International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

ABE Data Transfer viva Key Authorities between Sender & Reviser by using Strong Nodes

K.Naresh[1]& K.Lalitha[2]

[1]M-Tech Dept. of CSE from Aurora's Scientific, Technological and Research Academy Email: - knareshm03@gmail.com

[2]Associate Professor Dept. of CSE from Aurora's Scientific, Technological and Research Academy Email: -lalithakurma06@gmail.com

Abstract-

In military environments, like battlefield or a hostile region, the mobile nodes might suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technology is the successful solution 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. Here, authorization policies are needed in order to retrieve the data securely. Ciphertext-policy attribute-based encryption (CP-ABE) can be provided as the cryptographic solution for the control issues. CP-ABE is applied to the decentralized DTNs. It introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. Here, a scheme where decentralized DTNs use CP-ABE with multiple key authorities to manage their attributes with mutual communication is used.Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming 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. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval.

KEYWORDS: Disruption Tolerant Network (DTN); secure data retrieval; Trust Management; intrusion detection; Attribute Based Encryption

1. INTRODUCTION:

The design of the current Internet service models is based on a few assumptions such as (a) the existence of an end to-end path between a source and destination pair, and (b) low round-trip latency between any node pair. However, these assumptions do not hold in some emerging networks. Some examples are: (i) battlefield ad-hoc networks in which wireless devices carried by soldiers operate in hostile environments where jamming, environmental factors and mobility may cause temporary disconnections, and (ii) vehicular ad-hoc networks where buses are equipped with wireless modems and have intermittent RF connectivity with one another. Requirement in some security-critical applications is to design an access control system to protect the confidential data stored in the storage nodes or contents of the confidential messages routed through the network. As an example, in a battlefield DTN, a storage node may have some confidential information which should be accessed only by a member of „Battalion 6" or a participant in „Mission 3". Several current solutions follow the traditional

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

cryptographic based approach where the contents are encrypted before being stored in storage nodes, and the decryption keys are distributed only to authorized users. In such approaches, flexibility and granularity of content access control relies heavily on the underlying cryptographic primitives being used. It is hard to balance between the complexity of key management and the granularity of access control using any solutions that are based on the conventional pair wise key or group key primitives. Thus, we still need to design a scalable solution that can provide fine-grain access control. That is a DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

Fig.1. Military Networks

2. RELATED WORK

Existing System

In CP-ABE, authority's master secret key is used to generates private keys of users associated set of attributes. So, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries 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 inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal problem The concept of attribute-based encryption (ABE) full fills the requirements for secure data retrieval in DTNs. It provides an access control over encrypted data using access policies and attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encrypt or defines the attribute set that the decrypt or needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy. However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point, or some private keys might be compromised, key revocation for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during re-keying procedure or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

Proposed System

This Section focus on how to overcome the above drawback by using a new technique called ETMS. The motive is to make a secure data retrieval in DTN. it can be achieved by using Efficient Trust Management Scheme. In addition to this Geographical Routing Algorithm is introduced for finding the Neighbor nodes or users in the extreme

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Military Network. ETMS: In order to detect the misbehaving nodes with less computation, an innovative technique is introduced which called Efficient Trust management system (ETMS) and using geographical is routing to identify the location of the nodes in the network. This method can learn from past experiences and adapt to changing environment conditions to maximize application performance and enhance operation agility. The learning process and adaptive designs of trust management system are reflected in trust aggregation, trust propagation and trust formulation. For trust composition, aggregation and propagation, firstly explore novel social and QoS trust components and then devise trust aggregation and propagation protocols for peer-to-peer subjective trust evaluation of individual social and QoS trust components, and prove the accuracy by means of theoretical analysis with simulation validation. For trust formation, explore a new design concept of mission-dependent trust formation with the goal of application performance optimization, allowing trust being formed out of social and QoS trust properties. Dynamic trust management is achieved by first determining the best trust formation model given a set of model parameters specifying the environment conditions, and then at runtime this trust system learns and adapts to changing environment conditions by using the best trust formation model identified from static analysis. We use a misbehaving node detection application as an example for which we identify the best application-level drop-dead trust threshold below which a node is considered misbehaving, and that the minimum trust threshold can be adjusted in response to changing conditions to minimize the false alarm probability.

3. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective

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 a set of attributes satisfying 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

Key Authorities: 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 assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system; however they would like to learn information of encrypted contents as much as possible.

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 (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

Storage Nodes: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

previous schemes, we also assume the storage node to be semi-trusted that is honest-but-curious.

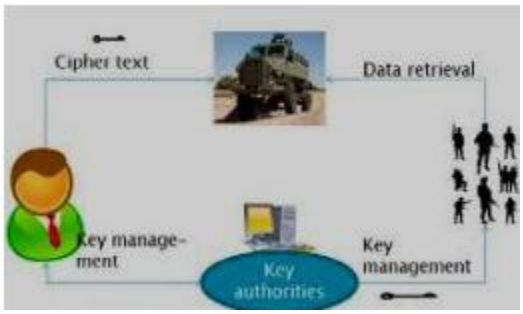

Fig:-2 Flow of the Project

4. EXPERIMENTAL RESULTS

Fig:-3 Key Login Frame

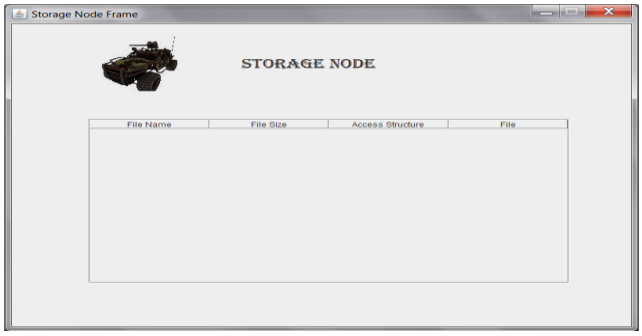

Fig:-4 Strong Node Frame

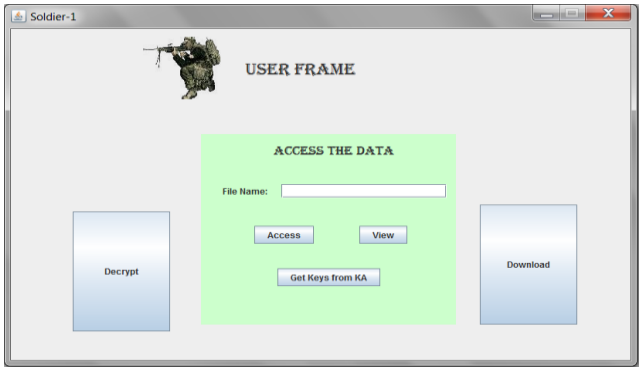

Fig:-5 Users Frame

Fig:-6 Senders Frame

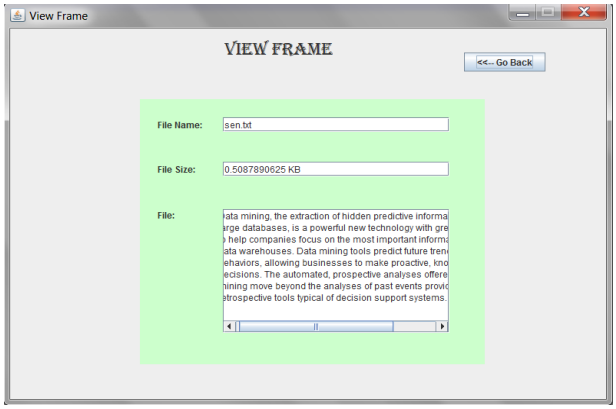

Fig:-7 Results

5. CONCLUSION

The secure and efficient data retrieval will be provided while communicating through the wireless devices, in order to communicate with each other and access the confidential information reliably by exploiting external storage nodes. And the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. When a user keyed in some attributes that matches or corresponds with the one in the access policy, it is updated to match with the group attributes which provides security for group members. We show how to apply the proposed scheme in securing and effectively manage the confidential data distribution in the DTN network.

6. FUTURE WORK:

Besides, we plan to investigate the feasibility of incorporating value compare predicates in policy tree in the future so that the sender can control the lifetime of attributes

7. 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 contentbased information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7. [6] M. Kallahalla, E. Riedel, R.

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

[7] 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.

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

[9] 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.

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