Data Rescue Process in Network Medium with Higher End Security Measures

Praveena.S, RajeshKannan.C

Abstract— **In the large number of outgrowing commercial environment each and everything depends on the other sources to transmit the data securely and maintain the data as well in the regular medium. In military environments such as a battlefield or an unfriendly region are likely to experience from irregular network connectivity and frequent partitions. A new methodology is introduced to provide successful communication between each other as well as access the confidential information provided by some major authorities like commander or other superiors. The methodology is called Disruption-Tolerant Network (DTN). This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases. The most promising cryptographic solution is introduced to control the access issues called Cipher text Policy Attribute Based Encryption (CP-ABE). On the other hand, the difficulty of affect CP-ABE in decentralized DTNs set up more than a few security and privacy challenge with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. This system proposes a secure data rescue scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently as well as demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption tolerant military network. The military network is nothing but the collection of nodes like soldiers and commanders are tied together and provide the better results in regular data transmission mechanisms.**

Index Terms— **Confidential information, Disruption-Tolerant Network (DTN), Cipher text Policy Attribute Based Encryption (CP-ABE), Security, Privacy**

I. INTRODUCTION

In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. Typically, when there is no end-to-end connection between source and destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. Several application scenarios require a security design that provides fine grain access control to contents stored in storage nodes within a DTN or to contents of the messages routed through the network.

Our scheme provides a flexible fine-grained access control such that the encrypted contents can only be accessed by authorized users. Two unique features our schemes provide are: (i) the incorporation of dynamic attributes whose value may change over time, and (ii) the revocation feature. We also provide some performance results from our implementation. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced. Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. We explain the mechanisms in plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. As storage systems and individual storage devices themselves become networked, they must defend both against the usual attacks on messages traversing an untrusted, potentially public, network as well as attacks on the stored data itself. To protect stored data, it is not sufficient to use traditional network security techniques that are used for securing messages between pairs of users or between clients and servers.

In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes [7], and the ciphertext is associated with an access policy over attributes. The user can decrypt the ciphertext if and only if the attribute set of his secret key satisfies the access policy specified in the ciphertext. A secret key holder can decrypt the ciphertext if the attributes associated with his secret key satisfy the access policy associated with the cipher text.

A. Bilinear Diffie–Hellman Assumption

The Bilinear Diffie–Hellman (BDH) problem[6], is efficiently computed by the above mentioned algorithm by means of generating paired key with the help of Commander generated Public Key and the Guard Generated Shared Key. The data is further processed / encrypted with the help of the generated Paired Key.

Manuscript received Nov, 2014.

***Praveena.S**, Department of Computer Science and Engineering, Mount Zion College of Engineering and Technology, Pudukkottai India. +91-8754442360.*

***Rajeshkannan.C**, Department of Computer Science and Engineering, Mount Zion College of Engineering and Technology, Pudukkottai, India,+91-7598492789.*

ISSN: 2278 – 1323

B. Polynomial Time Algorithm

In computer science, the time complexity of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the size of the input to the problem. The time complexity of an algorithm is commonly expressed using big O notation, which suppresses multiplicative constants and lower order terms. When expressed this way, the time complexity is said to be described asymptotically, i.e., as the input size goes to infinity. Time complexity[3], is commonly estimated by counting the number of elementary operations performed by the algorithm, where an elementary operation takes a fixed amount of time to perform. Since an algorithm may take a different amount of time even on inputs of the same size, the most commonly used measure of time complexity, the worst-case time complexity of an algorithm, denoted as T (n), is the maximum amount of time taken on any input of size n. Time complexities are classified by the nature of the function T(n). For instance, an algorithm with T(n) = O(n) is called a linear time algorithm, and an algorithm with T(n) = O(2n) is said to be an exponential time algorithm.

C. Probabilistic Algorithm

The general rule of the Probabilistic Algorithm is either success or loss attained, but in this case we implement some additional functionality to maximize the success rate and minimize the failure rates. So that the additional case of Min-Max rule is applied here to attain the best results

D. Min-Max Algorithm

Minmax (sometimes minimax) is a decision rule used in decision theory, game theory, statistics and philosophy for minimizing the possible loss for a worst case (maximum loss) scenario. Alternatively, it can be thought of as maximizing the minimum gain (maximin). Originally formulated for two-player zero-sum game theory, covering both the cases where players take alternate moves and those where they make simultaneous moves, it has also been extended to more complex games and to general decision making in the presence of uncertainty[8].

E. Cp-Abe Algorithm

A new methodology[7], is introduced to provide successful communication between each other as well as access the confidential information provided by some major authorities like commander or other superiors. The methodology is called Disruption-Tolerant Network (DTN). This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases. The most promising cryptographic solution is introduced to control the access issues called Ciphertext Policy Attribute Based Encryption (CP-ABE). On the other hand, the difficulty of affect CP-ABE in decentralized DTNs set up more than a few security and privacy challenge with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. This system proposes a secure data rescue scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently as well as demonstrate how to mechanism to securely and efficiently manage the confidential data distributed in the disruption tolerant military network.

II. LITERATURE SURVEY

This section literature review has provides an overview and a critical evaluation of a body of literature relating to a research problem. Literature review is the most important step in software development process. In many network scenarios, even it may be regular network or military network or wireless communication models, the connections produced by the provider may be jammed and disconnected by the intruders and the data will be theft, especially when they operate in distributed network schemas. All the existing routing technologies are becoming successful solutions that allow source and destinations to communicate with each other in the extreme network environments, but they provide services in certain limit as well as with certain conditions. Typically there is no end to end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediates for a substantial amount of time until the connection would be eventually established.

A. Maxprop: Routing for vehicle-based disruption tolerant networks

In this paper[1], we propose MaxProp, a protocol for effective routing of DTN messages. MaxProp is based on prioritizing both the schedule of packets transmitted to other peers and the schedule of packets to be dropped. These priorities are based on the path likelihoods to peers according to historical data and also on several complementary mechanisms, including acknowledgments, a head-start for new packets, and lists of previous intermediaries. This paper presents [1], a protocol for effective routing of DTN messages. MaxProp is based on prioritizing both the schedule of packets transmitted to other peers and the schedule of packets to be dropped. The main advantage is Fault Tolerant Network Architecture and main drawback of this paper is supports only Limited Resource transmission.

B. Decentralizing attribute-based encryption

We prove our system secure using the recent dual system, encryption methodology where the security proof works by first converting the challenge ciphertext and private keys to a semi-functional form and then arguing security. We follow a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of composite order. We prove security under similar static assumptions to the LW paper in the random oracle model. According to this paper [3], any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. The advantage of this paper encryption techniques are followed to secure the data and drawback is key complexity occurs in several cases of transmission.

C. Node density-based adaptive routing scheme for disruption tolerant networks

In that paper [2], we assume that a special node is designated to be a message ferry. A more flexible approach is to let regular nodes volunteer to be message ferries when network dynamics mandate the presence of such ferries to ensure communications. Thus, in this paper, we design a node-density based adaptive routing (NDBAR) scheme that

allows regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of continued communication clustering algorithms based on energy consideration. In this paper, we design a node-density based adaptive routing (NDBAR) scheme that allows regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of continued communications. The main advantage is node density based routing methodology, so the node lifetime increases and drawback is cost is high to implement.

D. Secure attribute based systems

Ciphertext-policy attribute based encryption (CPABE) provides an encrypted access control mechanism for broadcasting messages. Basically, a sender encrypts a message with an access control policy tree which is logically composed of attributes; receivers are able to decrypt the message when their attributes satisfy the policy tree. A user's attributes stand for the properties that he current has. It is required for a user to keep his attributes up-to-date. . In this paper [5], we introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives. A performance analysis of our ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions. Our attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems. The advantage along with this paper is attribute based destination identification, so possibility of intrusion is comparatively low and other drawback is sequence of packet flow is missing, so confusion occurs in the optimization process.

III. PROPOSED APPROACH

In the Proposed Approach, Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow source and destinations to communicate with each other in the extreme complicated network environments. To securely transmit the data in regular network medium with existing security measures like cipher text and all but the way of handling the cipher text schema should guarantees the performance and security measures. In this system a new approach is handled to provide a secure data rescue scheme using CP-ABE for decentralized DTNs, where multiple key authorities manage the key attributes independently. The proposed mechanism demonstrates how efficiently and securely manages the confidential data in distributed network architecture.

- The key authority can decrypt every cipher text addressed to specific users by generating their attribute keys.
- Using multiple key revocation method
- Time saving process, because of the transmission mode is guaranteed, this made the process more easier to transmit confidential data between commanders and guards.
- Performance is high.
- Privacy Issues are successfully retained.

The major contribution of this system is to securely transmit the data in regular network medium with existing security measures like cipher text and all but the way of handling the cipher text schema should guarantees the performance and security measures. The regular ABE comes in two essence called Key Policy ABE (KP-ABE) and Ciphertext Policy ABE (CP-ABE). In the first one KP-ABE the Commander can encrypt and gets a ciphertext with a set of labeled Paired Key. The key influence decides a rule for each user that determines which ciphertexts the Guard can decrypt and issues the key to each user by drive in the policy into the guard key. On the other hand, the position of the ciphertexts and keys are upturned in CP-ABE. In CP-ABE, the ciphertext is encrypted with a right to use policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes.

IV. SYSTEM DESIGN

A. System Architecture

The major part of the project development sector considers and fully survey all the required needs for developing the project. Before developing the tools and the associated designing it is necessary to determine and survey the time factor, resource requirement, man power, economy, and company strength. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations. Generally algorithms shows a result for exploring a single thing that is either be a performance, or speed, or accuracy, and so on. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them.

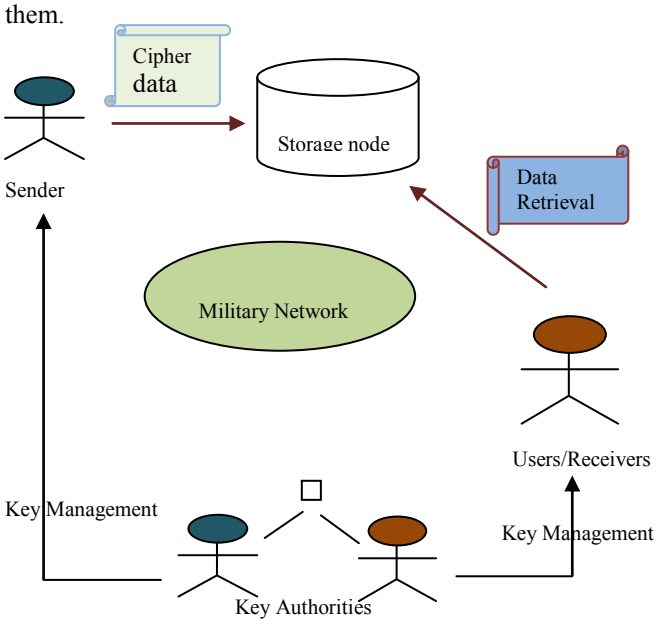

Fig. A System Architecture

ISSN: 2278 – 1323

B. Modules

1. *Commander/Guard Identity Authorization*
2. *Identity Key Generation*
3. *Ciphertext Policy Attribute Based Encryption*
4. *Confidential Data Interchange*
5. *Administrative Access Controller*

1) Commander/Guard Identity Authorization

This module allows the user (Commander / Guard) to register their identity into the system with proper input parameters. The key generation centers play a vital role in it, which generates public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. Assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system however they would like to learn information of encrypted contents as much as possible.

2) Identity Key Generation

The key generation module helps the users to share the information between source and destination. After getting the confirmation response from the receiver side the sender fix the information and encrypt it. At this time a key will be generated and sent to the receiver area. That key is useful for decrypt the data at receiver end. As well as an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, and also assume the storage node to be semi trusted that is honest-but-curious.

3) Ciphertext Policy Attribute Based Encryption

In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor. This techniques encrypted data can be kept confidential even if the storage server is untrusted. Moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

4) Confidential Data Interchange

This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node. This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

5) Administrative Access Controller

The administrator owns full access rights of this entire site. Once the administrator find out any illegal activity or other misusing happens into the way of transaction between the respective sender and receiver then the admin immediately block the user access rights to transact using this site. The block will be unblocked after getting meaningful reason from the user end.

V. CONCLUSION

The proposed DTN approach provides most successful solutions in military as well as other secured networks that allow even wireless devices to transmit the confidential information between each other with reliable amount of cost. The security algorithm CP-ABE is implemented because it is more scalable to make the encryption and decryption process securely. This approach produces a well-organized and secure information repossession technique by means of CP-ABE for decentralized DTNs where multiple key establishments supervise their quality independently. Through this system the commander and guards can assure the data confidentiality between one and another. The proposed mechanism guarantees to maintain the confidential data securely and efficiently manage the data distributed in the disruption tolerant military network.

ACKNOWLEDGMENT

We would like to sincerely thank Assistant Prof. C.Rajeshkannan for his advice and guidance at the start of this article. His guidance has also been essential during some steps of this article and his quick invaluable insights have always been very helpful. His hard working and passion for research also has set an example that we would like to follow. We really appreciate his interest and enthusiasm during this article. Finally we thank the Editor in chief, the Associate Editor and anonymous Referees for their comments.

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] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

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

[5] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in Proc. ACM Conf. Computer Communication Security, 2006, pp. 99–112.

[6] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Computer Survey, vol. 35, no. 3, pp. 309–329, 2003.

[7] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proc. ASIACCS*,2009, pp. 343–352.

.

[8] M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in Proc. ACM Conf. Computer Communication Security, 2009, pp. 121–130.

[9] M.Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A.Hysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in Proc. Crypto, LNCS 5677, pp. 108–125.

[10] C. K.Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," in Proc. ACM SIGCOMM, 1998, pp. 68–79.

[11] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conference of Computer Communication Security, 2007, pp. 456–465.

[12] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Computer Communication Security, 2008, pp. 417–426.

BIOGRAPHY

Praveena.S is currently a PG scholar in Computer Science Engineering from the Department of Computer Science and Engineering at Mount Zion College of Engineering and Technology, Pudukkottai. She received his Bachelor Degree in Information Technology from Mount Zion College of Engineering, Pudukkottai and Tamilnadu. Her Research areas include Data mining, grid computing and wireless sensor networks.

Rajeshkannan.C is currently working as an Asst. Prof. from the Department of Computer Science and Engineering at Mount Zion College of Engineering and Technology, Pudukkottai. His main research interests lie in the area of Data mining, Data warehousing and Wireless Sensor Networks.

ISSN: 2278 – 1323