Secure File Storage System for Disruption-Tolerant Military Environment

[1]MR. Sanjay Mali, [2]Prof. Dr. Vivek Sharma

[1,2]TIT College Bhopal, Madhy Pradesh, India.

sanjaymalimca@yahoo.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 frequent medium. 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), multiauthority, 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 contented 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 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.

DOI : 10.18231/2454-9150.2018.0047

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 ANALYSIS

A. *Existing System*

The idea of attribute-based encryption (ABE) is a promising approach that satisfies the requirements for protected information retrieval in DTNs. ABE characteristics a mechanism to empower an access control over encrypted information utilizing access policies and credited qualities among private keys and cipher texts. The issue of applying the ABE to DTNs introduces several a few security and privacy challenges. Since a few users may change their related attributes at a few point (for example, moving their region), or a few private keys may be compromised, key repudiation (or update) for each one characteristic is necessary in order to build systems secure.

This implies that revocation of any attribute or any single client in an attribute group would affect the other client in the group. For example, if a client joins or leaves an characteristic group, the associated attribute key be supposed to changed and redistributed to all the other users in the same group for backward or forward privacy. It may result in bottleneck during security or rekeying procedure degradation due to the windows of defenselessness if the previous attribute key is not updated immediately. Many military applications require improved security of the confidential information including access manage methods that are cryptographically enforce the Attribute-based encryption [6].

a. *Disadvantages*

However, the problem of applying the Attribute-based encryption to disruption-tolerant network introduces several security and confidentiality challenges.

Since a few users may change their associated attributes at a few point (for example, moving their region), or some private keys may be compromised, key revocation (or update) for each characteristic is essential in organize to make systems secure. However, this issue is still more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users.

B. *Proposed System*

In this project, we propose an attribute-based secure data retrieval scheme using RSA for decentralized DTNs. The proposed scheme features the following achievement. First, immediate attribute revocation enhances backward/forward secrecy of private information by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access rule using any monotone access structure under attributes issued from any chosen set of access. Third, the key escrow difficulty is resolve by an escrow-free key issuing protocol that exploits the attribute of the decentralized disruption-tolerant network architecture. The key issuing protocol generate and issues user secret key by performing a protected two-party computation 2PC protocol among the key authorities through their own master secret. The 2PC protocol deters the key authorities from obtaining any master secret information of each other like that none of them could generate the whole set of user keys only. Thus, users are not necessary to fully trust the authorities in order to protect their information to be shared. The data privacy and confidentiality can be cryptographically enforced against any curious data storage or key authority's nodes in the proposed scheme. We projected secure file storage system by using encryption technique data beside with the accessible privileges to another client and the key produce is associated with the user to whom the accessible right is offered.

Thus, users are not required to fully trust the authorities in order to protect their information to be shared. The data privacy and confidentiality can be cryptographically enforced against any curious key authorities or information storage nodes in the proposed scheme.

DOI : 10.18231/2454-9150.2018.0047

a. Advantages

Data confidentiality: Unauthorized users who don't have enough credentials satisfying the access policy should be deterred from accessing the simple data in the storage node. In addition, illegal access from the key or storage node authorities should be also prevented.

Collusion-resistance: If various users collude, they may be able to decrypt a cipher-text by combining their attributes even if each one of the users cannot decrypt the cipher-text alone.

IV. System Architecture

In this, we describe the Disruption tolerant network architecture.

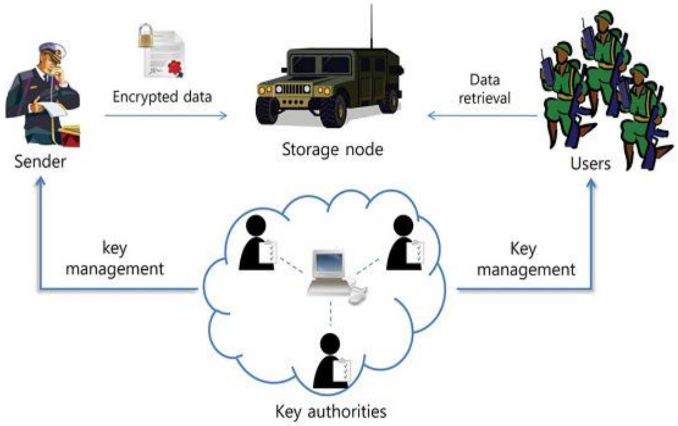

Fig.1. Architecture of secure data retrieval in disruption-tolerant military network [1].

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 as possible.

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 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 assumption that the central authority did not collude with the local access (otherwise, they can guess the secret key of every user by sharing their master secrets).

V. Implementation

In this way used the Java language to implement the RSA Algorithm for DTN. In the rest of this section, first we will talk about the proposed Disruption Tolerant military network then we merge our RSA Algorithm method with distributed DTN for secure data retrieval. First we have intended the Disruption Tolerant Network (DTN) which initiate the idea of storage nodes where in the private data is simulated or store such that only endorsed mobile nodes can access the required information rapidly and consistently. The sender or military commander who individual the secret data has the ability to register users military soldiers and offer access rights.

Admin module -

This is the authentication module of the system facilitate admin to add to themselves to the system as well as authenticate and utilize the system, thereby providing access to some valid registered admin in the system.

DOI : 10.18231/2454-9150.2018.0047

Data Storage module-

It uses the Distributed type of Structure for the Data Storage. In this Module, the user uploads the some desired data to server at two locations:

a) Main Server:

In Main Server, the User Stores its private data and Key Generation for Sender are public.

b) Secondary Storage Server:

In this Server, the User Stores the data along with the accessible rights to other user and the Key Generated is associated with its user to whom the accessible right is provided. The Key is sent to that other user to access the data.

Data Encryption-

The Encryption method will used during the Storage process is RSA Algorithm which is one of the primary practical public-key crypto systems and is widely used for the secure data transmission and Storage.

Data Retrieval-

In this module, the data is accessed by the private user using its own private key from the Secondary Storage thereby keeping the data as well as transmission secured and safe client wants to transfer key by mail to client.

VI. CONCLUSION

DTN technologies are suitable solutions in military applications so as to allocate wireless devices to converse with another and access the private information dependably by develops external storage nodes. RSA algorithm is a scalable cryptographic solution to the access control and protected data retrieval issue. We projected an capable and confident storage data recovery technique using RSA algorithm for decentralized DTNs where many key authorities handle their attributes separately.

The inbuilt key escrow problem is determined such that the privacy of the stored data is assured even under the antagonistic atmosphere where key authorities might be compromise or not fully belief. In addition, the fine-grained key revocation can be complete for each aspect collection. We display how to apply the projected mechanism to strongly and professionally handle the private data dispersed in the disruption-tolerant military network.

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**.

[14] 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**.

[15] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, **2007**, pp. **456– 465**.

[16] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with," in Proc. ASIACCS, **2010**, pp. **261–270**.

[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in Proc. ACMConf. Comput. Commun. Security, **2006**, pp. **99–112**.

DOI : 10.18231/2454-9150.2018.0047