve the expressiveness of the access control policy instead of building a new CP-ABE scheme from scratch.

A. Advantages Of Proposed System

1) Data Confidentiality: The users who are nor authorized do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, illegal access from the capacity node or key authorities should be also prevented.

*2) Collusion-Resistance***:** If multiple users get together, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone.

3) Backward And Forward Secrecy: In the context of ABE, backward secrecy tells that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy tells that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, except the other valid attributes that he is holding satisfy the access policy.

V. RESULTS

Basic Structure of DTN Router

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

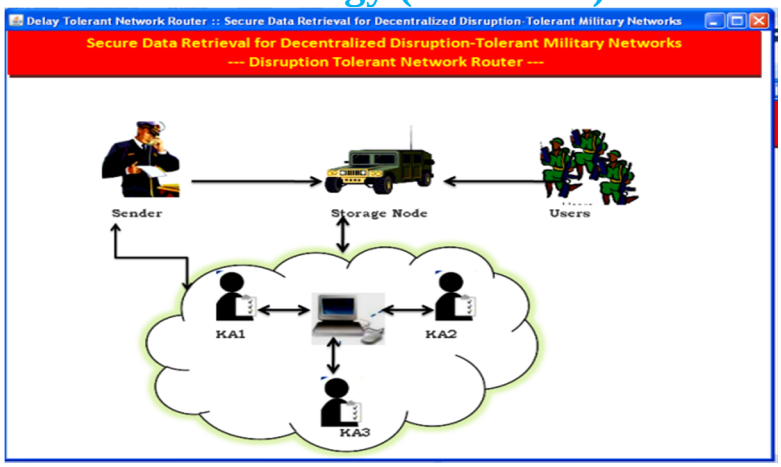


Fig 2: DTN ROUTER

Fig 3 shows the authentication of the user is with respect to their ID and Passwords.

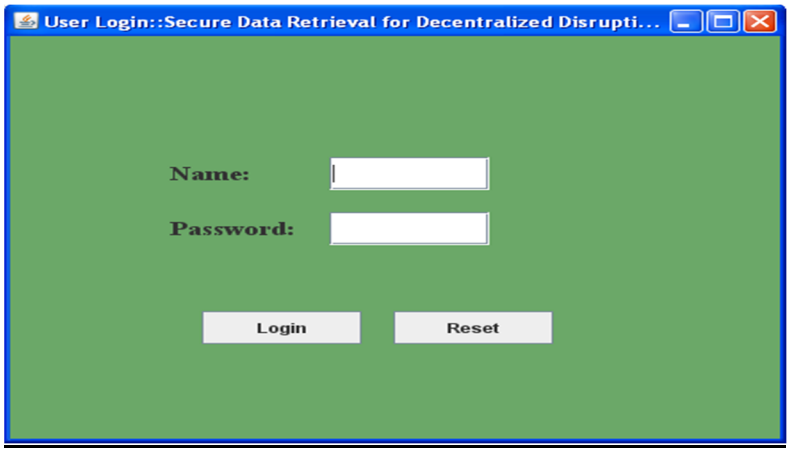


Fig 3: USER LOGIN

After successful Login the user is eligible to send and receive files

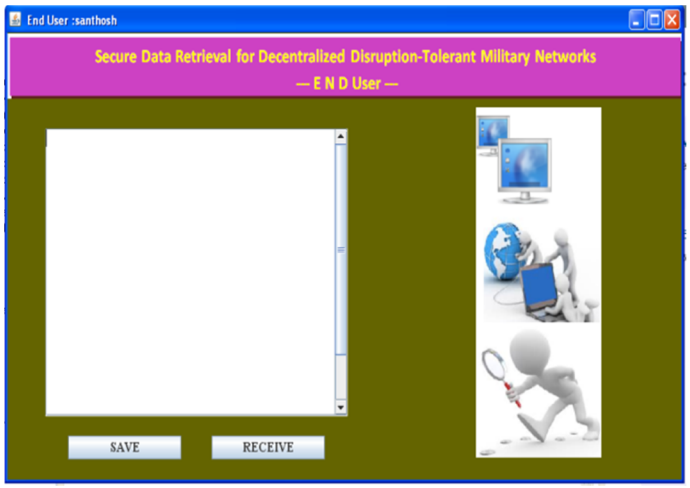


FIG 4: SEND AND RECEIVE FILES

The Fig 5 shows that the key authority who is able to generate the secret key to the user in order to access the data

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

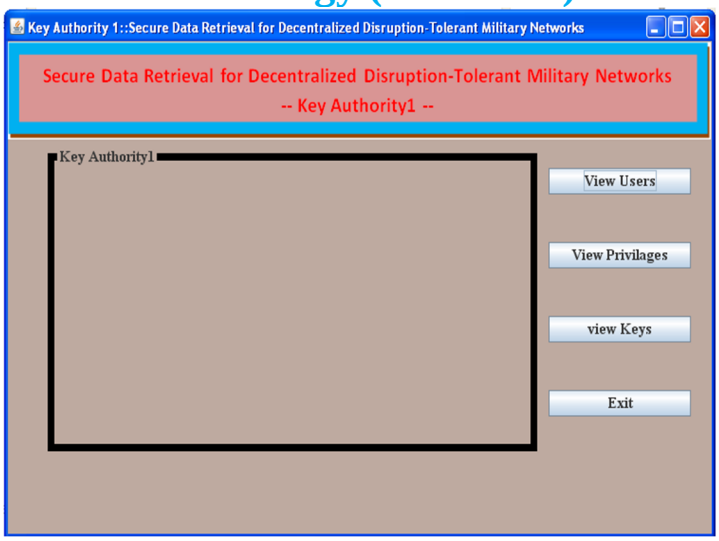


Fig 5 : KEY AUTHORITY

The Fig 6 shows sender who wants to send the files to the users

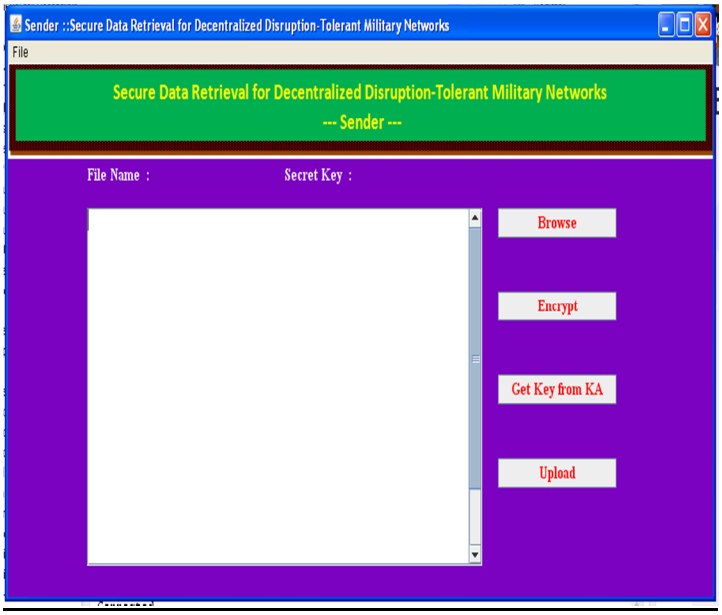


Fig 6: SENDER PAGE

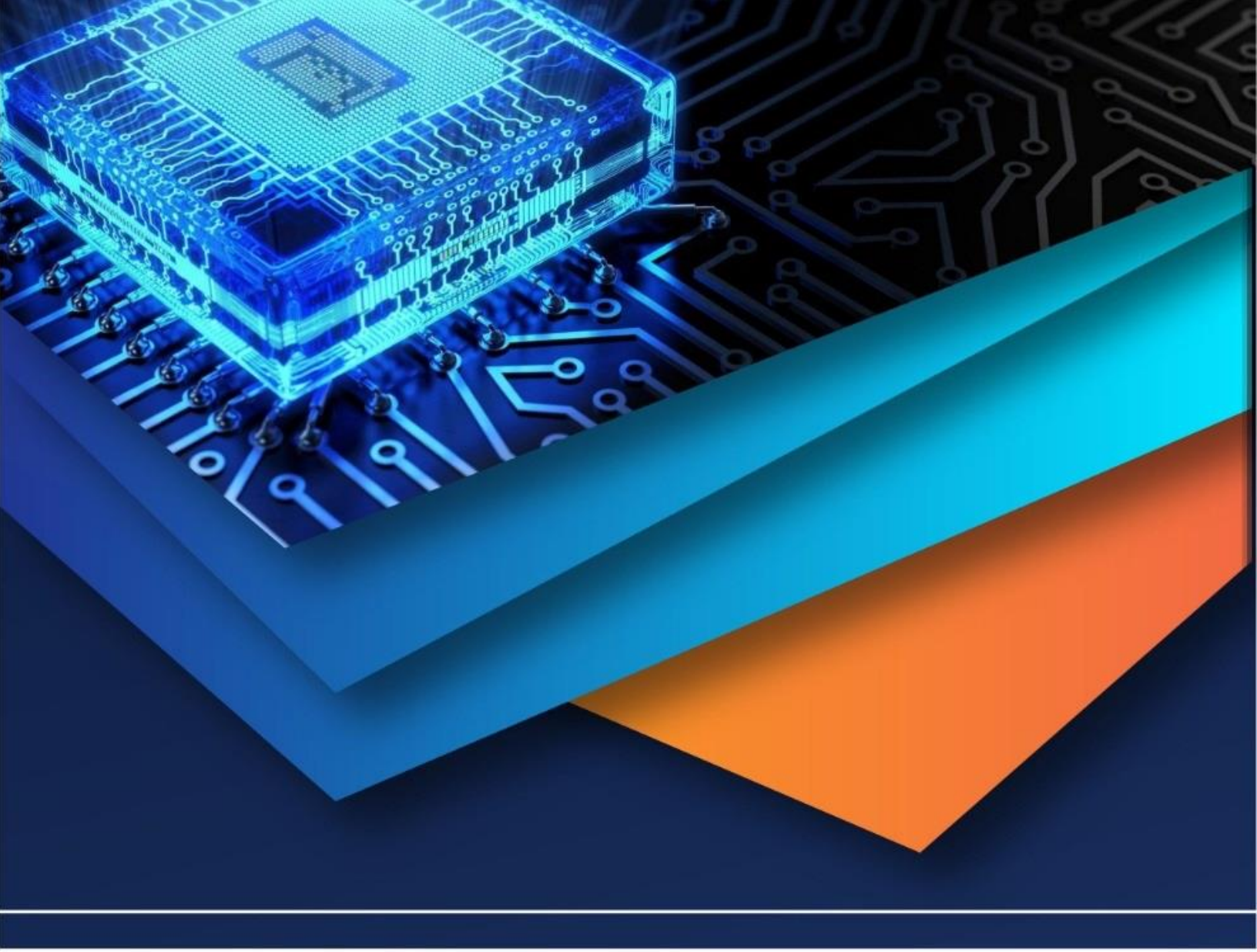
VI. CONCLUSIONS

Our project is not the unique one, but is an attempt to have a precise scenario of what the terms “secure data retrieval for decentralized disruption tolerant network” is meant to be and its implementation as well on which we are currently working. As stated before, our proposed system can enhance the security of military network by using CP-ABE mechanism. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. Here, we planned more efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes without depending on others. The inbuilt 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 semi trusted. In addition, the fine-grained key revocation can be done for each attribute group. We illustrate how to apply the proposed mechanism to securely and efficiently

manage the confidential data distributed in the disruption- tolerant military network.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang,, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks," in Proc. IEEE ACM, 2014, pp. 16–26.
[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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY