Survey Paper on an Efficient Secured system for data transactions in Decentralized Disruption Tolerant Networks

Rohan Jadhav
Department of CE,
University of Pune,
Pune,India.

Tasmin Pathan
Department of CE,
University of Pune,
Pune,India.

Ashok Kumbhar
Department of CE,
University of Pune,
Pune,India.

Prof. A. S. Hambarde
Asst. Prof. Dept. of CE,
KJCOEMR,
Pune, India.

Abstract: **If such type of system would not have been existed, it would be very difficult to manage data security in decentralize disruption tolerant network (DTN) due its moveable or changeable node Policies. The existing systems or software in the market are Defense Message System Messaging, Directory Services, and Security Services, MaxProp: Routing for vehicle based disruption tolerant network & Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks. One of the biggest disadvantage of these system are data can be easily get decrypted by any unauthorized person if he had both key and data so securing & managing data in DTN is difficult task.**

So this paper introduces proposed method that put an idea of setting up protocols for the receiver with its device unique number (MAC). And then the data will be sending to the storage node that can be movable in the network and once that node will deliver the data then the complete data will be securely transferred to the said device and with the help of Reverse circle cipher algorithm which is strongest encryption algorithm in networking domain will increase network security. So these methods will help to securely and effectively manage the confidential data in the disruption tolerant network.

Keywords: - Key Generation, Key Management, Reverse Circle Cipher.

I. INTRODUCTION

An Efficient Secured system for data transactions in Decentralized Disruption Tolerant Networks system introduces an idea of efficient and secure data delivery in Disruption Tolerant Networks where network connectivity is periodic, disconnected by jamming & adjustability. Due to these factors difficulties arise for sending messages and it also causes difficulties for the nodes to communicate with each other. The solution for this is provided by the Disruption Tolerant Networks. As there is no end to end connection between the source and destination nodes, storage nodes are been provided between them. Whenever the source node sends the data and if in case the destination node is not in network then for a while being or till the destination node comes into network the data is stored at the storage node and when the destination node comes into network then the destination nodes receives the data which was sent by the source node [1].

The methodologies used in other systems are multi-authority CP-ABE scheme.

Multi-authority CP-ABE scheme:

This scheme is used in decentralized disruption tolerant network for secure data decryption. The local authority provides few components to the user by performing a secure 2PC protocol with some authority named central authority & the components provided by the local authority to the user are partial personalized and attribute key. A 2PC protocol stands for two-phase commit protocol. It is atomic commitment protocol (ACP). If in case the system gets failed then also the 2PC protocol ensures the user that the system will achieve its goal. Only the attribute key of the user will get updated automatically and immediately. The attribute key gets updated individually it is not a case in which all the other components of the user get updated along with the attribute key. Thus in this way the security and scalability of the Multi-authority CP-ABE scheme can be increased.
To counter attack all the above methodology our system introduces technique of An Efficient Secured system for data transactions in Decentralized Disruption Tolerant Networks as:

Sender: The sender will send the data and the MAC address of authorized machine at the same to

A. Profile and data key generation &

B. Access control

ISSN: 2278 – 1323

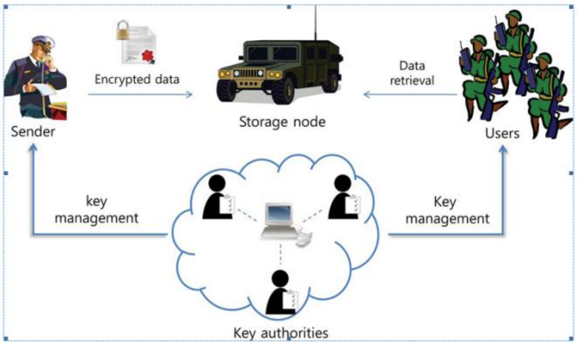

Fig.:- Architecture of Secure Data Retrieval in Disruption Tolerant Military Network.

A. Profile and data key generation:

It receives the data which is sent by the sender and according to the user the profile key and data key is generated.

1. Reverse Circle Encryption:

   It receives the data from profile and data key generation and in reverse circle encryption algorithm the data will get encrypted.

2. Storage node:

   It receives the data from the reverse circle encryption. If the key authorities want to change the data then they can change the data as the data is stored here for some period of time. If the receiver is in the coverage area then it will receive the data and if the receiver is not in the coverage area then storage node will continue the broadcast until the receiver comes in the coverage area.

3. Re-encryption:

   If the key authorities want to change the data then the data will get changed. If the data is changed by the key authorities then only the time-based key & profile and data key generation will get combined otherwise it will not get combined if the data is not changed

4. Key Management:

   When the time-based key & profile and data key both get combined then a third key gets generated and to manage all these keys the key management block is used.

5. Data delivery:

   In this block the data which was send by the sender to the receiver gets delivered at the particular MAC address.

B. Access Control:

The sender sends the data to the access control at the same time when it sends the profile and key generation block.

1. Time based key:

   It is the key which is based on current date and time. This key is gets generated whenever the key authorities want to change the data.

2. Two-tier key:

   Two-tier key is the key where two authorized users communicate with each other to maintain key and form new combined key for further function.

This paper is been classified for different sections like section II for Literature Survey, section III for Conclusion.

II. LITERATURE SURVEY

1) Introduces an idea of Attribute based key. Attribute based key is the type public key it allows user to encrypt & decrypt data based on the user attributes or profile based where the generated secret key of user depends on its personal attributes (e. g users name or kind of subscription he has or his mobile number). Attribute based key has different schemes available that are KP-ABE,CP-ABE. Decryption is possible only if user attributes data matches with cipher-text ABE allows to create multiple key.

   The major disadvantage of attribute based encryption is specially, data user needs to use, and every authorized persons attribute to encrypt the data. It is not used in real time application because it accesses monotonic attribute of user to control the system [2].

2) Explains the idea of Reverse circle cipher algorithm. Reverse circle cipher algorithm is encryption algorithm. It uses concept of circular substitution with reverse transposition to generate key. The circular substitution method is either clockwise or anticlockwise. To encrypt the data it uses confusion and diffusion matrix. The principle used in this matrix is ASCII or UTF based on arithmetic coding for algorithm .Circular substitution reduces the time and space complexity. It provides security for Disruption-

Tolerant Network, personal and network security [3].

If the data is too large then the disadvantage is that it will take too much time to encrypt or decrypt data. The drawback of this algorithm is that if we make any changes in the cipher text then the whole data gets changed and it causes data loss or information loss.

3) Narrates the idea of Time based key. It generates the key based on current time and date of the system. To generate password it removes extra symbols from the time and date (e. g colon and forward slash or dash).The advantage of time based key is a unique key because it was generated at specific time and date. We cannot create the same key again because that key is generated at particular time and date [4].

The problem of time based key is the machine on which we want to generate the key must be running at correct time and date. If not then it creates wrong key and it leads to information loss. Time based key is unique key. If we want to create same key again we cannot create it. If we lose the key then information associated with that key is also lost or we cannot retrieve it.

4) Describes the idea of Two-tier key. Two-tier key works like two tire architecture where web pages run on the client and process is done on the server. The actual application is run either on client or on server. Similarly in two-tire key, two authorized users communicate with each other to maintain key and form new combined key for further function.

5) States the idea of Re-encryption. Re-encryption scheme are cryptosystems which allows changing in cipher text for third user which was created for one user so that it may be decrypted by another user. Or Re-encryption allows changing cipher-text encrypted into one key and encryption of same data under another key [5].

6) Expresses the idea of Key management. Key management allows management and maintenance of keying relationship between authorized users. It supports several techniques such as storage, update, backup/recovery, revocation and archival of keying material. There are several key management models examples: offline mechanism, online mechanism, Ad-hoc methods [7].

III. CONCLUSION

All the methodologies which are mentioned in section 1 are having one or two major, minor flows in the field/area of An Efficient Secured system for data transactions in Decentralized Disruption Tolerant Networks. So as an alternate step towards this the proposed system introduces some ideas based on the detail study of some.

IV. ACKNOWLEDGEMENT

We would like to take this opportunity to express our profound gratitude and deep regard to our project guide “Prof. A. S. Hambarde”, for his guidance, valuable feedback and for constant encouragement for the project. Working under him was extremely knowledgeable experience for us.

V. REFERENCES

[1] Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM, *“Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks”*, IEEE TRANSACTIONS ON NETWORKING VOL: 22 NO: 1 YEAR 2014.

[2] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3, *“A Survey on Attribute Based Encryption Scheme in Cloud Computing”*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013.

[3] Sarika U. Kadla and Rahul L. Paikrao, *“Hybrid Cryptosystem for Secure Text File for Cloud”*, International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 2, February 2014.

[4] Kenneth G. Paterson and Douglas Stebila, *“One-time-password-authenticated key exchange”*, September 4, 2009.

[5] Giuseppe Ateniese, Karyn Benson and Susan Hohenberger, *“Key-Private Proxy Re-Encryption”*, January 22, 2009.

[6] T.Lalith, R.Umarani and G.M.Kadharnawaz, *“Key Management Techniques for Controlling the Distribution and Update of Cryptographic keys”, (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 1, No.6, December 2010.*