IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue3)
Available online at www.ijariit.com

Secure Data Retrieval for Decentralized Disruption Tolerant Military Networks

S. Anitha
Krishnasamy College Of Engineering and Technology, Anna University
narmathani19@gmil.com

K. Induja
Krishnasamy College Of Engineering and Technology, Anna University
indhuriya1995@gmail.com

N. Ramya
Krishnasamy College Of Engineering and Technology, Anna University
ramya8695@gmail.com

R. Sathishkumar
Krishnasamy College Of Engineering and Technology, Anna University
sathishkumar635@gmail.com

Abstract: 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. Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. Especially, Cipher text-Policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encrypt defines the attribute set that the decrypt 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.

Keyword: Data Retrieval, Encrypt, Decrypt, Storage Node, Cipher Text-Policy.

I.INTRODUCTION

The concept of attribute-based encryption is a promising approach that fulfills the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed 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 defines the attribute set that the decrypt 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.

In this project, propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements first, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.

Second, encrypt can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets.

The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

II.SYSTEM ANALYSIS

A .Existing System

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts 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 (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. 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 rekeying procedure or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

Disadvantage

- 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 (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure.
- The last challenge is the coordination of attributes issued by different authorities. When multiple authorities manage and issue attributes keys to users independently

  With their own master secrets, it is very hard to define fine-grained access policies over attributes issued by different authorities.

B. Proposed System

Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encrypt defines the attribute set that the decrypt 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. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, 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 open problem.

Advantage

- **Data confidentiality:** Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.
- **Collusion-resistance:** If multiple users collude, 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.

C. System Requirements

Software Requirements

Operating System: Windows7 32-bit Ultimate OS.
Front End: PHP
Back End: MY SQL
Programming tool: Dreamweaver

Hardware Requirements:-

System : Pentium IV 2.4 GHz.
Hard Disk: 40 GB.
Monitor: 14' Colour Monitor.
Mouse : Optical Mouse.
Ram : 512 Mb

D. List of Modules

1. Key Authorities

2. Storage Node

3. Sender

4. Soldier (User)

5. CP-ABE Method

E. Module Description

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.

Storage Node

This is an entity that stores data from senders and provides corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi-trusted that is honest-but-curious.

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.

Soldier (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 cipher text and obtain the data.

CP-ABE Method

In Cipher text Policy Attribute-based Encryption scheme, the encrypt can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the cipher text. We propose a method in which the access policy need not be sent along with the cipher text, by which we are able to preserve the privacy of the encrypt This techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

III. DIAGRAMS

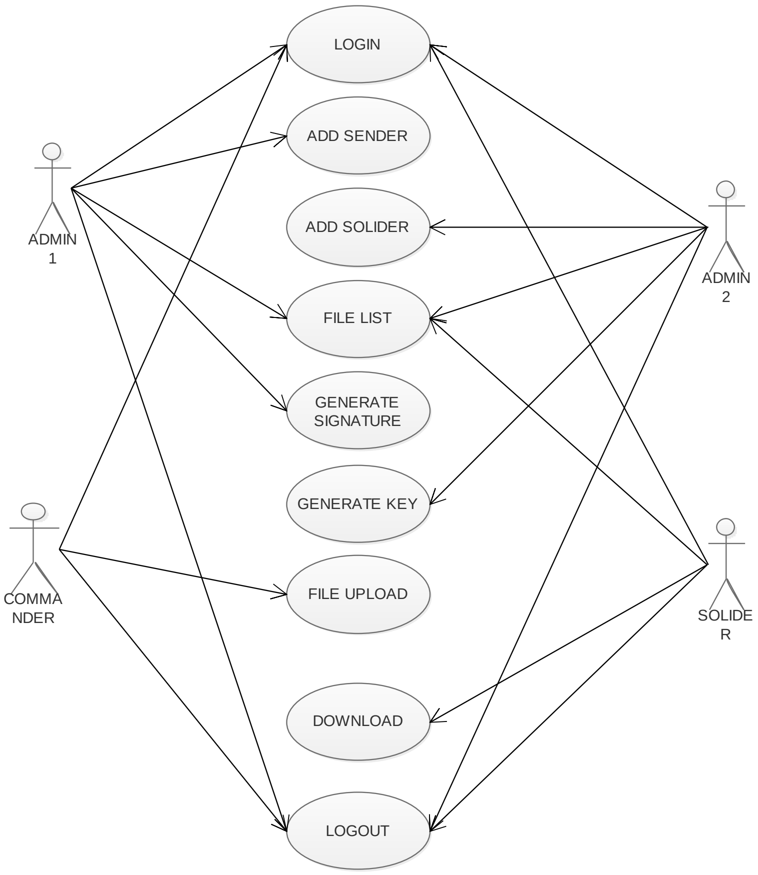
A.UML Diagrams

The Unified Modeling Language (UML) is a general-purpose, developmental, modeling language in the field of software engineering that is intended to provide a standard way to visualize the design of a system.

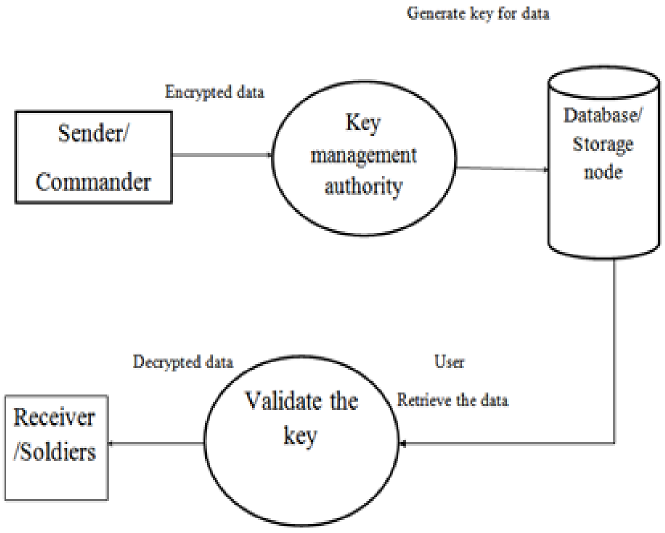
UML was originally motivated by the desire to standardize the disparate notational systems and approaches to software design developed by Grady Booch, Ivar Jacobson, and James Rumbaugh at Rational Software in 1994–1995, with further development led by them through 1996.

In 1997 UML was adopted as a standard by the Object Management Group (OMG), and has been managed by this organization ever since. In 2005 UML was also published by the International Organization for Standardization (ISO) as an approved ISO standard.[2] Since then it has been periodically revised to cover the latest revision of UML.

Use-case Diagram

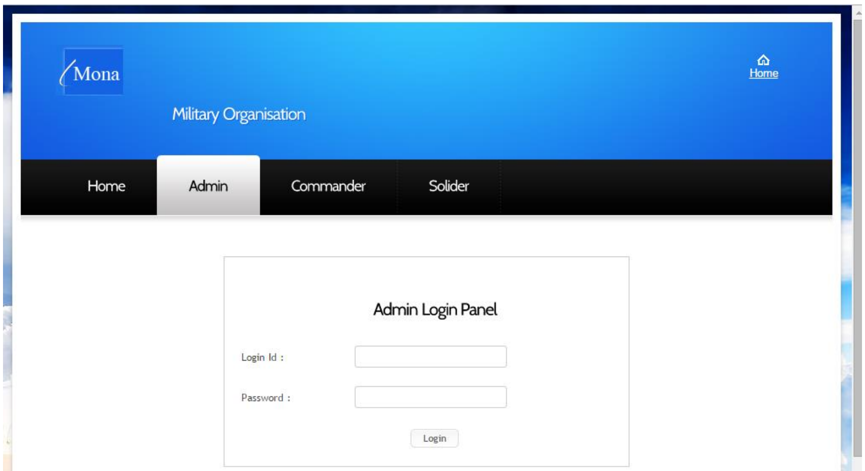


Data Flow Diagram



IV. SYSTEM DEVELOPMENT

Admin 1 and 2 Login:



Admin Login Panel

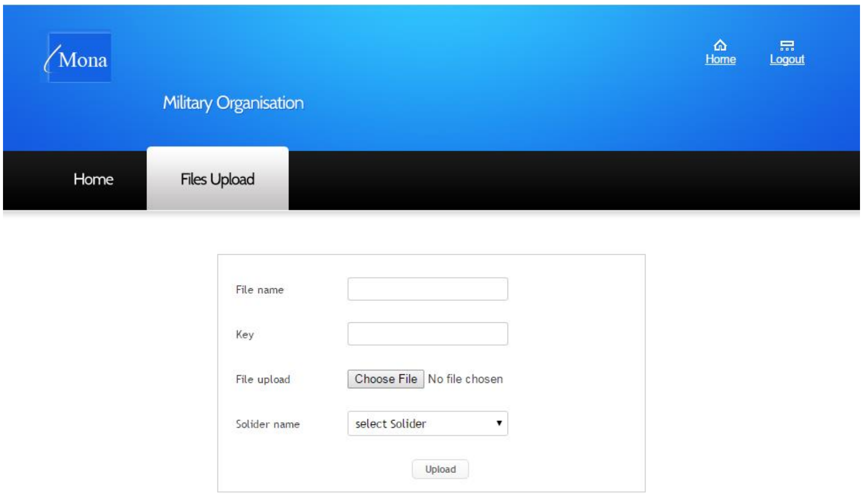
Login Id :

Password :

The administrator will enter the valid user id and password, if not it will display

The invalid username and password message.

Commander File Upload



File name

Key

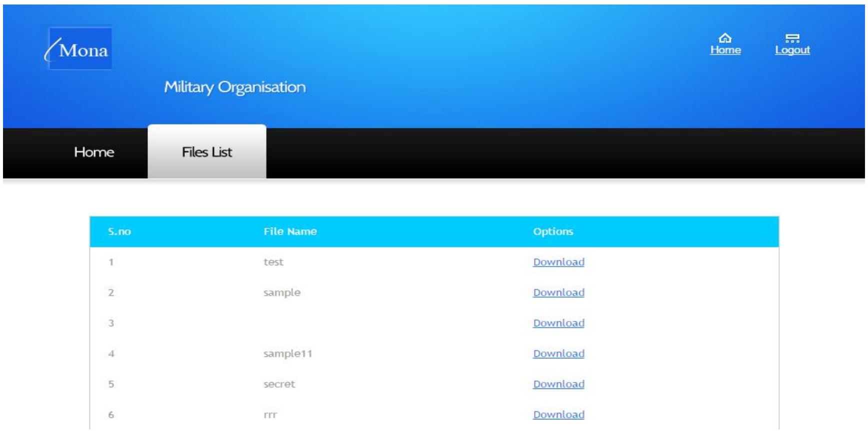
File upload — No file chosen

Solider name — select Solider

Commander can upload file and send to users with an encrypted key and send

Data and at receiver end user need to provide the same to download the files.

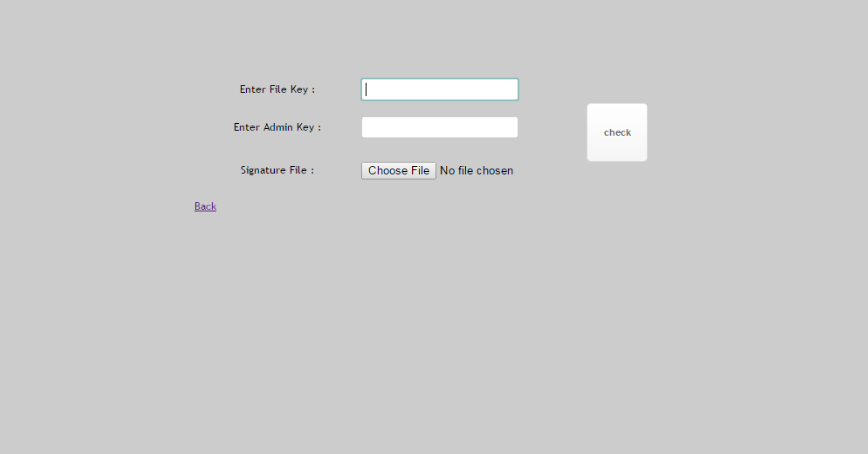
Solider File List



S.no	File Name	Options
1	test	Download
2	sample	Download
3		Download
4	sample11	Download
5	secret	Download
6	rrr	Download

Solider file using to the file list will get in downloaded.

Key Verification



The user can receive the file from more solid by using an encrypted key and then the user download the files.

CONCLUSIONS

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secured data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent 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 not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

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. 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.
4. http://www.w3schools.comttp://www.PHPTutor.com
5. http://www.html.net/tutorials/php/index.html
6. http://www.tutorialspoint.com/mysql/
7. http://www.mysql.com/training/