International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Decentralised Disruption Tolerant Military Network

Mouneshwara, H. P. Mohan Kumar
MCA Department, P.E.S. College of Engineering, Mandya, Karnataka, India

ABSTRACT

Disruption Tolerant Network technologies allow wireless devices carried by soldiers in military networks and access the confidential information by storage nodes. Data to be stored and retrieved from storage nodes, since the data handled by the soldiers are different, it is necessary to implement the security policy and access control policy to them. The authorization policies and secure data retrieval by soldiers are the key issues in DTN. Ciphertext Policy Attribute Based Encryption is a cryptographic resolution to the access control issues and fulfills the necessities for secure text retrieval in DTNs. To transmitting the secret image in DTN, Visual Cryptography Schemes are used. These schemes are used to hide the secret information in images. To support both text and image retrieval in DTN, the proposed algorithm can be enhanced. However, previous approach suffers attribute revocation problem in information, pixel expansion and noise problem in images. The proposed system provides secured retrieval of text and image, using Multiauthority CP-ABE with Data Revocation and customized GAS algorithm for decentralized disruption tolerant military network respectively. On demonstrating the proposed system, the private information is secured and efficiently managed in Disruption Tolerant Military Network.

Keywords : Access-control, Attribute-based encryption (ABE), Interruption-tolerant Network (ITN), Multiauthority, Secure Data Retrieval.

I. INTRODUCTION

A new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

II. RELATED WORKS

ABE comes in two flavors called key-policy ABE (KP-.ABE) and Cipher text policy attribute-based encryption[1]. 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[1],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[2]. Interruption tolerant network (DTN) advances are getting to be effective arrangements that allow nodes to speak with one another. Commonly, when there is no end-to-end association between a source and a destination combine, the messages from the source node may need to sit tight in the transitional nodes for a generous measure of time until the association would be in the long run set up. After the association is in the long run set up, the message is conveyed to the destination node. Roy and Chuah presented storage nodes in DTNs where information is stored or duplicated such that just approved portable nodes can get to the vital information rapidly and productively[3], The idea of characteristic based encryption (ABE) [4] is a guaranteeing approach that satisfies the necessities for secure information recovery in DTNs. ABE characteristics an instrument that empowers a right to gain entrance control over scrambled information utilizing access approaches and attributed qualities among private keys and ciphertexts. Especially, Ciphertext-policy attribute-based encryption gives an adaptable method for scrambling information such that the encryptor characterizes the characteristic set that the decryptor needs to have with a specific end goal to unscramble the ciphertext. Nowadays A fundamental characteristic [5] of wireless ad hoc networks is the time difference of the channel potency of the original communication links. Such time difference occur at numerous occasion scales and can be owing to multipath desertion, pathway loss using space attenuation, shadowing by obstacles, and intrusion from extra users. The impact of such time difference on the design of wireless ad hoc networks permeates throughout the layers, ranging from coding and power control at the physical layer to cellular handoff and coverage planning at the networking layer.

System Architecture

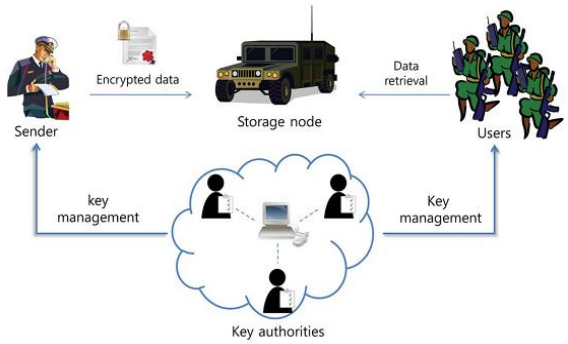

Figure 1. System Description and Assumptions

Fig.1 shows the architecture of the DTN. As shown in Fig1, the architecture consists of the following system entities.

1) KeyAuthorities:They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup 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 the users' attributes. The key authorities are as summed to be honest-but-curious. Thatis, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.
2)Storagenode :This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [4], [5]. Similar to the previous schemes, we also assume the storage node to be semitrusted, that is honest-but-curious. 3)Sender: This is 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. A sender is responsible for defining (attributebased) access policy and enforcing it on its own data by encrypting the data under the policy before storing into the storage node.

4) User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses asset of attributes at is flying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

III.SYSTEM ANALYSIS

Existing System

Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides.

Proposed System

Although we proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, proposed a distributed access control mechanism in cloud However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. In the preliminary version of this paper, we extend our previous work with added features that enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. In this version we also address user revocation, that was not addressed. We use ABS scheme to achieve authenticity and privacy. Unlike our scheme is resistant to replay attacks, in which a user can replace fresh data with stale data from a previous write, even if it no longer has valid claim policy. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud. We, therefore, add this extra feature in our scheme and modify appropriately. Our scheme also allows writing multiple times which was not permitted in our earlier work.

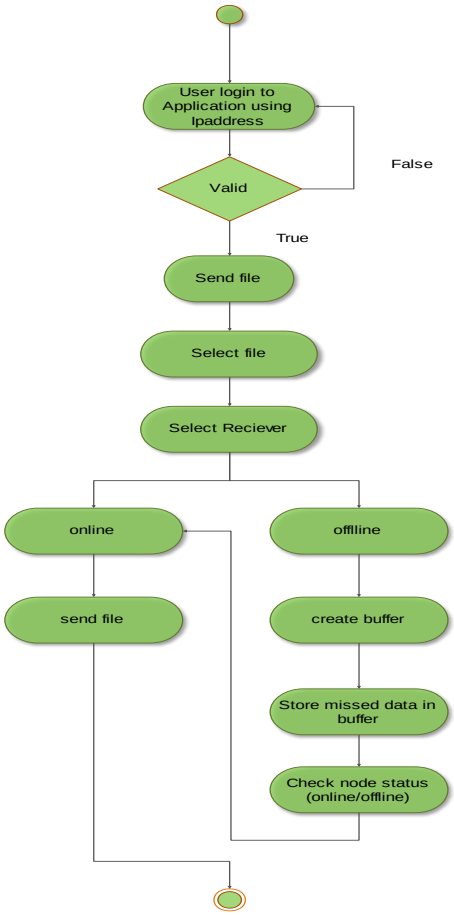

Figure 2 : Activity Diagram

The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement. Efficient search on encrypted data is also an important concern in clouds. The fig:2 it shows complete work flow of the admin .The clouds should not know the query but should be able to return the records that satisfy the query.

III. RESULT

User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides.

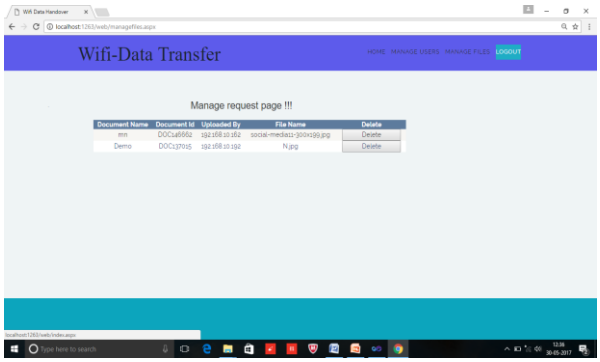

Figure 3 Final Result

VI.CONCLUSION

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.

VII. REFERENCES

[1]. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" IEEE/ACM Transactions on Networking VOL:22NO:1:2014

[2]. Karishma S. Dule M.B. Nagori" Secure Data Retrieval for Decentralized Military Networks" International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 8, April 2015.

[3]. K. Sai Baba,A sandeep kumar,B.Tarskeshwara Rao" Secure Data Retrieval for Decentralized DisruptionTolerant Military Networks" International Journal of Computer Applications (0975 – 8887) Volume 132 – No.17, December2015

[4]. Korra Bichya" Secure Information Recovery for Decentralized Interruption Tolerant Defense Data Network" International journal of computer engineering in research trends volume 1, issue 3, september 2014, pp 119-126.

[5]. K. Kalaiselvi and B.Kabilarasan " Cipher Text-Policy Attribute based Encryption for Secure Data Retrieval in Disruption-Tolerant Military Networks (DTN)" International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 11 Issue 3 –NOVEMBER 2014.

[6]. Umoh Bassey Offiong M. B. Mukeshkrishnan" Securing Data Retrieval for Decentralized DisruptionTolerant Military Networks (DTNs) using Cipher textPolicy Attribute-Based Encryption " International Journal of Engineering Trends and Technology (IJETT) – Volume 26 Number 5- August 2015

Authors:

Mouneshwara, received has Bachelor's degree in Computer Applications from Gulbarga University, India and he is currently pursuing MCA in VTU, India.

Mohan Kumar H P, obtained MCA, MSC Tech and PhD from University of Mysore,India in 1998,2009 and 2015 respectively.He is woking as a professor in department of MCA, PES College of Engineering, Mandya, Karnataka, India. His areas of interest are biometric, video analysis and networking and Data Mining.