Enhancing Security in Data Retrieval by Using Cipher-Policy Attribute Based Encryption

Prasath[#1]

[#]*M.Tech Student, Department of Computer Science & Engineering, PRIST University*
Vallam, Thanjavur-613 403
[1]*prasadh2105@gmail.com*

***Abstract*—In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. In this paper we use the DTN (Distributed Tolerant Network) that is used to store and forward of data using for the users to a network in data security. This paper presenting a system for realizing complex access control on encrypted data that we use Cipher text-Policy Attribute-Based Encryption in Distributed Tolerant Network (DTN). In this, CP-ABE techniques used for encrypted data can be kept confidential even if the storage server is untrusted; moreover, the propose technique is more secure against collusion attacks.**

***Keywords*— Misbehavior detection, incentive scheme, delay tolerant networks, security**

I. INTRODUCTION

DELAY tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., local ads, traffic reports, parking information), and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent disconnectivity. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears (e.g., a new node moves into the range or an existing one wakes up). This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" fashion. In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities). Routing misbehavior can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks.

II. DTN

The recent researches show that routing misbehavior will significantly reduce the packet delivery rate and, thus, pose a serious threat against the network performance of DTN.

A. Misbehavior Detection and Mitigation Protocol

A misbehavior detection and mitigation protocol is highly desirable to assure the secure DTN routing as well as the establishment of the trust among DTN nodes in DTNs. Mitigating routing misbehavior has been well studied in traditional mobile ad hoc networks. These works use neighborhood monitoring or destination acknowledgement to detect packet dropping, and exploit credit-based and reputation-based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes. Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficult to predict mobility patterns, and long feedback delay have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs. Selfish node B receives the packets from node A but launches the black hole attack by refusing to forward the packets to the next hop receiver C. Since there may be no neighboring nodes at the moment that B meets C, the misbehavior (e.g., dropping messages) cannot be detected due to lack of witness, which renders the monitoring-based misbehavior detection less.

II. RELATED WORK.

A. Attribute based data sharing with attribute revocation

The entire document CP-ABE is resistant to collusion attacks from unauthorized users. All these nice properties make CP-ABE extremely suitable for fine-grained data access control on untrusted storage. As promising as it is, there also exist several issues when directly applying state-of-the-art CP-ABE schemes to practical applications. These issues can be summarized in two folds: firstly, existing CP-ABE schemes are not able to simultaneously achieve provable security, expressiveness of access structure, and efficient construction; secondly, user management, user revocation in particular, is extremely hard to realize in an efficient way. When current researches are mainly focusing on solving the former, the later has drawn less attention. In fact, user revocation is a challenge issue in many one-to-many communication systems. In attribute based systems, this issue is even more difficult since each attribute is conceivably shared by multiple users. Revocation of any single user would affect others who share his attributes. Moreover, user revocation in attribute based systems may be flexible and occur in different granularities. That is, it may require to revoke either the entire user access privilege, or just partial access right of the user, i.e., a subset of his/her attributes. Existing CP-ABE schemes suggest associating expiration time attributes to user secret keys. However, this type of solutions always have a trade-off between granularity of user revocation and the load placed on the system authority, and require interaction between users and the authority. In addition, the expiration method is not able to efficiently revoke user attributes on the fly. In,

Boldyreva et al. proposed an efficient revocation scheme for IBE, which is also applicable to KP-ABE and fuzzy IBE. However, it is not clear whether the proposed scheme is applicable to CP-ABE. Towards building a full fledged CP-ABE system, this paper focuses on the important yet difficult problem of user revocation. Instead of addressing the issue in general settings, we particularly focus on practical application scenarios such as data sharing, as shown by Fig.1, in which semi-trustable proxy servers are always available for providing various types of content services.

B. Decentralizing attribute-based encryption

In this, authorities can function entirely independently, and the failure or corruption of some authorities will not affect the operation of functioning, uncorrupted authorities. This makes our system more robust then the other approaches outlined above. Challenges and Our Techniques In constructing our system, our central technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. Such randomization would make the different key components compatible with each other, but not with the parts of a key issued to another user. In our setting, we want to satisfy the simultaneous goals of autonomous key generation and collusion resistance. The requirement of autonomous key generation means that established techniques for key randomization cannot be applied since there is no one party to compile all the pieces together. Furthermore, in our system each component may come from a different authority, where such authorities have no coordination and are possibly not even aware of each other and there is no preset access structure.

C. Fuzzy identity-based encryption

. In this paper we propose a new type of Identity-Based Encryption that we call Fuzzy Identity-Based Encryption in which we view identities as a set of descriptive attributes. In a Fuzzy IdentityBased Encryption scheme, a user with the secret key for the identity ω is able to decrypt a ciphertext encrypted with the public key ωif and only if ω and ωare within a certain distance of each other as judged by some metric. Therefore, our system allows for a certain amount of error-tolerance in the identities.Fuzzy-IBE gives rise to two interesting new applications. The first is an Identity-Based Encryption system that uses biometric identities. That is we can view a user's biometric, for example an iris scan, as that user's identity described by several attributes and then encrypt to the user using their biometric identity. Since biometric measurements are noisy, we cannot use existing IBE systems. However, the error-tolerance property of Fuzzy-IBE allows for a private key (derived from a measurement of a biometric) to decrypt a ciphertext encrypted with a slightly different measurement of the same biometric.

III. EXISTING Vs PROPOSED

A. Existing System

1) Advantages

- In this existing system the individual user data can be exchanged over the thirds party server.
- Individual data can be accessed through the third party server, and it can be out sourced.
- Before outsourcing, the secrecy data to be encrypt and outsource the data.
- In this system, the particular secrecy data can be maintained by the central authority (CA) to the key management on behalf of third party owners.
- In this system, the malicious behaviors which may lead to the exposure of the secrecy data.
- In Existing the access policy based mechanism is not used.
- The nodes are trusted blindly.

2) Disadvantages

- In this system, for the individual user having the central authority for the encrypting and decrypting the Data.
- The Data can be accessed by the third party server and can be accessed by unauthorized users.
- Easily Compromised nodes and Reveals Secure Data.

B. Proposed System

- In the proposed system, the secure sharing of secrecy data is storing on the trusted server storage nodes in presence of key management by users.
- It can be protected using the CP-ABE (Cipher text-Policy Attribute-Based Encryption) can be used to encrypt the particular user data as per the user needs.
- The encryption and the decryption of the key generation can be based on the type of attributes that user chooses.
- In this to improve security the user is categorized into public access data and the personal domains can be categorized.
- In the public domain, we will use multi authority to improve the security and to avoid unauthorized user access problem.
- Probabilistic Value is Calculated for Every nodes to identify node Trust.

1) Architecture

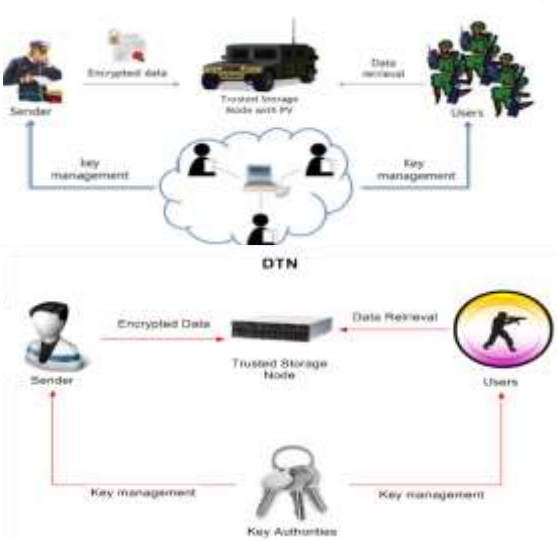

Fig. 1 System Design

2) Advantages

- ❖ Data Integrity and Data Confidentiality is maintained in CP-ABE
- ❖ In this system, improve the performance and Security of accessing the information based on Access policy and CP-ABE Algorithm.
- ❖ In this system, the individual user attribute information is selected based on the user needs of encrypting the data and for easily access using the CP-ABE.
- ❖ Probabilistic value based node trust raises Node Security for Data Transfer.

IV. MODULES

In the proposed system, there are four modules

1) DTN Network Initialization
2) Identify Possible Path from Source to Destination
3) Calculate Probabilistic Values of Intermediate Node
4) Secure Data Transfer by using CB-ABE based on Probabilistic Values

A. Module Description

1) DTN Network Initialization

The DTN network is used for data transfer in Military Applications, due to the Storage Capacity and Coverage type. The DTN network is constructed to the Military Users for Communication to the group of users based on the Coverage range.

The User requested to the DTN network is joined to the network by the network provider Admin. Each Node or User is provided with Network Id and Secure Key for Data Transfer and Communication.

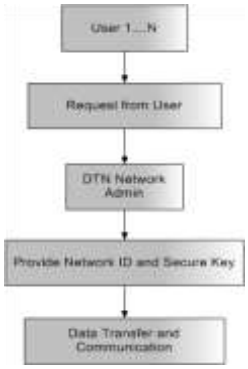

Fig. 2 Network Initialization

2) Identify Possible Path from Source to Destination

In DTN network, the users to communicate with each other, the network users should be within the communicate range. The Network User is to be aware of destination user and make request to the destination user, if the connection is establish to the destination user, then the number of possible path is to be identify from Source User to the Destination user. Then for each path the Intermediate node is to be Determined.

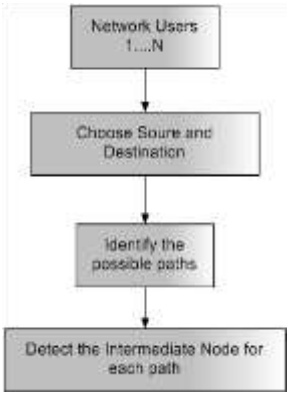

Fig. 3 Identification of Path

3) *Calculate Probabilistic Values of Intermediate Node*

The DTN node is monitored by the Trusted Authority. The Trusted Authority is to calculate the Probability value for each node, For Example consider 3 nodes A,B,C So it distributes a broadcast message to each node A and C enquiring B, If the node A and B relays the Data Transfer Information and Acknowledgement of B to the Trusted Authority, then the trusted Authority calculates the Probabilistic values of the User/Node B based on the received Information.

4) Secure Data Transfer by using CB-ABE based on Probabilistic Values

The DTN node is trusted based on the Probabilistic value, and the Node Security is determined, Now to improve the Security of the Data, the CP-ABE Encryption Scheme is Used, CP-ABE means Cipher Text Policy Attribute based

Encryption it Encrypts thee Plain text to Cipher Text, then the Cipher text is transferred through the trusted node, then the Cipher text is received and decrypted by the Destination node by Efficient Key Management.

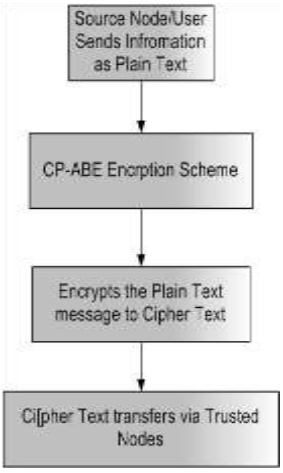

Fig. 4 Data Transfer

B. Algorithm

a. Algorithm 1: The Basic Misbehavior Detection Algorithm

Procedure Basic Detection

((j, $S_{task,}$ $S_{forward,}$[t1,t2], R, D))

1: For Each m € S_{task} do
2: If m not € $S_{forward}$ and R!=0 then return 1
3: else if m € $S_{forward}$ and $N_k(m)$ not C R then
4: return 1
5: else if m € $S_{forward}$ and $N_k(m)$ C R and
6: | $N_k(m)$ |<D then
7: return 1
8: end if
9: end for
10: return 0
11: end procedure

b. Algorithm 2: The Proposed Probabilistic Misbehavior Detection Algorithm

1: Initialize the number of nodes n
2: For i← 1 to n do
3: Generate a random number $m_{i \text{ from } 0 \text{ to } 10n-1}$
4: If $m_{I/10}n < p_b$ then
5: Ask all the nodes (including node i) to provide evidence about node i
6: If Basic Detection (I, $S_{task,}S_{forward,}[t_1,t_2]$,R,D then
7: give a punishment C to node i
8: else
9: pay node i the compensation w
10: end if
11: else
12: pay node i the compensation w
13: end if
14: end for

c. Algorithm 3: CP-ABE

1: Choose a group generator of g=7 and an order of p=13. Group G0={1…12}is Generated.
2: e(X,Y)=gXY mod p
3: Calculate the Public Key and the Master Key with two random integers α=3;β=4:
4: MK={β,gα, e(X,Y)}={4,73}={4,343mod13}={4,5}
5:PK={G0,g,h=gβ,f=g1/β,e(g,g)α}={G0,7,74mod13,71/4mod13,77∗7∗3mod13}={G0,7,9}
6: Encrypt(Ciphertext,MK,PK)

V. CONCLUSION

DTN technologies are becoming successful solutions in military 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 secure 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.

REFERENCES

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANETBased Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, Apr. 2009.
[2] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," Proc. IEEE INFOCOM '10, 2010.
[3] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.
[4] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A SecureMultilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 828-836, 2009.
[5] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858-3868, Oct. 2008.

