Result Analysis on Secure File Storage System for DisruptionTolerant Military Environment

Prof. Rajesh Dilip Dahiwade

Vidya Bhavan College of Management & Research, Yavatmal, MS, India.

rajeshdahiwade@gmail.com

Abstract - Secure File Storage System is application to provide security to user for protect his file and also share file bin categorize we will implement some module like data storage module, data encryption module and data retrieval module and facilitate main storage and secondary storage. Now the massive quantity of expanding industrial atmosphere each and everything depends on the other sources to broadcast the data strongly and maintain the data as well in the frequentmedium. Convenient nodes in military surroundings, for example, a frontage line or a hostile area are prone to experience irregular system network and common partition. Disruption-tolerant network (DTN) improvement are getting to be productive results that allow remote device get across by officers to tell with other and access the private data consistently by exploitation external capacity nodes or storage nodes. The new approach is to offer effective communication beside to another also access the different information supply through various key establishments like commander or other superiors. This system offer competent scenario for approval strategy and the strategy renew for protected data salvage in most demanding situation. The most assure cryptographic result is commenced to manage the access RSA algorithm.

***Keywords* — Secure storage, RSA algorithm, disruption-tolerant network (DTN), multi authority, data retrieval, data encryption, data decryption.**

I. INTRODUCTION

Secure File Storage technologies are suitable successful solutions in military applications to facilitate allow correspond with one node to other node and access the private information efficiently by developing the external storage node. We projected a capable, secure and private data retrieval technique using the Encryption method used during the storage process is RSA algorithm which is one of the primary practical public-key cryptosystems and is frequently used for protected data transmission and Storage. Data is access by the client using its individual private key from the secondary storage which keeping the data as well as transmission protected and undisruptive [1]. In military environmental network, connections of wireless devices carried by soldiers could be conditionally rigorous by congestion, conservation or ecological factors, and mobility, particularly when they manage in hostile environments. Disruption-tolerant network technologies are suitable successful way that permits nodes to correspond with each other [3].

Storage nodes in DTNs information is stored or pretend such that only allowed mobile nodes can access the required information rapidly and competently [3]. Requirement in some security significant application is to design an access manage system to protect the private data stored in the main storage node and secret messages routed throughout the network. As an example, in a combat zone disruption- tolerant network. A storage node may have several secret information should be accessed only by a member of participant in secret mission. Various recent results track the conventional cryptographic strategies where the contents are encrypted prior to store in storage nodes. Also the decryption keys are disseminated only to authorized user [10]. In such approach, tractability and granularity of content access control relies heavily on the basic cryptographic primitives being used. It is hard to balance among the complexity of key management and the granularity of access control using any solutions that are based on the conservative pair wise key or cluster key primitives. Thus, we still need to design a scalable solution

 DOI : 10.35291/2454-9150.2022.0024

that can provide fine-grain access control [1], [2], [12].

II. LITERATURE SURVEY

Major phase in software development is survey of the existing system. Before developing required to decide the instant aspect, economy and business strength. Formerly the programmers begin implement the tool programmers need lot of external support.

A. Attribute Revocation:

The key mechanism in KP-ABE and CP-ABE respectively. Their solutions are to attach to each characteristic an expiration date and allocate a new set of keys to valid users after the expiration. The periodic characteristic revocable ABE schemes have two main problems [1], [15], [16], [17].

B. Key Escrow:

Most of the existing Attribute-Based Encryption methods are construct on the architecture where a particular trusted authority has the power to produce the whole secret keys of users with its master private information [11], [13]. Thus, the key escrow difficulty is inherent such that the key authority can decrypt each cipher text addressed to users in the system by generate their secret key at any time [7]. M. Chase existing a distributed KP-ABE idea that solves the key escrow difficulty in a multi authority method [14][17]. In this approach, all (disjoint) characteristic authorities are participating in the key generation set of rules in a distributed way such that they cannot pool their data and link multiple characteristic sets belong to the same user. Individual disadvantage of this fully distributed approach is the performance degradation.

C. Decentralized Attribute-Based Encryption:

The author A. Lewko and B. Waters proposed decentralized CP-ABE schemes in the multi authority network surrounding. They achieved a combined access policy over the characteristic issued from different authorities by simply encrypting information multiple times. The major disadvantages of this approach are efficiency and expressiveness of access policy [9], [10].

III.SYSTEM ARCHITECTURE

In this, we describe the Disruption tolerant network architecture.

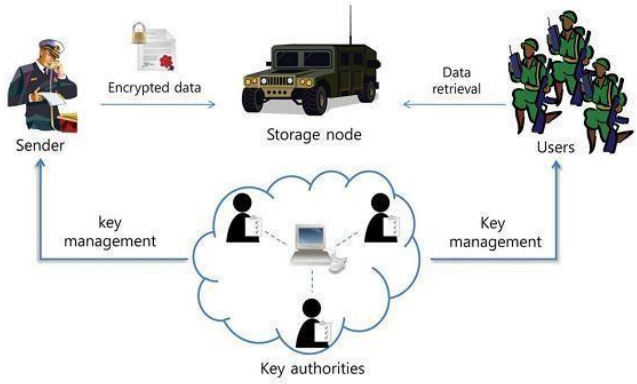


Fig.1. Architecture of secure data retrieval in disruption-tolerant military network [1].

As shown in Fig. 1, the architecture consists of the following system entities.

A. Key Authorities:

Here we generate key generation centers that generate public/secret parameters for the CP-ABE. The key authorities made up of a central access and multiple local accesses. We assume that there are reliable and secure communication channels between a each local authorities and central located authority during the initial key setup and generation phase. The key authorities are assumed to be honest-but-curious. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant different access right authorization to individual users based on the users' attributes. That is, they will sincerely execute the given tasks in the system; however they learn information of encrypted information as much aspossible.

B. Storage node:

This is a key that stores/loads data from senders and provide the access to the users. It may be mobile or static for the device. Similar to the previous scheme, we also consider the storage node to be partially trusted that is honest but curious[4], [5].

C. Sender:

This is an entity that purchased private messages or wishes and data (e.g., a commander) to store them into the external information storage node for easy of sharing or for safest delivery to users in the severe networking environments. A sender is responsible for explaining (characteristic based) access policy and enforcing it on its own information by encrypting the information under the

 DOI : 10.35291/2454-9150.2022.0024

policy before storing/load it to the storage node.

D. User:

This is a mobile node that needs to access the data stored/load at the storage node (e.g., a soldier). If the user posses set of characteristic satisfying the access policy of the encrypted/secured data defined by the sender, and is never aware in any of the attributes, then he will be able to decrypt the cipher text and catch the data. Since the key authorities are semi-trusted, they should be deterred from getting access of plaintext of the information in the storage node; meanwhile, it should be still able to issue secretes keys to users. In order to realize this something contradictory requirement, the central permissions and the local permissions connecting in the arithmetic 2PC protocol with master secret key of their own and issue independent key components to users while the key issuing phase. The 2PC protocol prevents them from knowing each other master secrets so that nothing can create the whole set of secret keys of users individually. Thus, we taken assumptionthat the central authority did not collude with the localaccess (otherwise, they can guess the secret key of every user by sharing their master secrets).

IV. CONSTRUCTION ALGORITHM

A. Algorithm:

1. first we set a random number in the main storage and unique client id for every client.
2. Whenever the client id is being register in the main storage, then client id and random number is getting EXORed ( ) with each other to generate seed block for the particular client.
3. Whenever client creates the file in cloud first time, it is stored at the main storage.
4. When it is stored in main storage (blob), the main file of client is being EXORed with the Seed Block of the particular client.
5. It is also encrypted using public key RSA
6. That output file is stored at the backup storage (blob) in the form of file' (pronounced as Filedash).
7. During Retrieval, check if data present in main storage.
8. If present then EXOR with seed block and retrieve data.
9. If not present, retrieve data from backup storage.
10. During Retrieval from backup storage , the private key of the user will used to decrypt file'.

    The user will get the original file by EXORing on decrypted file' with the seed block of the corresponding client toproduce.

B. Mathematical Module:

Mathematics is shared because it is reach and interesting discipline it provides set of ideas and tools. That are effective in solving problems which is useful in theoretical studies in other field when used problem already posed in Mathematical model form, I theory construction mathematics provides abstract structures which did in understand situations arising in other fields. Problem formulation and theory construction involve across known as mathematical model building. given a situation and formulates other than mathematics or in everyday life mathematical model building is activity that begins with situation and formulates a precise mathematical problem whose situation or analysis in case of theory construction is enables us the better understand of original situation. Mathematical modeling originally begins with situation in real world sometimes in relatively controlled conditions of laboratory and sometimes in the much less complete understood environment of me ow sand forests offices and factories and everyday life.

In proposed system input can be give in the encrypted message form.

Output

Message should be generated in decrypted form using secretkey.

Registration and login

This function is used user, admin as well as receiver or soldiers. If have new user then they need to be registration then after it can be enter in system.

Key generation

When user entered or send the cofidentional message that time secret is generated.

Transfer key

Using this main storage server or node can transfer secret key to particular nodes or soldiers. Success Conditions Encrypted message should be meet successfully. Failure Conditions Key cannot be generated, Network failure,

 DOI : 10.35291/2454-9150.2022.0024

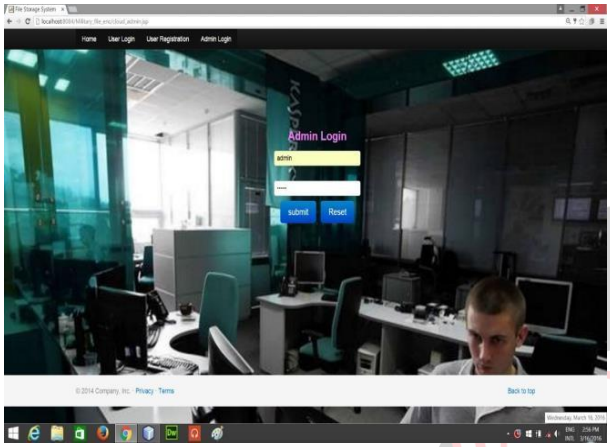
Hardware failure.

S=(s, e, X, Y, F, DD, NDD, Ffriend, Fme, Mshared, CPUcorecnt, Success, Failure)

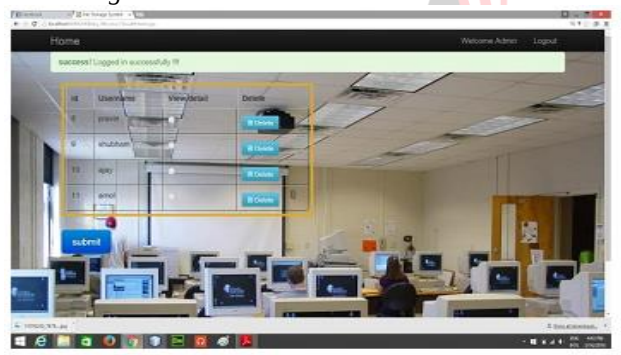
Here,
s− >Registration / login
e− >key generation and decrypt dataX− > Send message
Y− >Transfer keyFme− >Soldier DD− >Encryption
Ffriend− >Decrypt message NDD− >Secret key
CPUcorecnt − > 01 Success− > Encrypt message
Failure− >Key generation failed

V. RESULT ANALYSIS

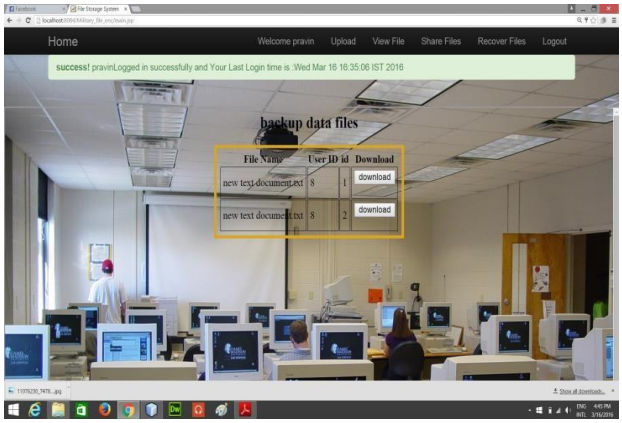
Description Input*User Login*



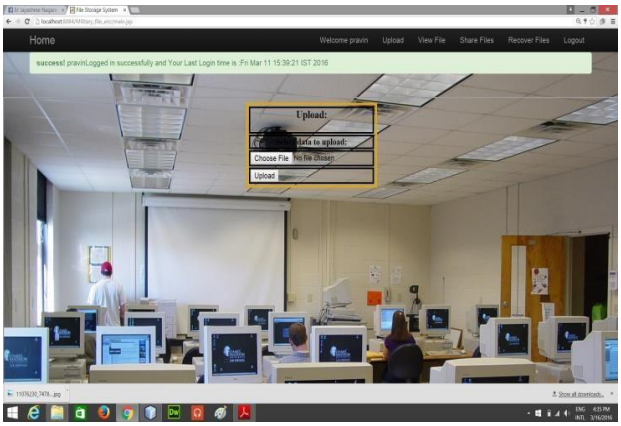
Admin Login



User Details and History
Recover File



File Upload



VI. CONCLUSION

Please include a brief summary of the possible clinical implications of your work in the conclusion section. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. Consider elaborating on the translational importance of the work or suggest applications and extensions.

REFERENCES

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

[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,"CryptologyePrint Archive: Rep. **2010/351**, **2010**.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc.Eurocrypt, **2005,** pp. **457–473**.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute- based encryption for fine-grained access control of encrypted data," in Proc.ACM Conf. Comput. Commun. Security, **2006**, pp. **89–98**.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, **2007**, pp.**321–334**.

 DOI : 10.35291/2454-9150.2022.0024