International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December2016

Secure Data Retrieval for Decentralized Disruption-Tolerant Military Network

P.Yejdani Khan, Department. OF CSE
A1 GLOBAL INSTITUTE OF ENGINEERING & TECHNOLOGY

Vempati.Rajasekhar M.Tech, Computer Science &Engineering
A1 GLOBAL INSTITUTE OF ENGINEERING & TECHNOLOGY
,

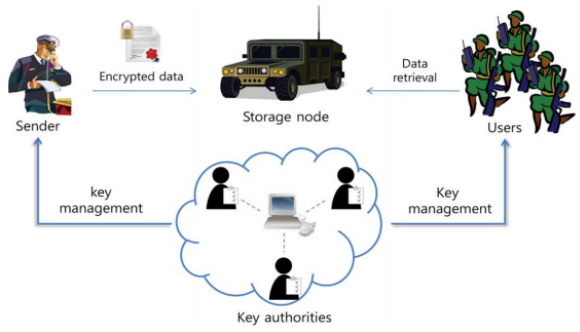
ABSTRACT:

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. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, 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, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the

Introduction

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.

Process diagram



LITERATURE SURVEY

Decentralizing Attribute-Based Encryption

This paper proposed a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their

attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, this system does not require any central authority. In constructing this system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority tied" together different components (representing different attributes) of a user's private key by randomizing the key.

Ciphertext-Policy Attribute-Based Encryption:

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption.

Fuzzy Identity-Based Encryption

This paper introduces a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω0, if and only if the identities ω and ω0 are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, it shows that Fuzzy-IBE can be used for a type of application that it term "attribute-based encryption".

SYSTEM ANALYSIS

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 ciphertexts.

Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to de-crypt the ciphertext.

Thus, different users are allowed to decrypt different pieces of data per the security policy.

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes.

Proposed system

- In this paper, propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.

- It demonstrates how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.
- First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.

Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities

FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

ECONOMICAL FEASIBILITY

TECHNICAL FEASIBILITY

SOCIAL FEASIBILITY

SYSTEM REQUIREMENT SPECIFICATION(SRS)

Introduction

Software Requirements Specification plays an important role in creating quality software solutions. Specification is basically a representation process. Requirements are represented in a manner that ultimately leads to successful software implementation.

2. Requirements may be specified in a variety of ways. However there are some guidelines worth following: -
3. Representation format and content should be relevant to the problem
4. Information contained within the specification should be nested

Software requirements:

- Operating System : Windows 7
- Programming Package : Net Beans IDE 7.3.1
- Coding Language : JDK 1.7

Hardware requirements

- Processor Type : Pentium IV
- Speed : 2.4 GHZ
- RAM : 1 GB
- Hard disk : 80 GB

Functional requirements

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December2016

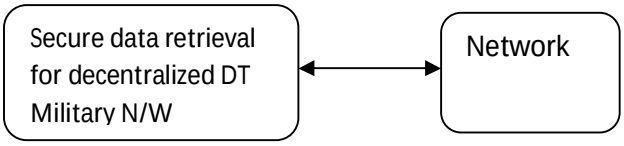
SYSTEM DESIGN

Data Flow Diagram / Use Case Diagram / Flow Diagram

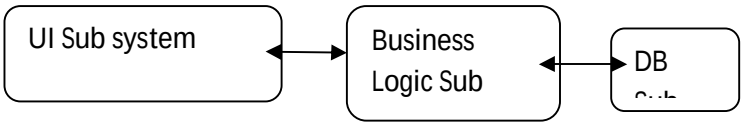
REQ_NO	Requirement
SDRD_01	System should provide provision for key authorization to access attributes.
SDRD_02	System should provide provision for key authorization to central key authority
SDRD_03	System should provide provision for nodes to upload files local key authority
SDRD_04	System should provide provision for key authorization to access personal key generation
SDRD_05	System should provide provision for key authorization to access attribute key generation
SDRD_06	System should provide provision for sender to give his id, region id, file id and file size.
SDRD_07	System should provide provision for sender to upload file.
SDRD_08	System should provide provision for sender to view the file
SDRD_09	System should provide provision for sender to submit the file
SDRD_10	System should provide provision for sender to get keys from key authorities

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system

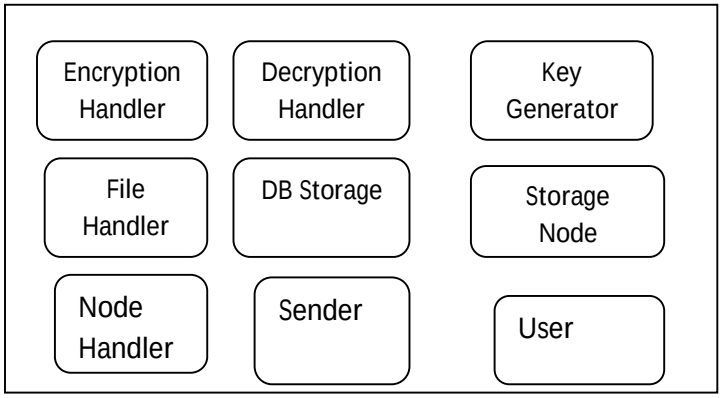
System Design:-



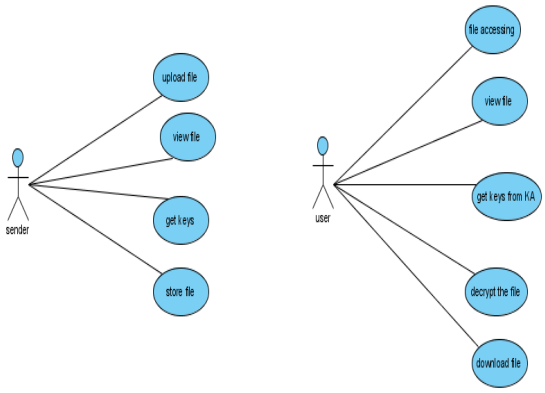
Sub system Design:-

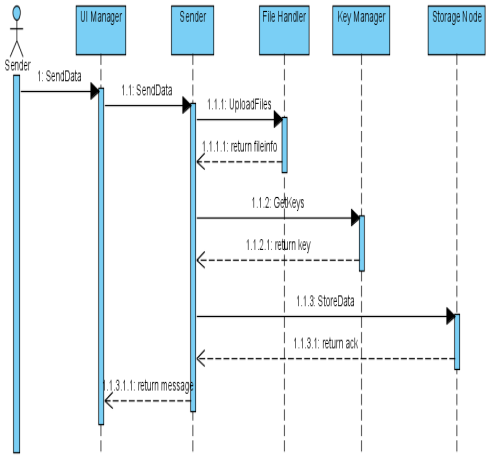


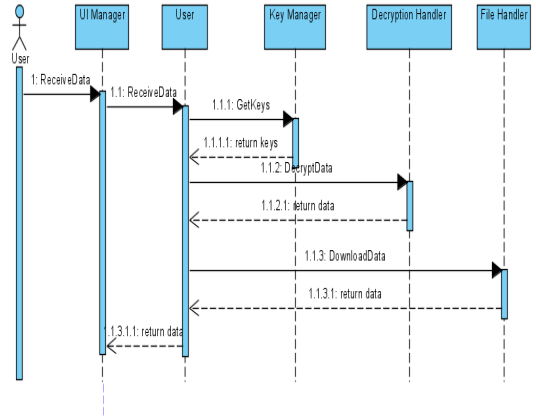
Block Design:-



Sequence diagram







Software Description

Java is a simple and yet powerful object oriented programming language and it is in many respects similar to C++. Java originated at Sun Microsystems, Inc. in 1991. It was conceived by James Gosling, Patrick Naughton, Chris Warth, Ed Frank, and Mike Sheridan at Sun Microsystems, Inc. It was developed to provide a platform-independent programming language.

SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

Unit testing

Integration testing

Functional test

System Test

White Box Testing

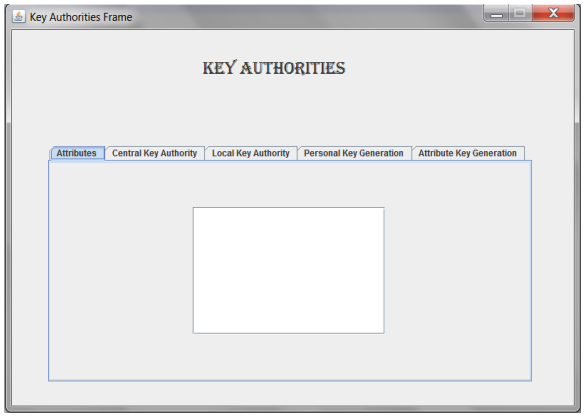
Black Box Testing

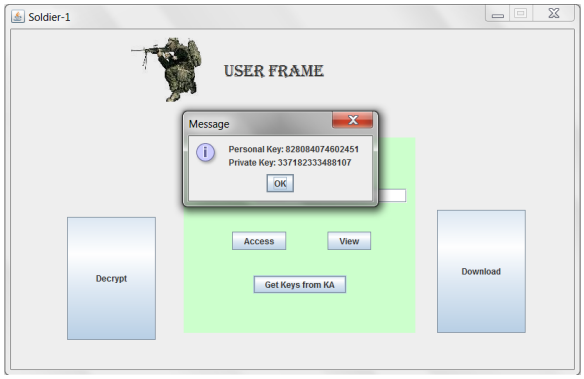
Unit Testing:

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

SCREEN SHOTS





CONCLUSION

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 secure 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.

BIBLIOGRAPHY

- A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
- J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334
- S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp. 261–270.
- A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Computer. Community. Security, 2008, pp. 417–426.
- L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.
- 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.
- A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473