Protect Knowledge Retrieval for Localized Disruption Tolerant Military Networks

B. Srihari[#1], K.V.G.N.Naidu[*2], P. Nirupama[3]

[1]*M.Tech student,* [2]*Assistant Professor,* [3] *Professor,*

Department of Computer Science & Engineering, Siddharth institute of engineering and technology, Puttur-517583, Andhra Pradesh

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 — *Put your keywords here, keywords are separated by comma.*

I. INTRODUCTION

Networking is basically relating to computers and their connectivity. It is very often used in the world of computers and their use in different connections. The term networking implies the link between two or more computers and their devices, with the vital purpose of sharing the data stored in the computers, with each other. The networks between the computing devices are very common these days due to the launch of various hardware and computer software which aid in making the activity much more convenient to build and use.

Figure 1: Structure of Networking

When computers communicate on a network, they send out data packets without knowing if anyone is listening. Computers in a network all have a connection to the network and that is called to be connected to a network bus (figure1). What one computer sends out will reach all the other computers on the local network (figure 2).

For the different computers to be able to distinguish between each other, every computer has a unique ID called MAC-address (Media Access Control Address) [1]. This address is not only unique on your network but unique for all devices that can be hooked up to a network. The MAC-address is tied to the hardware and has nothing to do with IP-addresses. Since all computers on the network receives everything that is sent out from all other computers the MAC-addresses is primarily used by the computers to filter out incoming network traffic that is addressed to the individual computer [6]. When a computer communicates with another computer on the network, it sends out both the other computers MAC-address and the MAC-address of its own. In that way the receiving computer will not only recognize that this packet is for me but also, who sent this data packet so a return response can be sent to the sender [2].

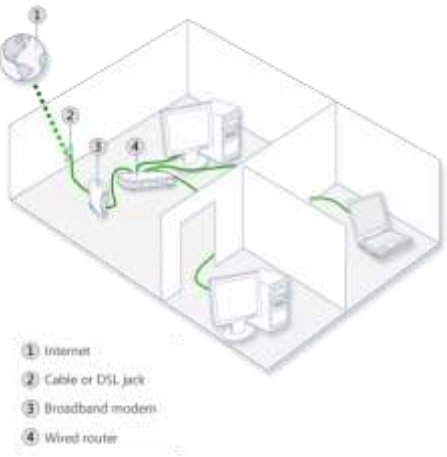

Figure 2: networking functions

On an Ethernet network, all computers hear all network traffic since they are connected to the same bus. This network structure is called multi-drop. One problem with this network structure is that when you have, let say ten (10) computers on a network and they communicate frequently and due to that

they sends out there data packets randomly, collisions occur when two or more computers sends data at the same time. When that happens data gets corrupted and has to be resent. On a network that is heavy loaded even the resent packets collide with other packets and have to be resent again. In reality this soon becomes a bandwidth problem. If several computers communicate with each other at high speed they may not be able to utilize more than 25% of the total network bandwidth since the rest of the bandwidth is used for resending previously corrupted packets. The way to minimize this problem is to use network switches.

Characteristics of Networking:

1) Availability: It is typically measured in a percentage based on the number of minutes that exist in a year. Therefore, uptime would be the number of minutes the network is available divided by the number of minutes in a year.
2) Cost: cost of the network components, their installation, and their ongoing maintenance.
3) Reliability of the network components and the connectivity between them. Mean time between failures (MTBF) is commonly used to measure reliability.
4) Security includes the protection of the network components and the data they contain and/or the data transmitted between them.
5) Speed includes how fast data is transmitted between network end points (the data rate).
6) Scalability defines how well the network can adapt to new growth, including new users, applications, and network components.
7) Topology describes the physical cabling layout and the logical way data moves between components.

Based on the networking components, a system model is proposed in this paper, which shows visual modelling based on the DFD and UML.

II. VISUAL MODELLING

Visual modelling contains both the data circulation plan and the UML blueprints. Modelling is a main part of all the actions that lead up to the implementation of good software. Developed designs to connect the preferred framework and actions of our program. Developed designs to imagine and control the body framework. Developed designs to better understand the program we are building, often revealing the possibilities for generality and recycling. And developed designs to handle risk [3,4]

The DFD (data flow diagram) is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

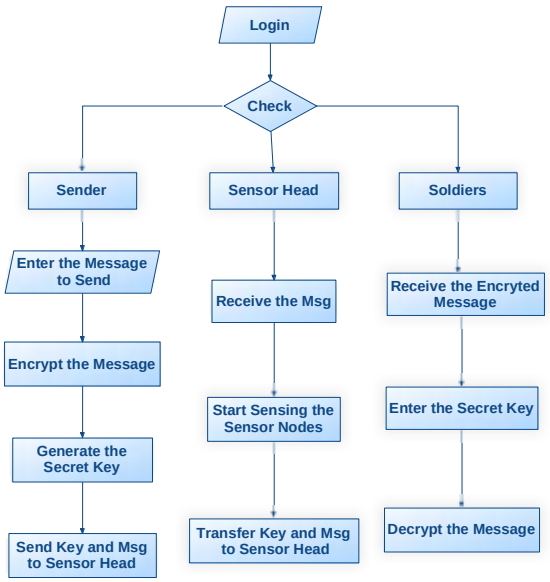

Figure 3: Information flow and functional detail of DFD.

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. UML main goal is to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects[7,8].

The best design of the UML is as follows [5]:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.

4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

III. System Implementation and Results

The system was implemented using Java programme. The results are described in the form of screen shots, which will show the complete process of execution (figure 4 to 13).

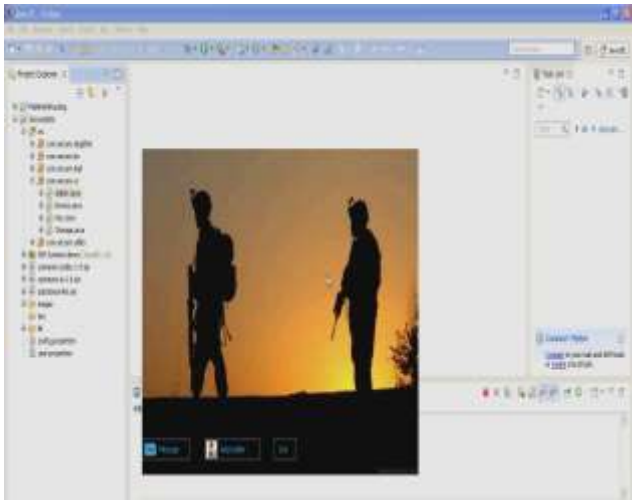

Figure 4: Login to secured system

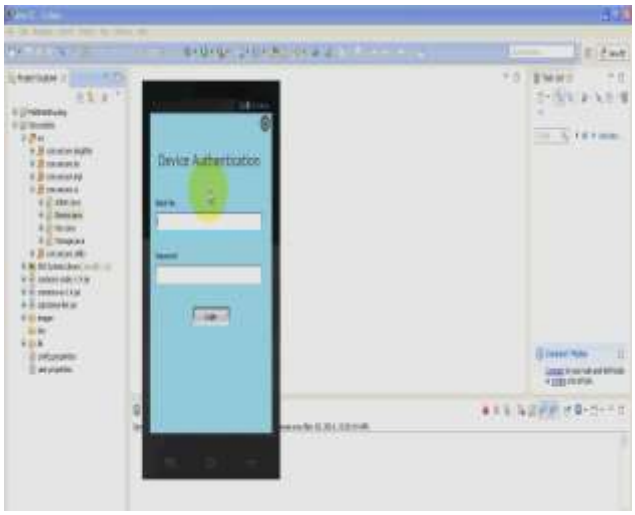

Figure 5: user authentication and keyword

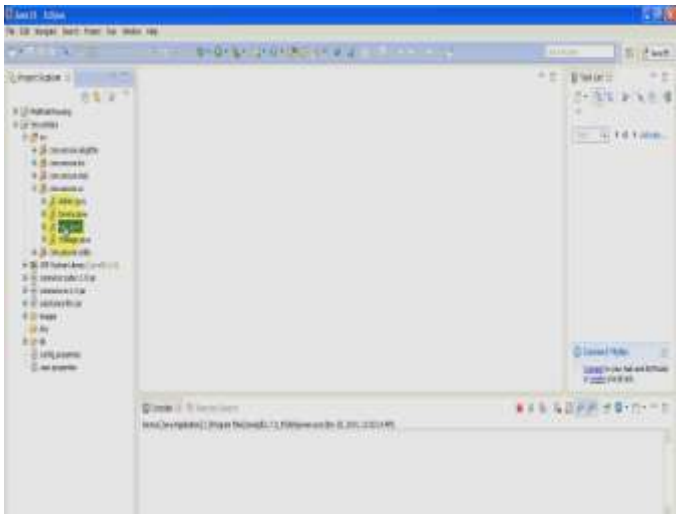

Figure 6: Securing login in the database

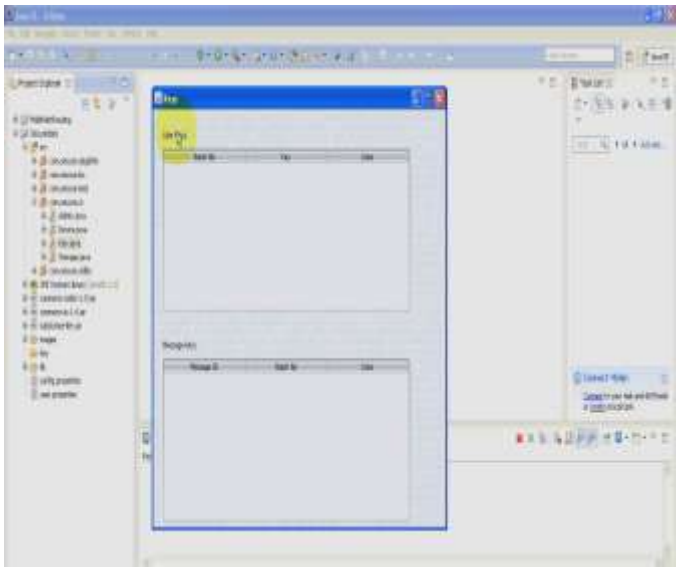

Figure 7. Pop-up for the database entry

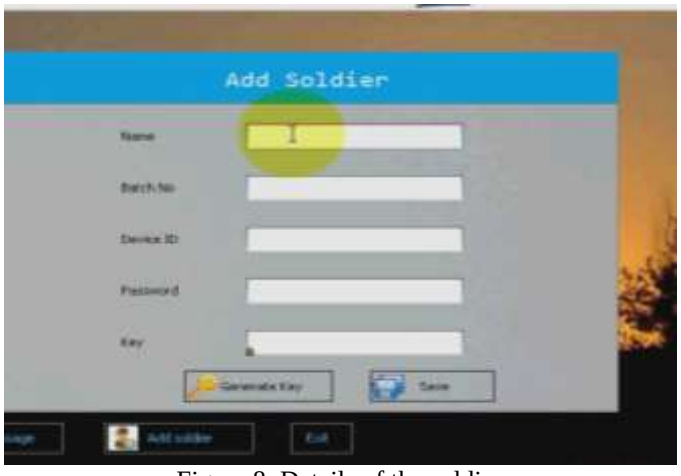

Figure 8: Details of the soldier

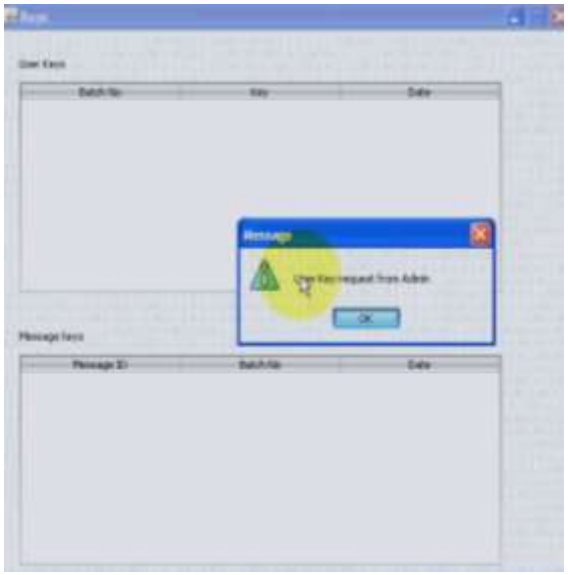

Figure 9. Requesting key from administrator

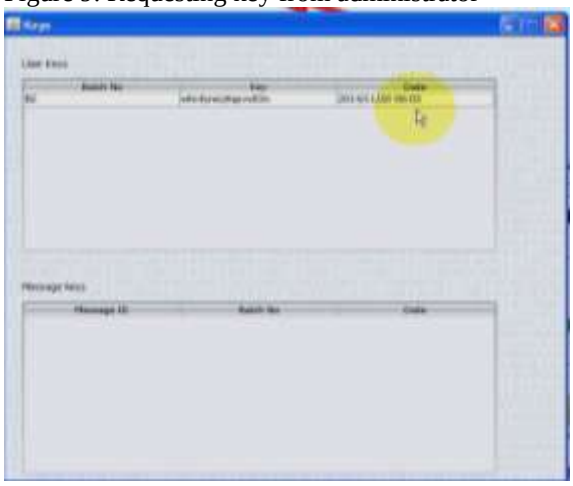

Figure 10. Key generation followed by secure login

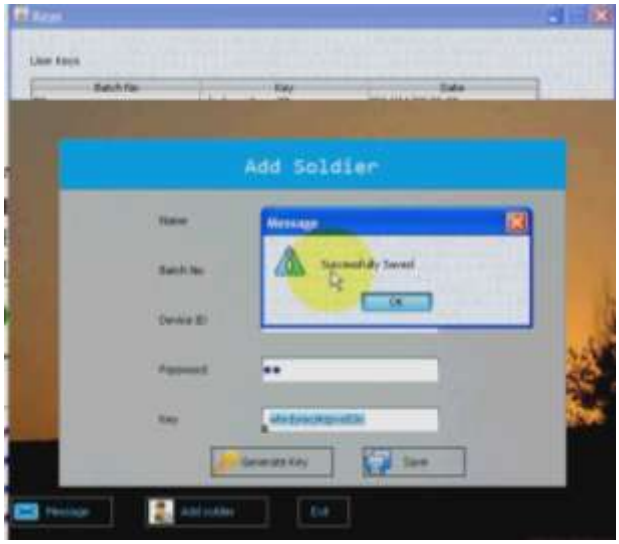

Figure 11. Saved the database

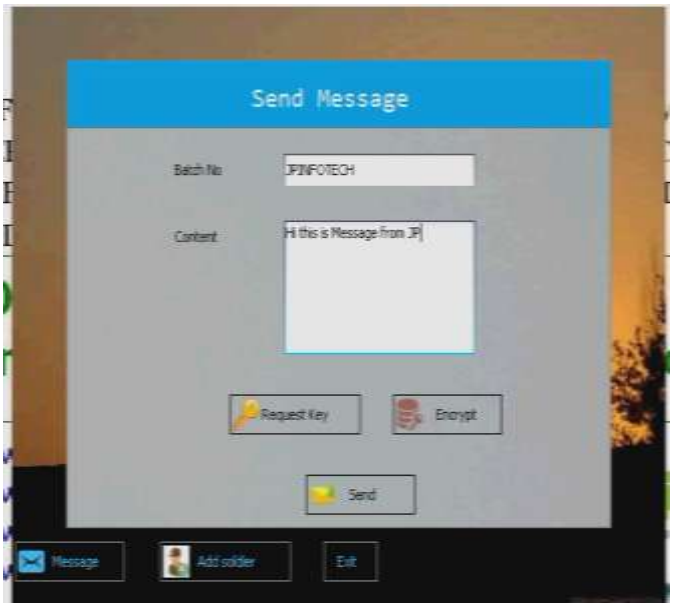

Figure 12. data sharing followed by encryption

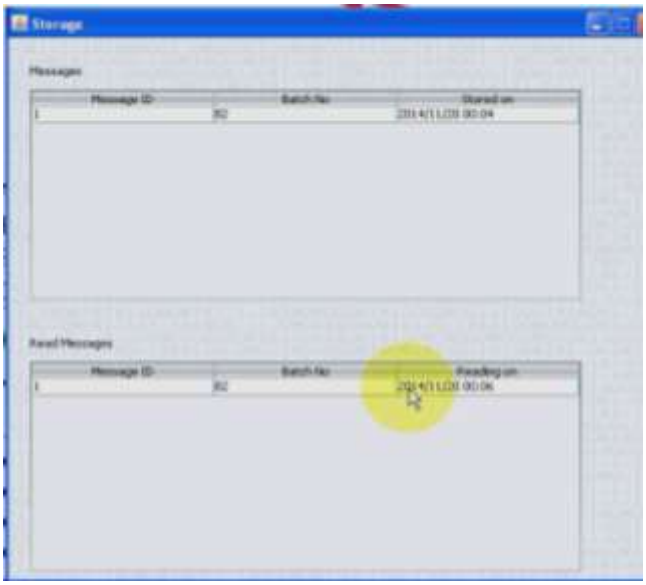

Figure 13. Storage of the database and the maintenance of logging details

IV. Conclusion

DTN technologies are becoming successful solutions in many 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 secures 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

ACKNOWLEDGMENT

We would like to thank the support by staff and friends during the project work.

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] J.Saranya , P.Ilango,"Efficient Information Retrieval By Using Multi-Modality Manifold Ranking Based On Syntactic/Semantic Measurement"*International Journal of Computer Trends and Technology (IJCTT)*,V4(9):3311-3315 September Issue 2013

[7] CH.Sivaram Prasad , T.Venu , N.Subhash Chandra, A New Design for Deduce User Search Results with Feedback Sessions, International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 2 – Sep 2014

[8] Tariq O. Fadl Elsid, Mirghani. A. Eltahir, "Data Mining: Classification Techniques of Students' Database A Case Study of the Nile Valley University, North Sudan", International Journal of Computer Trends and Technology (IJCTT) – volume 16 number 5 – Oct 2014