SHARING AND RETRIEVING DATA IN DECENTRALIZED DISRUPTION-TOLERANT MILITARY NETWORKS

[1]S.SURUTHI, [2]C.RAMYA

[1]M.C.A, [2]M.C.A, M.E, ASSOCIATED PROFESSOR,
A.R.J COLLEGE OF ENGINEERING AND TECHNOLOGY, MANNARGUDI.

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. Cipher text-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 confidential data distributed in the disruption-tolerant military network

Keywords : DTN, Mobile nodes, Military network, Network.

I.INTRODUCTION

Due to the factors of environment, mobility and jamming, wireless devices connections carried by soldiers may be disconnected for limited time, particularly when they are operating in hostile of military network scenarios. Through the DTN technologies, Nodes for contact with each other are becoming successful solutions in these environments of extreme networking. Typically, for the time in considerable amount, when there is no end-to-end contact between a source and a destination pair, until the connection would be ultimately produced, there may wait the messages from the source node in the transitional nodes. In DTNs Roy and Chuah introduced storage nodes that data is stored or reflect such that the required information efficiently and quickly can access by only and only authorized mobile nodes. Including methods of access control which are cryptographically enforced. In many cases, policies of data access `are defined over attributes of user or roles, it is desirable for providing the comprehend service access, which are handled by the key authorities. The needs for retrieval of data securely in DTNs are fulfill by the concept of ABE approach. By ABE, a mechanism features that enables an control of access over encrypted data using policies of access and ascribed attributes between cipher texts and private keys. Especially, a scalable way of encrypting data provided by CP-ABE such that to possess in order to decrypt the cipher text, the encrypt or defines the attribute set that the decrypt or needs. Thus, as per the security policies, by different users there are different pieces of data are decrypted. However, there specify the many privacy and security challenges due to the problem of applying the ABE to DTNs. Since, at some point, associated attributes may be alter by some users or for system security, there might be compromised some private keys, and for each attribute is required the revocation of keys. However, especially in ABE systems, this concern is even more difficult, as a group of attribute, we refer to such a collection of users) since by multiple users, each attribute is maybe shared, the other users in the group would be afflicted by revocation of any attribute or any single user in an attribute group. The problem of key escrow is other challenge. In CP-ABE, by applying the master secret keys authority to users connect to the set of attributes, there produce private

II.DESIGN OF PROPOSED SYSTEM

Cipher text-policy provides a scalable way of encrypting data such that the encrypt define 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 user by applying the authority's master secrets keys to users associated set of attributes. Thus, key authority can decrypt every cipher text addressed to specific users by generating their attributes keys. If the key authority is compromised by adversaries when deployed in the hostile environments

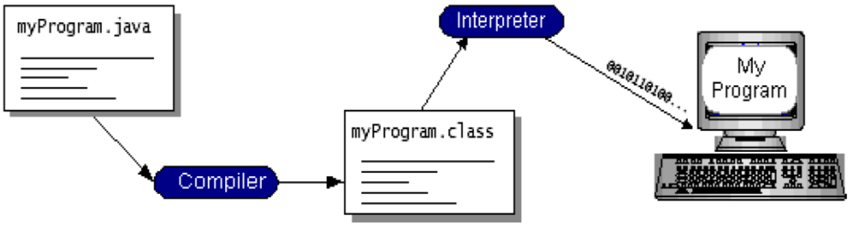


Figure 2.1. Working of java

An application is a standalone program that runs directly on the Java platform. A special kind of application known as a *server* serves and supports clients on a network. Examples of servers are Web servers, proxy servers, mail servers, and print servers. Another specialized program is a *servlet*. A servlet can almost be thought of as an applet that runs on the server side. Java Servlets are a popular choice for building interactive web applications, replacing the use of CGI scripts. Servlet are similar to applets in that they are runtime extensions of applications. Instead of working in browsers, though, servlet run within Java Web servers, configuring or tailoring the server

III.BACK END DESCRIPTION

MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by MySQL AB. MySQL AB is a commercial company, founded by the MySQL developers and now owned by Oracle Corporation. It is a second generation Open Source company that unites Open Source values and methodology with a successful business model.

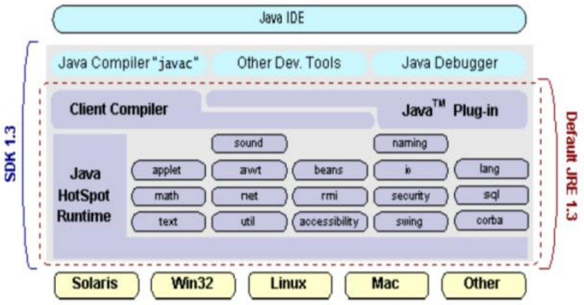


Figure 3.1 Java 2 SDK

URL rewriting is another way to support anonymous session tracking, With URL rewriting every local URL the user might click on is dynamically modified. Or rewritten, to include extra, information. The extra information can be in the form of extra path information, added parameters, or some custom, server-specific.URL change. Due to the limited space available in rewriting a URL, the extra information is usually limited to a unique session.

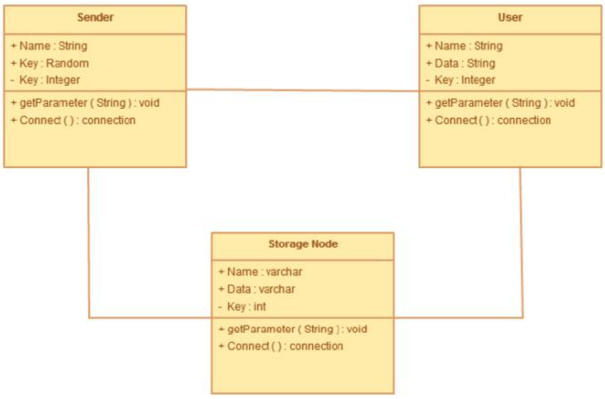
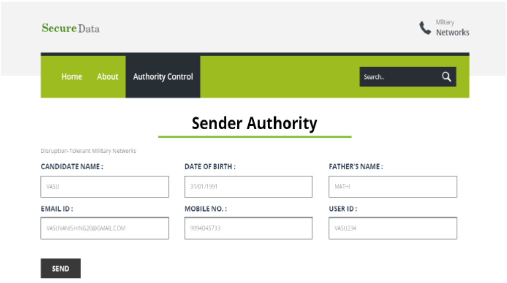

Sender
+ Name : String
+ Key : Random
- Key : Integer
+ getParameter (String) : void
+ Connect ( ) : connection
User
+ Name : String
+ Data : String
- Key : Integer
+ getParameter (String) : void
+ Connect ( ) : connection
Storage Node
+ Name : varchar
+ Data : varchar
- Key : int
+ getParamoter (String) : void
+ Connect ( ) : connection

Figure 3.2 Class Diagram

Servlet invocation is highly efficient, Once a servlet is loaded it generally remains in the server's memory as a single object instance, There after the server invokes the servlet to handle a request using a simple, light weighted method invocation .Unlike the CGI, there's no process to spawn or interpreter to invoke, so the servlet can begin handling the request almost immediately, Multiple, concurrent requests are handled the request almost immediately. Multiple, concurrent requests are handled by separate threads, so servlets are highly scalable

IV.TESTING AND VALIDATION

System testing involves user training system testing and successful running of the developed proposed system. The user tests the developed system and changes are made according to their needs. The testing phase involves the testing of developed system using various kinds of data.An elaborate testing of data is prepared and the system is tested using the test data. While testing, errors are noted and the corrections are made. The corrections are also noted for the future use. The users are trained to operate the developed system. System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points. Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.



Sender Authority

Disruption-Tolerant Military Networks

CANDIDATE NAME : VASU

DATE OF BIRTH : 31/01/1991

FATHER'S NAME : MATHI

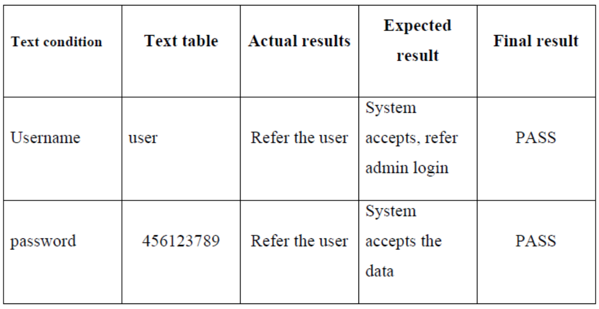
EMAIL ID : VASUVANISHING20@GMAIL.COM

MOBILE NO. : 9994045733

USER ID : VASU234

Figure 4.1 Sample of test case without error

During the deployment design phase of the solution life cycle, you design a high-level deployment architecture and a low-level implementation specification, and prepare a series of plans and specifications necessary to implement the solution. Project approval occurs in the deployment design phase.The whole process has been designed for the user side to enable the standard level of security to their important information and data that has been stored into the cloud. It develops the administrators' performance evaluation in a better way.



Text condition	Text table	Actual results	Expected result	Final result
Username	user	Refer the user	System accepts, refer admin login	PASS
password	456123789	Refer the user	System accepts the data	PASS

Figure 4.2 Testing status

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

V.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..

VI.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 content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.
6. 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.
7. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.
8. 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. 1–8.
9. D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.
10. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.