"DTN Technology To Provide Security to The Military Networks"

Kamala R
4th Sem
4sm13scs06
Sjmit Chitradurga

Smt.Basantha Kumari Be.Mtech
Project Guide:

***Abstract*—Mobilenodes inmilitaryenvironmentssuch as a battlefieldora hostileregionare likelyto sufferfromintermittent networkconnectivityandfrequentpartitions.Disruption-tolerant network(DTN)technologies arebecomingsuccessful solutions thatallowwireless devices carriedbysoldiers tocommunicate witheachotherandaccesstheconfidential informationorcom- mandreliablybyexploiting external storagenodes. Inthisproject,thepropose of asecuredataretrievalschemeusingCP-ABEfordecentralizedDTNs wheremultiplekeyauthorities managetheirattributesindependently. The demonstration ofhowtoapply theproposedmechanismto securelyandefficiently managetheconfidential datadistributed inthedisruption-tolerantmilitarynetwork.**

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 a source and a 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.

A.RELATED WORK

Roy and Chuah introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, a commander may store a confidential information at a storage node, which should be accessed by members of "Battalion 1" who are participating in"Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing current location of moving soldiers) this project refer to DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

1.2 Proposed System And Its Advantages

The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example,moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a collection of users as an attribute group).

This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example ,if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure, or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy specially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption system such as the attribute-based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their ownmaster secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities. For example, suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and

"region 2" are managed by the authority B. Then, it is impossible to generate an access policy (("role 1" OR "role 2") AND ("region 1" or "region2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Here for, general access policies, such as " -out-of- " logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

B.CONTRIBUTION

Inthispaper,weproposeanattribute-based securedatare-trievalschemeusingCP-ABEfor decentralizedDTNs.Thepro-posedschemefeaturesthefollowingachievements.First,imme-diateattributerevocation enhancesbackward/forward secrecy of confidentialdatabyreducingthewindowsof vulnerability. Second,encryptorscan defineafine-grainedaccesspolicyusing any monotoneaccessstructureunderattributesissuedfromany chosensetofauthorities. Third,thekeyescrowproblemisre-solved byanescrow-freekeyissuingprotocolthatexploitsthe characteristic ofthedecentralized DTNarchitecture. Thekey issuingprotocol generates andissuesusersecretkeysbyper- formingasecuretwo-partycomputation(2PC)protocolamong thekeyauthoritieswiththeirownmastersecrets.The2PCpro-tocoldetersthekeyauthoritiesfromobtaininganymastersecre t information ofeachothersuchthatnoneofthemcouldgen-eratethewhole set ofuserkeysalone. Thus, users arenotre-quiredto fullytrusttheauthoritiesin orderto protecttheirdata tobeshared.Thedataconfidentialityandprivacycanbecrypto-graphicallyenforcedagainstanycuriouskeyauthoritiesordat a storage nodesintheproposedscheme.Fig. 1.Architecture of secure data retrieval in a disruption-tolerant military network.

A.Network architecture

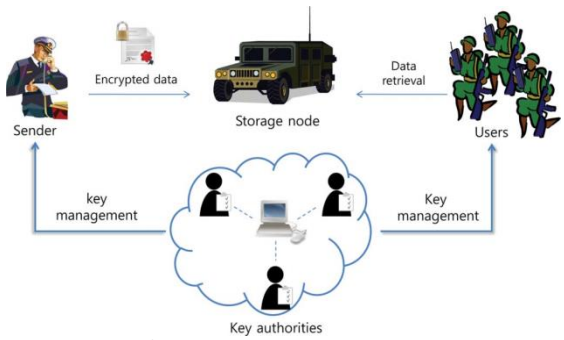

Fig.1.Architectureofsecuredataretrievalinadisruption-tolerant military network.

A. System Description and Assumptions

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

1) Key Authorities: They are key generation centers that gen- erate public/secret parameters for CP-ABE. The key au- thorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and gen- eration phase. Each local authority manages different at- tributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are as- sumed 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) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mo- bile or static [4], [5]. Similar to the previous schemes, we also assume the storage node to be semitrusted, that is honest-but-curious.

3) Sender: 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 envi- ronments. 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.

4) User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user pos- sesses 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.

B. hreatModelandSecurityRequirements

) Dataconfidentiality:Unauthorized userswhodonothave enoughcredentials satisfyingtheaccesspolicyshouldbe deterredfromaccessingtheplaindatainthestoragenode. Inaddition,unauthorized accessfromthestoragenodeor keyauthoritiesshouldbealsoprevented.

2) Collusion-resistance:Ifmultipleuserscollude,theymay beable todecryptaciphertextbycombiningtheirattributes even ifeach ofthe users cannot decrypt the ciphertextalone[11]–[13]. Forexample, supposethereexistauser withattributes {"Battalion 1","Region 1"}andanother userwithattributes{"Battalion2", "Region2"}.Theymay succeedindecryptinga ciphertextencryptedundertheac-cesspolicyof("Battalion 1"AND"Region 2"),evenif eachofthemcannotdecryptitindividually.Wedonotwant thesecolluders tobeabletodecrypt thesecretinforma-tionby combiningtheirattributes.Wealsoconsidercollu-sionattackamongcuriouslocalauthoritiesto deriveusers' keys.

3) Backward andforward Secrecy: Inthecontext ofABE, backwardsecrecymeansthatanyuserwhocomestohold an attribute(thatsatisfiestheaccesspolicy)shouldbe pre-ventedfromaccessing theplaintext oftheprevious data exchangedbeforehe holdstheattribute.Ontheotherhand, forwardsecrecymeansthat any userwhodropsanattribute should beprevented fromaccessing theplaintext ofthe subsequentdataexchangedafterhe dropstheattribute,un-lesstheothervalidattributesthatheis holdingsatisfythe accesspolicy.

III. MODULES

Server Module

Server module allows user to take database space and store their data in the cloud server and here cloud also provide application product as a service by which customer can add their contents to database. And he can also modify and view the contents according to the filename as and when necessary.

Authority Module

Authority module is handled by authority owner which helps customer to register their details to get the authority key to manage the cloud server data and it allows modifying the key when necessary and viewing the key value if user forgot the key. **Customer Module**

Customer is the user who is interested to access Storage as a service and Data as a service from the cloud and they are interested to control the database on their own authorization.

Customer can get authority key from the multiple authorities and use that authority keys to make control the database of cloud server, by using this keys the application and database is all controlled by the customer.

Hardware Requirements

- System : Pentium Dual Core 2.4 GHz.
- Hard Disk : Minimum of 10 GB.
- RAM : Minimum of 1 GB .
- Monitor : 15 VGA Colour.
- Mouse : Standard mouse

Software Requirements

- Operating System : Windows 7 or Higher version.
- Front End : JAVA.
- DATABASE : MYSQL.
- Web Server**:** Glass fish
- Database Connector**:** MySQL ODBC 5.1 Driver
- Front End Designing**:** HTML , Cascading Style Sheet CSS

IV.ALGORITHM

The algorithm used for the security purpose is the Advanced EncrytionStandard(AES) algorithm. The four steps used in each round of AES are Add round key, Byte substitution, Shift rows, and Mix columns.AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits.An iteration of the above steps is called a round. The amount of rounds of the algorithm depends on the key size.

Key Size (bytes)	Block Size (bytes)	Rounds
16	16	10
24	16	12
32	16	14

The only exception being that in the last round the Mix Column step is not performed, to make the algorithm reversible during decryption. AES also has the notion of a word. A word consists of four bytes, that is 32 bits. Therefore, each column of the state array is a word, as is each row. Each round of processing works on the input state array and produces an output state array. AES is an iterated symmetric block cipher, which means that AES works by repeating the same defined steps multiple times. AES is a secret key encryption algorithm. AES operates on a fixed number of bytes.

AES as well as most encryption algorithm is reversible. This means that almost the same steps are performed to complete both encryption and decryption in reverse order. The AES algorithm operates on bytes, which makes it simpler to implement and explain.AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text.

V.IMPLEMENTATION

- **Basic Validation** - First of all, the form must be checked to make sure data was entered into each form field that required it. This would need just loop through each field in the form and check for data.
- **Data Format Validation** - Secondly, the data that is entered must be checked for correct form and value. This would need to put more logic to test correctness of data.

Code as follows:

```
<script>function check(){

n=document.form1.uname.value;

p=document.form1.pass.value;

if(n=="")

{

alert(" Please Enter User Name");

document.form1.uname.focus();

return false;

}
```

```
else if(p=="")
                    {          …….
                               …….}
                    else if(n=="biet" && p=="cse "){
return true;
                    }else
                    {alert(" Invalid User / Password..");
                                        …..
                    return false;}}
```

VI.TESTING

Requirements

Test Cases are derived from the Cloud Server module to test whether cloud properly support storage structure and also to verify whether cloud support proper access of data from the cloud server to user system.

Another Test case are derived from the Customer module where we need to test whether Customer entering data properly or not and the format of the data for validation and storing and retrieving of data from cloud server etc..

Another set of test cases are derived from the Authorities whether authorities properly providing information about key or Not etc..,

VI.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. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

REFERENCES

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

[2] 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.

[3] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–6.

[4] 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.

[5] 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.