Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (82-87), Month: January-April 2016, Available at: www.noveltyjournals.com

Secure and Efficient Data Retrieval in Decentralized DTN Using MAC

[1]U.Amirtha vishah, [2]Dr.P.Marikannu

[1,2] Information Technology Anna University Regional Campus CBE, India

***Abstract*: Disruption Tolerant Network is a network architecture that reduces intermittent communication issues by addressing the problems in networks that cause lack of continuous connectivity. It played a major role in military environment. In military environments connection of wireless devices carried by soldiers may disconnected due to some environmental factors. Disruption Tolerant Network has been introduced to provide a successful solution for that problem. Message Authentication Code (MAC) technique has been used to maintaining the integrity of the message from source to destination. For each round of Message Authentication Code (MAC) generation different key has been generated by Key Distribution Centre (KDC). Here, the message has been encrypted and decrypted using Advanced Encryption Standard (AES) algorithm. Advanced Encryption Standard is a symmetric block cipher that will using the same key for both encryption and decryption at the sender and receiver side.**

***Keywords:* Advanced Encryption Standard (AES), Disruption Tolerant Network (DTN), key, Message Authentication Code (MAC), Storage node, wireless devices.**

I. INTRODUCTION

Network security consists of policies adopted by a network administrator to prevent and monitor unauthorized access, misuse and modification of the messages within the network. Network security involves authorization of access to data in a network. Users choose or assigned an ID and secret code to authenticating information that allow access within their authority. Network security have a variety of computer networks, both public and private networks, which are used in conducting transactions and communications among business, government agencies and individuals. Sometimes networks can be private within a company, and for others to be open to access. Network security secures the network as much as protected.

The most common and the simple way of protecting a network resource is by assigning username and password. The basic security for large business may requires high-maintenance and advanced software and hardware in the direction of prevents attacks like hacking and spamming. Network security starts with authenticating username and password and it is termed as one-factor authentication. With the two-factor authentication, something user 'has' also used and for three-factor authentication then the user 'is' used once authenticated (e.g. fingerprint or retinal scan).

An attribute-based encryption secure data retrieval scheme using CP-ABE for decentralized DTNs. In the first way, attribute revocation enhances the backward/forward secrecy of confidential data by reducing the vulnerability. Then Second encryptor can define a fine-grained access policy using monotone access structure. Third, the key escrow problem is resolved by an escrow-free key issuing protocol.The key issuing protocol generates the user secret keys by a secure two-party computation (2PC) protocol among the key authorities with their own secrets information using those keys. The two-party computation (2PC) protocol defines the key authorities from obtaining any master secret information of each other. Then the users need not to fully trust the authorities in order to protect their data to be shared. Then the confidential

data and privacy can be protected from the curious key authorities. The key authorities consist of a single central authority and multiple local authorities.

Many secure and reliable communication channels between a central authority and each local authorities during the initial key set up 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 their user attributes. The key authorities are assumed to be honest-but-curious. They will honestly execute the assigned tasks in the system but they like to learn information of encrypted contents. This is an entity who owns the confidential messages or data and to store the information into the external data storage node for ease of sharing or for reliable delivery to users in the networking environments. A sender is responsible for defining access policy and enforcing its own data by encrypting the original data under the policy before storing it to the storage node.

II. LITERATURE SURVEY

Secure data retrieval based on cipher text policy attribute-based encryption:

Ciphertext policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. The problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. It demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data has been dustributed over the disruption-tolerant military network. There are four main modules has been deal in this paper they are sender, user, storage node and Key authorities. The central key authority has been connected with the many local authorities and issuing the key to both the sender and receiver.

Multi-authority attribute-based encryption:

A user first formulates his access policy for encrypting a message. Depending on the construction the form of this policy may be a Boolean formula, a different formalism or a linear secret sharing scheme. The user can finally encrypt an information under a policy by using public keys corresponding to set of attributes at the user side. To decrypt a cipher text a user needs at least access to some set of attributes which satisfies the access policy. There is only one challenge at multi-authority CP-ABE as an extension of multi-authority threshold ABE construction. However, the scheme does not make available the full flexibility of DABE scheme and can only be used for a constrained type of contact policies. We first define the concept of Distributed characteristic- Based Encryption and introduce the attacker model considered in the employment subsequently. There are two DABE construction the first one is very efficient, but its security can be proven only in an idealized model and the second construction is a uncomplicated extension of a recent work by Waters can be proven secure under a number-theoretic assumption, but is less efficient and requires a weaker invader model. The user can finally encrypt a message under a policy by using the public keys corresponding to the attributes occurring in the policy. To decrypt a cipher text, a user needs at least access to some set of attributes which satisfies the access policy. There is only one challenge at multi-authority CP-ABE, proposed by as an extension of her multi-authority threshold ABE construction. But the scheme does not make available full flexibility of DABE scheme and can only be used for a constrained type of contact policies.

Removing escrow from identity-based encryption:

Identity-Based Encryption (IBE) is an alternative approach to public-key encryption. IBE eliminates the need for a Public Key Infrastructure (PKI). PKI or identity-based encryption must provide a means to revoke users. Efficient revocation is a well-studied problem in the traditional PKI. In the setting of IBE, there has been little work on revocation mechanisms. The solution requires the senders to use time periods when encrypting and all the receivers to update their secret keys frequently contacting the trusted authority. But it does not scale well as the number of users increases the key updating frequently becomes a bottleneck. We propose an IBE scheme that significantly improves key-update efficiency on the side of the trusted party, while staying efficient for the users. Our scheme builds on the ideas of the Fuzzy IBE primitive and binary tree data structure is provably secure.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (82-87), Month: January-April 2016, Available at: www.noveltyjournals.com

Decentralizing attribute-based encryption:

Decentralized ABE schemes in the multi authority network environment. They achieved a combined access policy over the attributes issued from different authorities by encrypting the original data multiple times. The main disadvantages of this approach are expressiveness and then efficiency of access policy. Thus the access policy which can be achieved by encrypting a message and then encrypting the resulting cipher text with by and then encrypting resulting cipher text until this multi encryption generates the final cipher text.

Thus, the access logic should be only AND, and they will require an iterative encryption operations where is the number of attribute authorities. It can be restricted in terms of expressiveness of the access policy and it requires computation and storage costs.

III. PROPOSED METHOD

The proposed system using main algorithm is Advanced Encryption Standard (AES). AES is a symmetric block cipher. Using AES encryption and decryption technique the text message can be used to stored and retrieve the message. Both the sender and the receiver needs to use the same key for encrypt and decrypt the message. The text message can be encrypted using AES algorithm then Message Authentication Code (MAC) will be appended with the encrypted message. Then message can be stored in the storage node. The receiver will retrieve the message by comparing Message Authentication Code (MAC). If the Message Authentication Code (MAC) same means on that case remove the Message Authentication Code (MAC). Finally decrypt the message using Advanced Encryption Standard (AES) decryption. If it is not same means, then the process will be drop.

A. System Architecture:

The architecture for the proposed method is explained in the Fig 1.

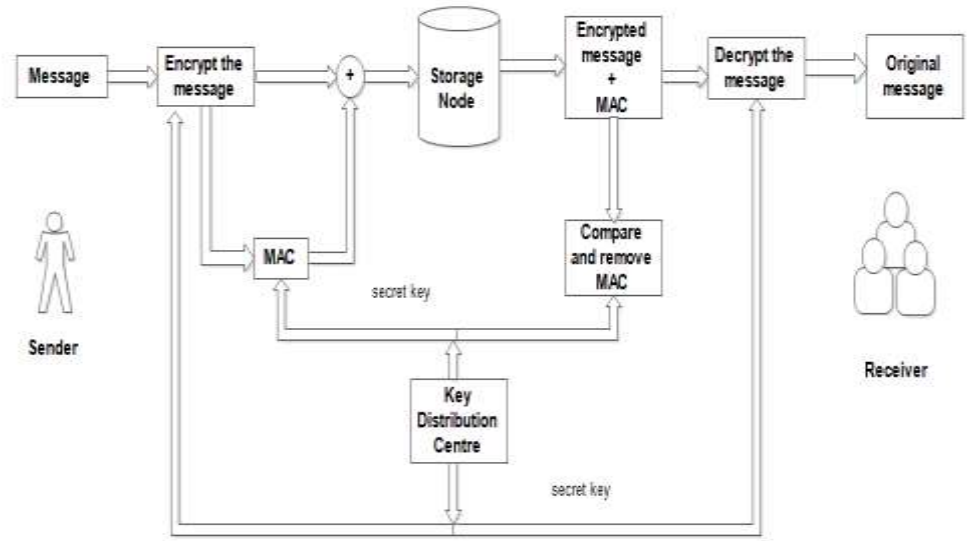

Fig 1.

B. Implementation:

➢ ***Key Distribution Centre*:** Generate the different key for each round of process. Both the sender and the receiver use the same key.

➢ ***Sender:*** 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.

➢ ***Receiver:*** This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses the set of policies will decrypt the message. Finally get the original message.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (82-87), Month: January-April 2016, Available at: www.noveltyjournals.com

- ***Storage node:*** It stores the data from senders and provide corresponding access to users.

IV. ANALYSIS AND RESULTS

The result produced here is the output of file transform using AES algorithm. The sample output of the download the original message without modification at the receiver side is also obtained at the end of this experiment is also shown in this paper.

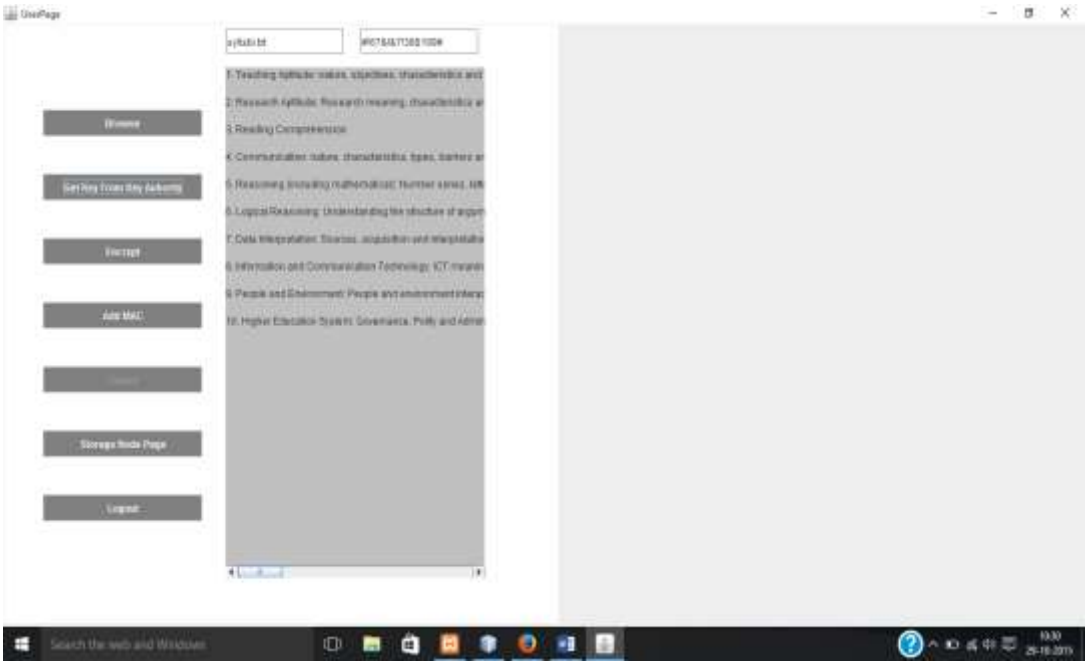

Fig.2 Getting Key

The above figure 2 shows that for encrypting the message the sender needs to get the key from key distribution centre.

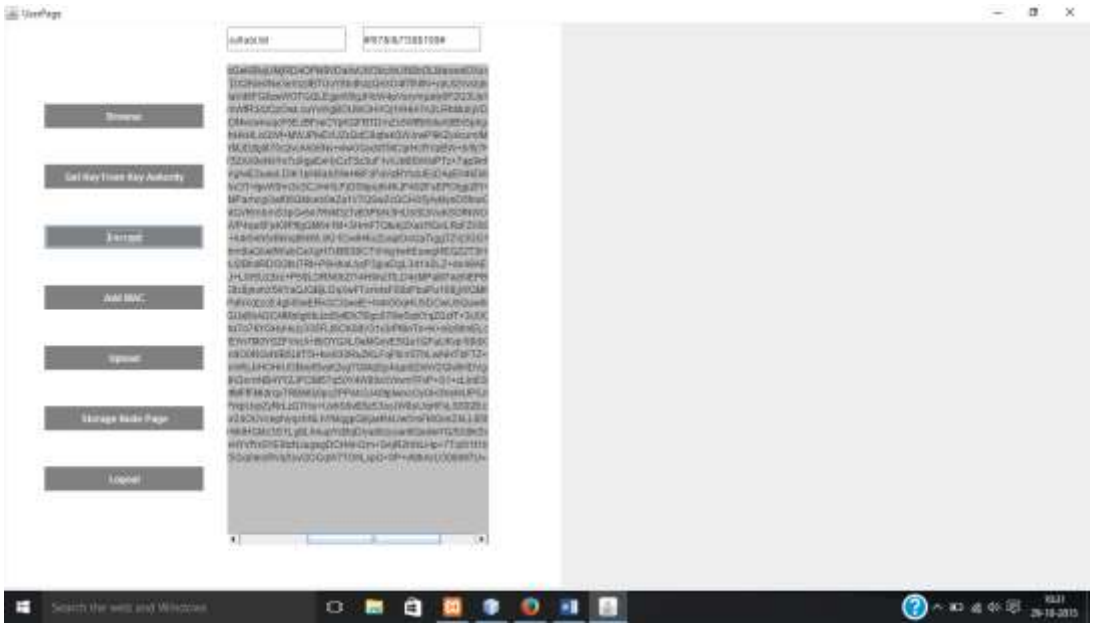

Fig.3 Encrypting the message

The above figure 3 shows that encrypting the original message using key from the key distribution centre.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (82-87), Month: January-April 2016, Available at: www.noveltyjournals.com

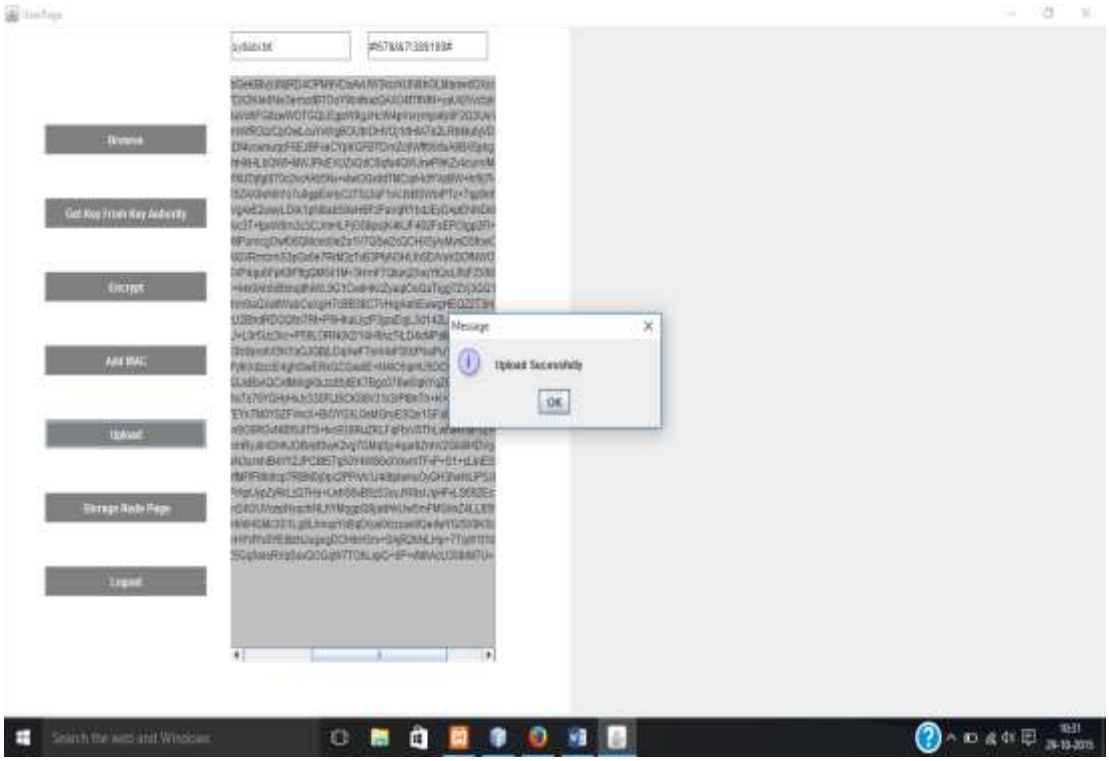

Fig.4 Uploading page

The above figure 4 shows sender will uploading the encrypted message to be stored into the storage node.

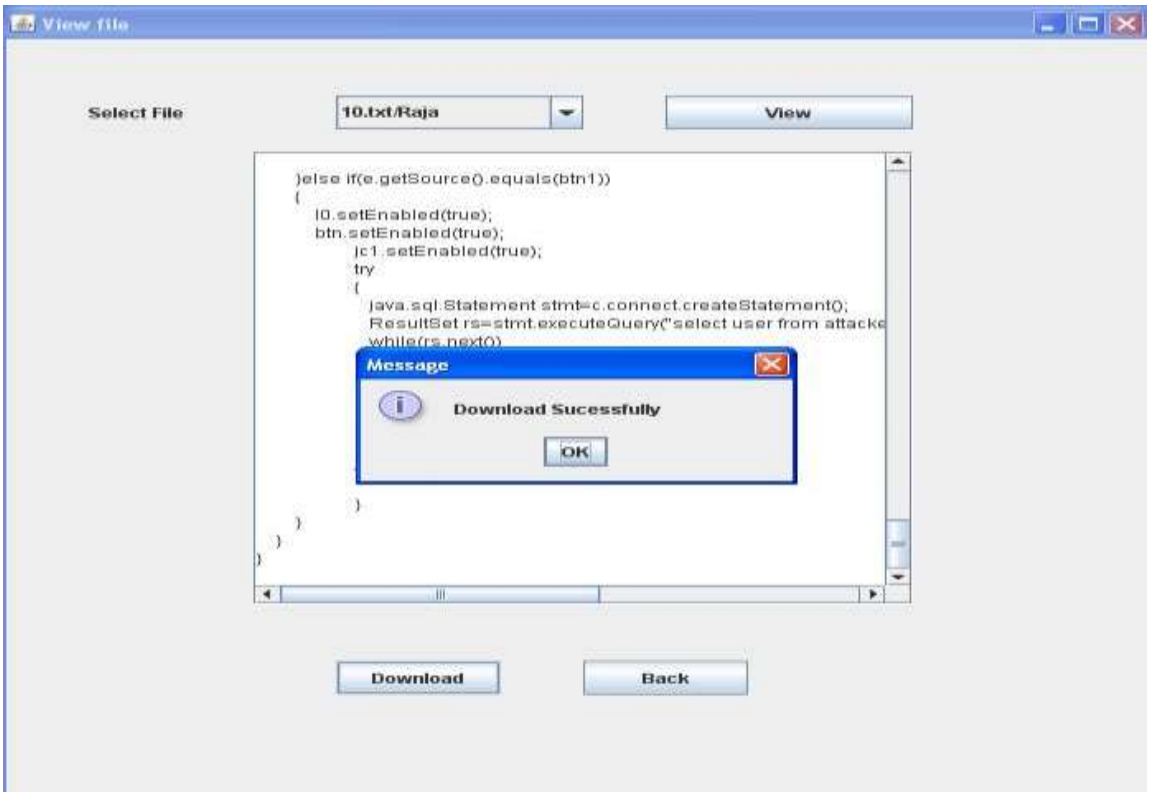

Fig.5 Sample output

The above figure 5 shows that sample output for download successfully the file at the receiver side.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (82-87), Month: January-April 2016, Available at: www.noveltyjournals.com

V. CONCLUSION

The proposed method is designed to making the confidentiality and integrity of the message to be secure while transforming the message from one place to other. I have completed making the original message in an encrypted form by getting key from the key distribution Centre (KDC) and encrypted using Advanced Encryption Standard (AES) algorithm. The encrypted message will successfully store in the database. In the receiver side needs to decrypt the message by comparing the integrity of the message authentication code. Finally decrypt the message in level of both confidentiality and integrity.

Steganography technique has been used to making secured transformation using image as a future work. Which means that hiding the file behind the image which would be more convenient for security purpose.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang "Secure Data Retrieval for Decentralized Disruption-Tolerant Military", *Member IEEE, ACM*, 2012.

[2] S. Roy and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[3] M. Chase, "Multi-authority attribute based encryption," inProc. TCC, LNCS 4329, pp. 515–534, 2007.

[4] S. S. M. Chow, "Removing escrow from identity-based encryption," in Proc. PKC, LNCS 5443, pp. 256–276, 2009.

[5] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep.2010/351, 2010.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," inProc. ASIACCS, pp. 261–270, 2010.

[7] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," inProc. IEEE MILCOM, , pp. 1–7, 2007.

[8] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," inProc. ACM Conf. Comput.Commun. Security, pp. 121–130, 2009.