ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Attribute-based secure policy encryption in ad hoc networks

M. Udaya Nandhini, R. Mahadevan

1. PG Scholar,SRG College of Engineering,Namakkal
2. Assistant Professor,SRG College of Engineering,Namakkal.,

Manuscript Info

Manuscript History:

Received: 15 March 2015
Final Accepted: 18 April 2015
Published Online: May 2015

Key words:
DTN Technologies,CP-ABE,decentralized DTNs

****Corresponding Author***

M.UdayaNandhini

Abstract

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several securities and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities.

In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

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.

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 methodsthat 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 confidential information at a storage node. 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. The attribute representing current location of moving soldiers. DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN. The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data.

II.BACKGROUND

As high-speed networks and ubiquitous Internet access become available in recent years, many services are provided on the Internet such that users can use them from anywhere at any time. For example, the email service is probably the most popular one. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a cloud. Users just use services without being concerned about how computation is done and storage is managed. Designing a cloud storage system for robustness, confidentialityand functionality. A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers. Data robustness is a major requirement for storage systems. There have been many proposals of storing data over storage servers.

A storage server failure corresponds to an erasure error of the codeword symbol. As long as the number of failure servers is under the tolerance threshold of the erasure code, the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process. This provides a tradeoff between the storage size and the tolerance threshold of failure servers. A decentralized erasure code is an erasure code that independently computes each codeword symbol for a message. Thus, the encoding process for a message can be split into n parallel tasks of generating codeword symbols. A decentralized erasure code is suitable for use in a distributed storage system. After the message symbols are sent to storage servers, each storage server independently computes a codeword symbol for the received message symbols and stores it. This finishes the encoding and storing process.

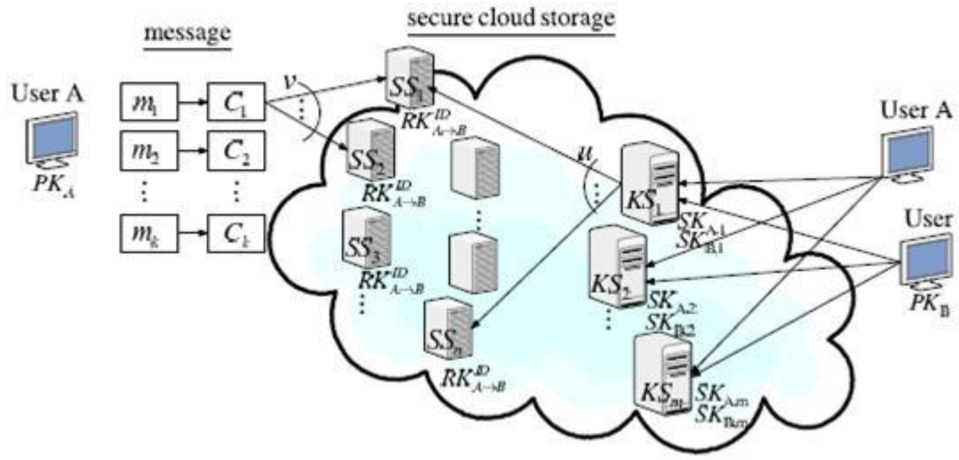

Fig.1cloud storage system

The recovery process is the same. Storing data in a third party's cloud system causes serious concern on data confidentiality. In order to provide strong confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages.

The system model that consists of distributed storage servers and key servers. Since storing cryptographic keys in a single device is risky, a user distributes his cryptographic key to key servers that shall perform cryptographic functions on behalf of the user. These key servers are highly protected by security mechanisms. The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and to encodemessages. The tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding.System meets the requirements that storage servers independently perform encoding and re-encryption and key servers independently perform partial decryption.

Disruption-tolerant network

Disruption-tolerant network is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the networkwould normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications. It is an experimental protocol developed by the Delay & Disruption Tolerant Networking Research Group, which operates under the Internet Research Task Force**.**

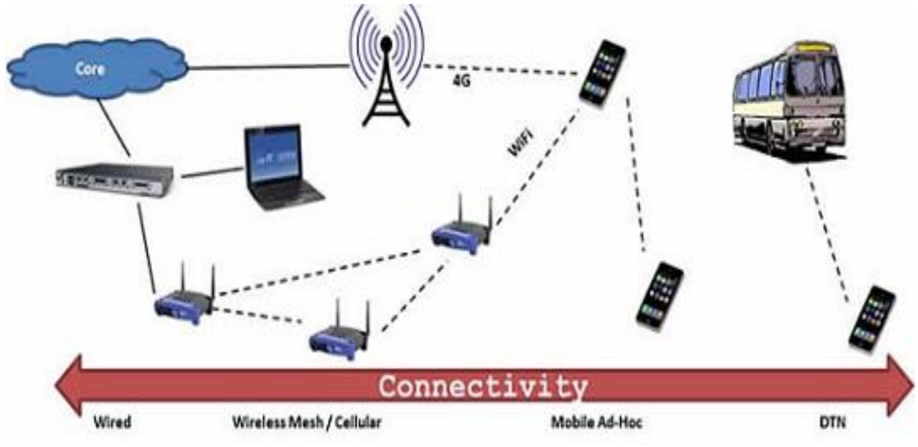

Fig.2: Disruption-Tolerant Networks

A disruption-tolerant network (DTN) is a network architecture that reduces intermittent communication issues by addressing technical problems in heterogeneous networks that lack continuous connectivity. DTN defines a series of contiguous network data bundles that enable applications. This architecture serves as a network overlay that bases new naming on endpoint identifiers.

Effective DTN design depends on the following features:

- ✓ Fault-tolerant methods and technologies
- ✓ Electronic attack recovery
- ✓ Degradation quality from heavy traffic loads
- ✓ Minimal latency due to unreliable routers

DTN nodes enhance network path selection via a naming syntax that supports a broad range of addressing conventions for improved interoperability.

III.PROPOSED SYSTEM

Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts.Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy.

Shamir Key Distribution Algorithm

It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

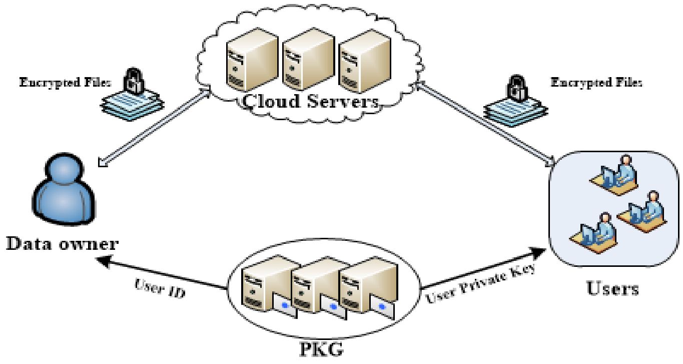

Fig.3: Key Distribution System

Public-Key Cryptography

Public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient.

CP-ABE for decentralized DTNs

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes. The key authority chooses a policy for each user that determines which ciphertexts he can decrypt and issues the key to each user by embedding the policy into the user’s key. However, the roles of the ciphertexts and keys are reversed in CP-ABE. In CP-ABE, the ciphertext is encrypted with an access 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.

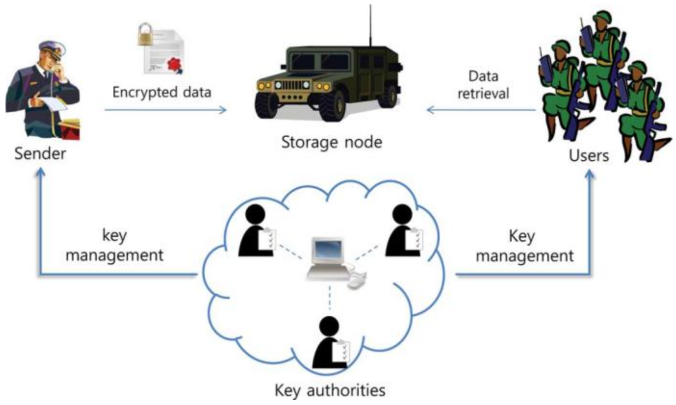

Fig 4:CP-ABE for decentralized DTNs

An attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture.

Key-Policy ABE

KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE, data are associated with attributes for each of which a public key component is defined. The encryptor associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes, i.e., interior nodes of the access tree are threshold gates and leaf nodes are associated with attributes. User secret key is defined to reflect the access structure so that the user is able to decrypt a ciphertext if and only if the data attributes satisfy his access structure

Secure Two-Party Computation (2pc)

The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

Personal Key Generation

In CP-ABE, user secret key components consist of a single personalized key and multiple attribute keys. The personalized key is uniquely determined for each user to prevent collusion attack among users with different attributes. The proposed key generation protocol is composed of the personal key generation followed by the attribute key generation protocols. It exploits arithmetic secure 2PC protocol to eliminate the key escrow problem such that none of the authorities can determine the whole key components of users individually.

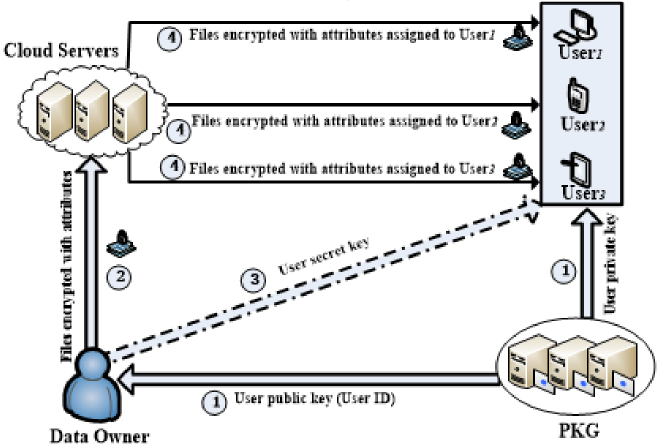
Cloud Servers
4 Files encrypted with attributes assigned to User1
4 Files encrypted with attributes assigned to User2
4 Files encrypted with attributes assigned to User3
User1
User2
User3
Files encrypted with attributes
2
3 User secret key
1 User private key
1 User public key (User ID)
Data Owner
PKG

Fig 5: Personal Key Generations

Attribute Key Generation

During the key generation phase using the 2PC protocol, the proposed scheme (especially 2PC protocol) requires messages additively to the key issuing overhead in the previous multiauthority ABE schemes in terms of the communication cost, where is number of key authorities the user is associated with, and is the bit size of an element in . However, it is important to note that the 2PC protocol is done only once during the initial key generation phase for each user. Therefore, it is negligible compared to the communication overhead for encryption or key update, which could be much more frequently performed in the DTNs.

Advantages of Proposed System

- The secret key is changed dynamically, so the adversaries cannot able to predict the key for cipher text decryption.
- The scalability of data transmission is high due to the access policies generation based on the user's role

IV. IMPLEMENTATION

System Setup

In the system setup phase, the system manager chooses system parameters and publishes them. Everyusers are assigned to a public – secret key pair. Every user wants to share them secret keys with the key servers for secure data forwarding. The users key is divided and distributed to the available key server when the user willing to transfer the data through the cloud storage servers.

Data Storage

In the data storage phase, user A encrypts his message M and dispatches it to storage servers. A message M is decomposed into k blocks m1, m2; ...;m and has a n identifier ID . User A encrypts each block m I k into a ciphertext C and sends it to v randomly chosen storage servers. Upon receiving ciphertexts from a user, each storage server linearly combines them with randomly chosen coefficients into a codeword symbol and stores it. Note that a storage server may receive less than k message blocks and we assume that all storage servers know the value k in advance.

Data Forwarding

In the data forwarding phase, user A forwards his encrypted message with an identifier ID stored in storage servers to user B such that B can decrypt the forwarded message by his secret key. To do so, A uses his secret key SK and B's public key to compute a re-encryption key and then sends to all storage servers. Each storage server uses the encryption key to re-encrypt its codeword symbol for later retrieval requests by B. The re-encrypted codeword symbol is the combination of cipher-texts under B's public key. In order to distinguish re-encrypted codeword symbols from intact ones, we call them original code word symbols and re-encrypted codeword symbols, respectively.

Data Retrieval

In the data retrieval phase, user A requests to retrieve a message from storage servers. The message is either stored by him or forwarded to him. User A sends a retrieval request to key servers. Upon receiving the retrieval request and executing a proper authentication process with user A, each key server KS requests u randomly chosen storage servers to get codeword symbols and does partial decryption on the received codeword symbols by using the key share Sk. Finally, user A combines the partially decrypted codeword symbols to obtain the original message M.

V.CONCLUSION AND FUTURE WORK

A cloud storage system consists of storage servers and key servers. We integrate a newly proposed threshold proxy re-encrypt ion scheme and erasure codes over exponents. The threshold proxy encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. To decrypt a message of k blocks that are encrypted and encoded to n codeword symbols, each key server only has to partially decrypt two codeword symbols in our system. By using the threshold proxy re-encryption scheme, we present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure. Moreover, each storage server independently performs encoding and re-encryption and each key server independently perform partial decryption. Our storage system and some newly proposed content addressable file systems and storage system are highly compatible. Our storage servers act as storage nodes in a content addressable storage system for storing content addressable blocks. Our key servers act as access nodes for providing a front-end layer such as a traditional file system interface. Further study on detailed cooperation is required.

In the Future Work:

Disruption tolerant networks (DTNs) allow for routing in networks where contemporaneous end-to-end paths are unstable or unlikely. Unstable paths can be the result of several challenges at the link layer, for example: high node mobility, low node density, and short radio range; intermittent power from energy management schemes; environmental interference and obstruction; and denial-of-service attacks.

REFERENCES

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

[2] Burgess. J, Gallagher.B ,Jensen.D and Levine. B. N "Maxprop: Routing for vehicle-baseddisruption tolerant networks", Proc. IEEE INFOCOM, pp.1 -11 2006

[3]Chuah. M and Yang. P "Performance evaluation of content-basedinformation retrieval schemes for DTNs", Proc.IEEE MILCOM, pp.1 -7 2007

[4]Chuah. M and Yang. P "Node density-based adaptive routing schemefor disruption tolerant networks", Proc. IEEEMILCOM, pp.1 -6 2006

[5] Chen. N, Gerla. M, Huang. D and Hong. X "Secure, selective group broadcast in vehicular networksusing dynamic attribute based encryption", Proc.Ad Hoc Netw. Workshop, pp.1 -8 2010

[6]Goyal. V, Pandey. O, Sahai. A and Waters.B "Attribute-based encryption for fine-grainedaccess control of encrypted data", Proc. ACMConf. Comput.Commun. Security, pp.89 -98 2006

[7] Huang. D and Verma. M "ASPE: Attribute-based secure policy enforcementing vehicular ad hoc networks", Ad Hoc Netw., vol. 7, no. 8, pp.1526 -1535 2009

[8] Ibrahim. L ,Petkovic. M ,Nikova. S ,Hartel. P and Jonker. W "Mediated ciphertext-policyattribute-based encryption and its application", Proc.WISA, pp.309 -323 2009

[9]Kallahalla. M, Riedel. N,Swaminathan.R ,Wang. Q and Fu. K "Plutus: Scalable secure file sharing on untrusted storage", Proc. Conf. File Storage Technol., pp.29 -42 2003

[10]Lewko. A andWaters. B Decentralizing attribute-basedecryption, 2010

[11]Ostrovsky. R ,Sahai. A and Waters. B "Attribute-based encryption with non-monotonicaccess structures", Proc. ACM Conf. Comput.Commun. Security, pp.195 -203 2007

[12] Roy. S andChuah. M “Secure data retrieval based on ciphertext policy attribute-basedencryption (CP-ABE) system for the DTNs” , 2009

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

[14]Tariq. M. M. B,Ammar. M and Zequra. E "Message ferry route design for sparse adhoc networks with mobile nodes", Proc. ACM MobiHoc, pp.37 -48 2006

[15] Yu. S ,Wang. C ,Ren. K and Lou. W "Attributebased data sharing with attribute revocation", Proc.ASIACCS, pp.261 -270 2010