A

Seminar II Report

on

SECURE DATA RETRIEVAL FOR MILITARY NETWORKS

Submitted in Partial Fulfillment of
the Requirements for the Degree
of

Bachelor of Engineering

in

Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Snehal Anil Patil

Under the Guidance of

Mrs. Shital A. Patil

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI, JALGAON - 425 001 (MS)
2016 - 2017

SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the Seminar II entitled *Secure Data Retrieval for Military Networks*, submitted by

Snehal Anil Patil

in partial fulfillment of the degree of *Bachelor of Engineering* in *Computer Engineering* has been satisfactorily carried out under my guidance as per the requirement of North Maharashtra University, Jalgaon.

Date: October 5, 2016
Place: Jalgaon

Mrs. Shital A. Patil
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgements

I, Snehal Anil Patil would like to express my gratitude and appreciation to all those who helped me to complete this report. A special thanks to my guide Mrs. Shital A. Patil, whose help, stimulating suggestions and encouragement, helped me to coordinate my seminar especially in writing the report.

Many thanks goes to Dr. K. S. Wani (Principal of Shram Sadhana Bombay Trust, College of Engineering and Technology, Bambhori) and Dr.Girish Kumar Patnaik (Head of the Department,Computer Engineering, Shram Sadhana Bombay Trust, College of Engineering and Technology, Bambhori) who have given their full effort in guiding me in achieving the goal as well as encouraged me to maintain my progress in track. I would appreciate the guidance given by other supervisor as well as the panels especially in my Seminar II, that has improved my presentation skills by their comment and tips.

I would also like to acknowledge with much appreciation the crucial role of the staff of Computer Department, who helped me a lot and gave the permission to use all required machinery and the necessary material to complete the report.

Last but not the least, many thanks to my parents and friends who are always there to support me. Their support helped me a lot to complete the report and encouraged me to maintain my progress in track. Thank you!

Snehal Anil Patil

Contents

List of Figures

Abstract

DTN (Disruption Tolerant Network) is successfully solution to allow the wireless devices which is useful to soldiers to connecting each other mobile nodes in battlefield or hostile region to distress form the intermediate network connectivity and achieve secure data or some command by reliable to explore from external node. The most challenging thing in the cases are enforcement of authorized policies. Ciphertext-policy attribute-based encryption is a reliable cryptographic solution to access control problems. Hence the problem of applying (CP-ABE) Ciphertext Policy attribute based encryption for decentralized DTNs is providing many security and privacy challenges issued from different attributes.CP-ABE for decentralized DTNs define how to secure data and retrieval scheme multiple key authorities manage their attributes independently. It described that how securely and efficiency manage the confidential data by applying proposed mechanism which is distributed in the disruption-tolerant military network.

Chapter 1

Introduction

Network provides a sharing of data among different users with the help of wireless devices. For It, a network must provide a secure communication among the network for data transfer to the entire user in the network. With the wireless network, transfer of data done with the help of the intermediate node, Data lose because of unauthorized user in the network hack the data.

In Section 1.1 describes the Disruption-tolerant network (DTN). The Public keys and attributes are presented in section 1.2. Section 1.3 describes the summary of chapter.

1.1 Disruption-tolerant network (DTN)

In section,what is Disruption-tolerant network (DTN) is discuss.It is a technology which allows the node to communicate with each other in secure manner . It is one of the successful solutions for transferring the data in network.

Most of the military users use technology for secure transfer of the data. In the large number of outgrowing commercial environment such as military each and everything based on the another sources to broadcast the data strongly and maintain the data as well in the regular medium.when It is no end to end communication among a source and a destination pair, the data from the source node want to stay in the intermediate nodes for an extensive amount of time until the connection would be ultimately established.[8][9] DTNs maintain interoperability of networks by cooperating a long disruptions and delays among those networks, and by communicating among the communications protocols of those networks. DTNs can accommodate many kinds of wireless technologies, including radio frequency (RF),, free-space optical, and Transportable nodes in military environments, for example, in an antagonistic area are horizontal to practice in endure of asymmetrical system network and numerous partitions. Disruption-tolerant network (DTN) modernisms are receiving to be productive results that authorize remote device conveyed by officers to speak with one another and admit the private data or secret data or beckon unvaryingly by neglecting outside capacity

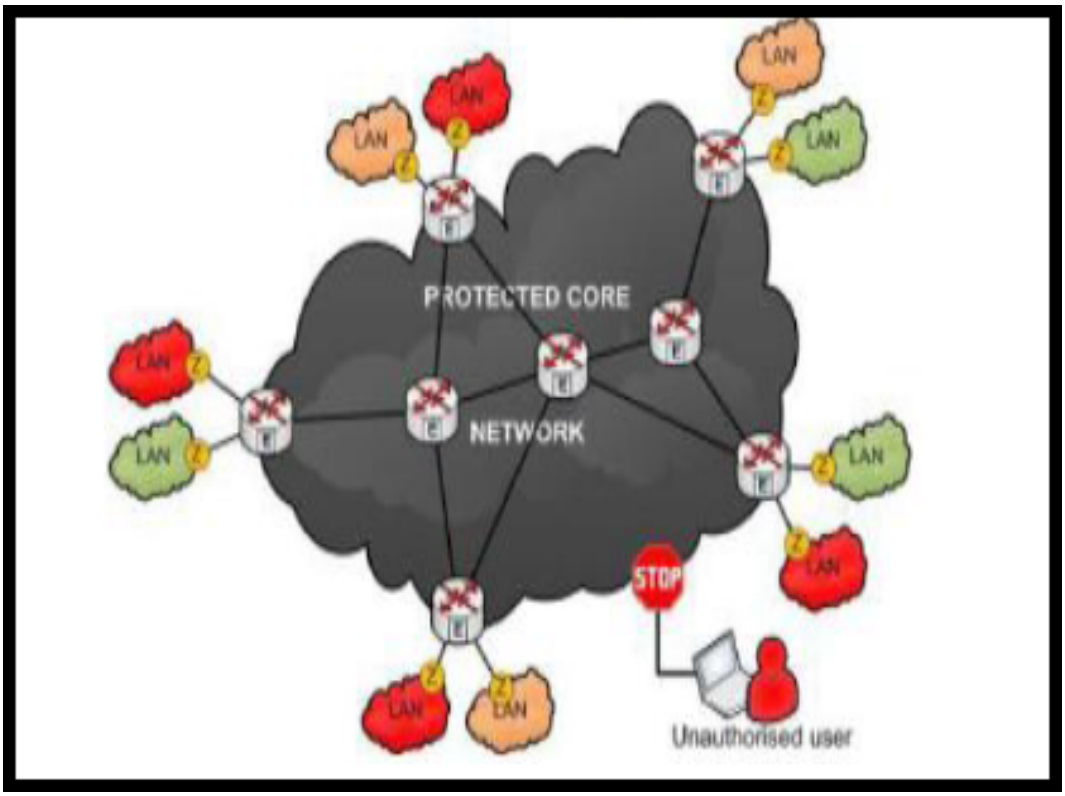

Figure 1.1: Military Networks

nodes or storage nodes.[?]

A DTN node can forward package between two or more other nodes in one of two situations they were Routing and Equivalent Forwarding. In DTNs, data is stored or pretend such that only authorized mobile nodes can entre the required information rapidly and efficiently. In DTN, the multiple authorities problem and to managing their own attribute keys independently as a decentralized DTN. In Military environment network have to provide a better secure manner of data transferring mechanism among the nodes.The comprehensive study of many techniques for the sharing of data in the network.[7]

In many military network scenarios, connections of wireless devices carried by soldiers be temporarily disconnected by jamming, environmental factors, and mobility,especially when It 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 no end to-end connection between a source and a destination pair, the messages from the source node need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. They introduced storage nodes in DTNs data is stored or replicated such that only authorized mobilenodes 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.[9][8]

In section what is Disruption-tolerant network (DTN) and next section describes the public key and attributes.

1.2 Public keys and attributes

In section the key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE) are discuss. 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 users key. 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.[5]

1.2.1 Attribute Revocation

Bethencourt et al. and Boldyreva et al.first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy .

It is a considerable scenario that users such as soldiers change their attributes frequently,e.g., position or location move when considering these as attributes. Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time, a ciphertext is encrypted with a policy that can be decrypted with a set of attributes (embedded in the users keys) for users with. After time say a user newly holds the attribute set.

Even if the new user should be disallowed to decrypt the ciphertext for the time instance, he can still decrypt the previous ciphertext until it is reencrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the encrypted data even if he does not hold the attribute any more until the next expiration time (forward secrecy). For example, when a user is disqualified with the attribute at time, he can still decrypt the ciphertext of the previous time instance unless the key of the user is expired and

the ciphertext is reencrypted with the newly updated key that the user cannot obtain.Call it uncontrolled period of time windows of vulnerability.[5]

The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the nonrevoked users can update their keys.Results in the 1-affects- problem, which means that the update of a single attribute affects the whole nonrevoked users who share the attribute.It could be a bottleneck for both the key authority and all nonrevoked users. The immediate key revocation can be done by revoking users using ABE that supports negative clauses.

To do so, one just adds conjunctively the AND of negation of revoked user identities (Each is considered as an attribute). Solution still somewhat lacks efficiency performance.Scheme pose overhead group elements1 additively to the size of the ciphertext and multiplicatively to the size of private key over the original CP-ABE scheme of Bethencourt et al, It is the maximum size of revoked attributes set. Golle et al. also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a ciphertext is exactly half of the universe size. [5]

1.2.2 Key Escrow

Most of the existing ABE schemes are constructed on the architecture a single trusted authority has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. Chase et al. presented a distributed KP-ABE scheme that solves the key escrow problem in a multiauthority system.

All (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of It's fully distributed approach is the performance degradation.It is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a users secret key. In communication overhead on the system setup and the rekeying phases and requires each user to store additional auxiliary key components besides the attributes keys,It is the number of authorities in the system.[5]

1.2.3 Decentralized ABE

The decentralized CP-ABE schemes in the multiauthority network environment. It achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages are efficiency and expressiveness

of access policy. For example, when a commander encrypts a secret mission to soldiers under the policy (Battalion 1 AND (Region 2 OR Region 3)),it cannot be expressed when each Region attribute is managed by different authorities, since simply multi encrypting approaches can by no means express any general -out-of- logics (e.g., OR, that is 1-out-of-). For example, let be the key authorities, and be attributes sets they independently manage, respectively.[**?**] The only access policy expressed with is, which can be achieved by encrypting a message with by, and then encrypting the resulting ciphertext with by (It is the ciphertext encrypted under), and then encrypting resulting ciphertext with by, and so on, until multiencryption generates the final ciphertext .The access logic should be only AND, and they require iterative encryption operations It is the number of attribute authorities. Somewhat restricted in terms of expressiveness of the access policy and require computation and storage costs.The multiauthority KP-ABE and CP-ABE schemes, respectively. Schemes also suffer from the key escrow problem like the prior decentralized schemes.[8]

In Section,Public keys and attributes are discussed and in the next section summary is discussed and the next section is about summary.

1.3 Summary

In this chapter,Introduction of Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks.In the next chapter Literature Survey is presented .

Chapter 2

Literature Survey

It is a technology which allows the node to communicate with each other in secure manner. It is one of the successful solutions for transferring the data in network.It is a considerable scenario that users such as soldiers change their attributes frequently, if user join or leave the group.

In section 2.1 is Background and History.It describes the history and development of Secure Data Retrieval for Military Networks is discuss and Finally the Summary is presented in last Section 2.2.

2.1 Backgroud and History

Bethencourt et al. and Boldyreva et al.first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively Key revocation mechanisms in CP-ABE.Technique use to solve the problem of attribute revocation. Solution to distribute a new key to valid users after the expiration. Scheme is secure against collusion attack. Problem of security degradation in terms of backward and forward secrecy. It is a considerable scenario that users such as soldiers change their attributes frequently, if user join or leave the group. For e.g., position or location move when considering these as attributes. Distributed KP-ABE scheme that solves the key escrow problem in a multi authority system.

All (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. The advantage of scheme is to enable more realistic deployment of attribute base access control. But One disadvantage of fully distributed approach is the performance degradation. It is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a users secret key.[1]

Decentralized CP-ABE schemes in the multi authority network environment. They achieved a combined access policy over the attributes issued from different authorities by

simply encrypting data multiple times. The advantage of scheme is flexible fine grained access policy. But the main disadvantages of approach are efficiency and expressiveness of access policy.Novel protocol called MaxProp for routing of DTN messages. MaxProp identifies the issue of scheduling packets for transmission to other peers and determining which packets should be deleted when buffers are low on space. Performance of the proposed protocol is better than the other protocols. Propose a DTN routing protocol, called MaxProp that performs significantly better than previous approaches. Proposed approach is depends upon prioritizing both the schedule of packets send to other peers and the schedule of packets to be dropped or deleted when buffers are low on space.[2]

Information retrieval system for disruption tolerant networks (DTN). They demonstrated a content-based information retrieval system designed for DTNs. While designing author address three main issues such as first, how data should be replicated and stored at multiple nodes, second how a query should be disseminated in sparsely connected networks and third how a query response should is routed back to the querying node. For query dissemination author used an scheme and Prophet routing scheme or scheme is used for message routing. Proposed approach achieved smaller query response time and hence achieve higher query success rate using the HEFR scheme.Novel method called Plutus as cryptographic storage system to achieve secure file sharing in the presence of untrusted servers. Almost all requirements for server trust are removed and handles by single data owners as base for a secure storage system that can defend and share data at very large scales and across trust boundaries. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. Proposed approach is more secure and efficient. Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.[4]

Attribute-Based Encryption (ABE) scheme that allows a users private key to be expressed in terms of any access formula over attributes. Previous ABE schemes were limited to expressing only monotonic access structures. It provide a proof of security for scheme based on the Decisional assumption. Furthermore, the performance of new scheme compares favorably with existing, less-expressive schemes.Efficient cryptosystem for fine-grained sharing of encrypted data that is . In proposed cryptosystem, ciphertexts are tag with sets of attributes and private keys are related with access structures that control which ciphertexts a user is able to decrypt. Proposed approach is applicable to sharing of audit-log information and broadcast encryption. It also supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).[3][1]

A System for realizing complex access control on encrypted data that call Cipher-text

Policy Attribute-Based Encryption. By using techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover,methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into users keys; while in system attributes are used to describe a users credentials, and a party encrypting data determines a policy for who can decrypt. Thus,methods are conceptually closer to traditional access control methods such as . In addition,Provide an implementation of system and give performance measurements.[2]

In section describes the Decentralise technology and the history and next is about the Summary about the chapter.

2.2 Summary

In this chapter, Background and History of Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks is discuss.It describes the all events related to the Secure Data Retrieval for military network. In the next chapter Methodology is presented.

Chapter 3

Methodology

System is composed of medical sensor nodes, a hand-held personal server, a hospital server and related services. medical sensor nodes are used to collect physiological signals including bio-signals, medical images, and voice signals. These obtained signals are fed into the personal server through wireless personal area network (WPAN).

Section 3.1 describes Architecture of System.It is composed of medical sensor nodes. The System Description and Assumptions is presented in section 3.2. Finally the Summary is presented in last section.

3.1 System Architecture

Key Powes: Key era focuses that create open/mystery parameters for CP-ABE. The key powers comprise of a focal power and numerous neighborhood powers. It is secure and dependable correspondence channels between a focal power and every neighborhood power amid the starting key setup and era stage. Every neighborhood power oversees diverse characteristics and issues relating credit keys to clients. It give differential access rights to individual clients focused around the clients' traits.The key powers are thought frankly inquisitive. That is, they sincerely execute the allotted undertakings in the framework; nonetheless they might want to learn data of scrambled substance much as could reasonably be expected.

Storage Nodes: It is a substance that stores information from senders and give comparing access to clients. It might be portable or static. Like the past plans, Additionally expect the capacity hub to be semiassumed that is fair yet inquisitive.

- Sender: It is an element who claims private messages or information (e.g., a commandant) and wishes to store them into the outer information stockpiling hub for simplicity of imparting or for dependable conveyance to clients in the amazing systems administration situations.[4]

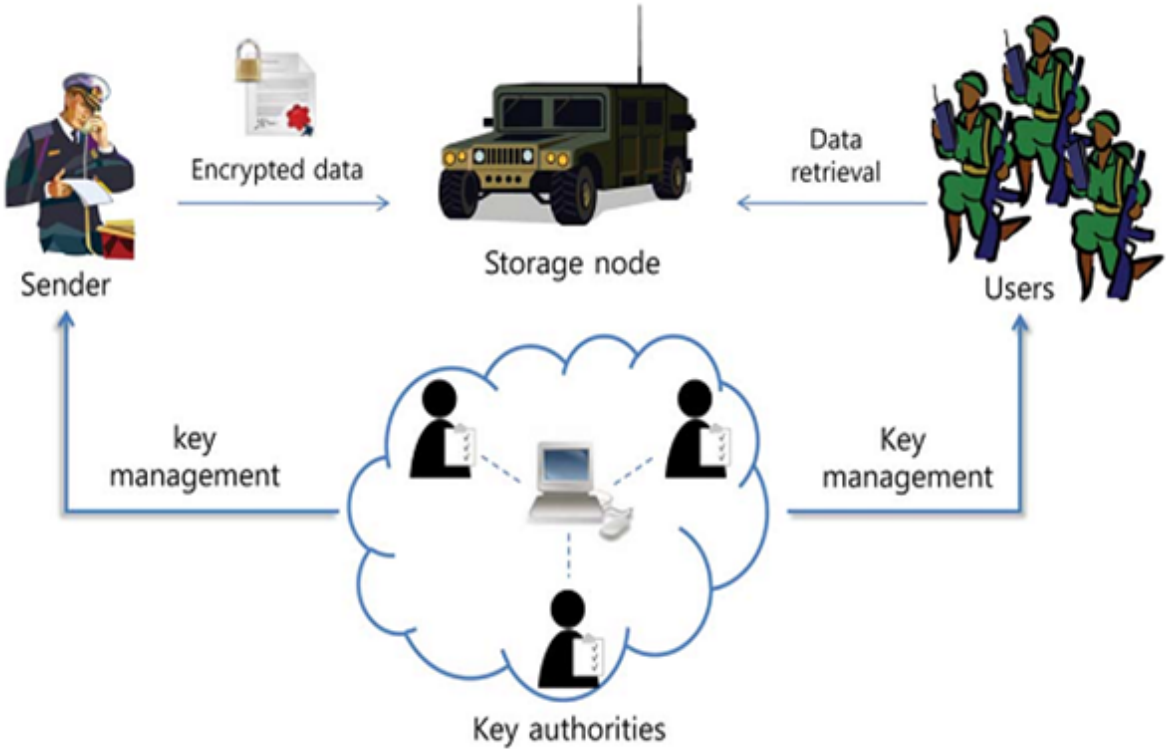

Figure 3.1: The Architecture of the DTN

- Clients: It is a versatile hub that needs to get to the information put away at the stockpiling hub (e.g., a fighter). In the event that a client has a set of properties fulfilling the right to gain entrance approach of the encoded information characterized by the sender, and is not disavowed in any of the qualities, then it has the capacity to decode the ciphertext and get the information.

CP-ABE Policy: In Ciphertext Approach Quality based Encryption plot, The encryptors can alter the arrangement, who can decode the scrambled message. The strategy could be structured with the assistance of characteristics. In CP-ABE, access arrangement is sent alongside the ciphertext. A system in which the right to gain entrance approach require not be sent alongside the ciphertext, by which It has the capacity safeguard the security of the encryptor. Methods encoded information might be kept classified regardless of the fact that the stockpiling server is untrusted; besides, techniques are secure against intrigue assaults. Past Characteristic Based Encryption frameworks utilized credits to portray the encoded information and incorporated arrangements with client's keys; while in framework ascribes are utilized to depict a client's qualifications, and a gathering encoding information decides an arrangement.[4]

So one factor have a tendency to do all time is store files on remote servers. It has varieties of reasons why It has a tendency to do it. It has a tendency to might want to supply

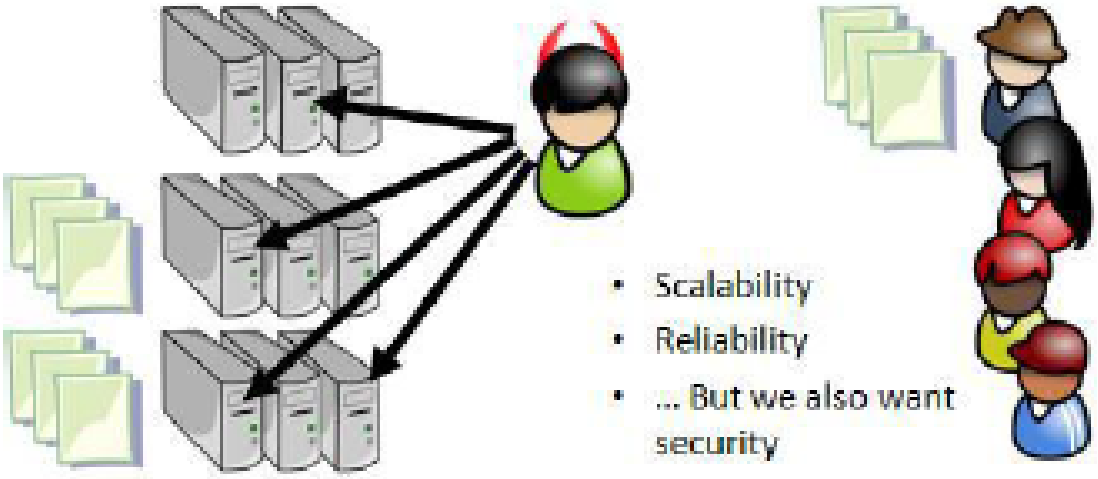

Figure 3.2: Remote File Storage: Interesting Challenges

scalable access to files to others victimization further resources on the market elsewhere.– It has a tendency to might want a lot of dependability just in case of failures. During case tendency to might want to duplicate files totally different information centers or with different organizations. It would like security. It has a tendency to could have needs on World Health Organization access that files. The fascinating factor is, Tension between security and the alternative properties.

The policy is satisfied, decryption just work, otherwise it wont. situation square measure the social control of authorization policies and the policies update for secure information retrieval. could be a promising cryptanalytic resolution to the access management problems. The matter of applying CP-ABE in suburbanized DTNs introduces many security and privacy challenges with relevance the attribute revocation, key escrow, and coordination of attributes issued from completely different authorities.[4] [10]

In section Describes the Functioning of the system and next is about the System Description And Assumption.

3.2 System Description and Assumptions

In section, describes about the System Description and assumptions like key authority,storage node,sender,user.

- Key Authorities: They are key generation centers that generatepublic/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. It assume, 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 honestly execute the assigned tasks in the system, They would like to learn information of encrypted contents as much as possible.[2]

- Storage node: It is an entity that stores data from senders and provide corresponding access to users. It mobile or static. Similar to the previous schemes,It also assume the storage node to be semitrusted, that is honest-but-curious.

- Sender: It 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 (attributebased) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

- User: It 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, the It is able to decrypt the ciphertext and obtain the data. Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users. In order to realize somewhat contradictory requirement, the central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and suing phase. The 2PC protocol prevents them from knowing each others master secrets so that none of them can generate the whole set of secret keys of users individually. Take an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).[1]

3.3 Summary

In this chapter System Architecture,System Description and Assumptions is Discussed.In the next chapter Discussion is Presented.

Chapter 4

Discussion

4.1 Advantages and Disadvantages

In section the Advantages and Disadvantages of Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks is presented.

4.1.1 Advantages of Secure Data Retrieval

In Subsection describes the Advantages[5]

- Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

- Collusion-resistance: If multiple users collude, It able to decrypt a ciphertext by combining attributes even if each of the users cannot decrypt the ciphertext alone. For example, Exist a user with attributes Battalion 1, Region 1 and another user with attributes Battalion 2, Region 2. It succeed in decrypting a ciphertext encrypted under the access policy of (Battalion 1 AND Region 2), even if each of them cannot decrypt it individually. it do not want these colluders to be able to decrypt the secret information by combining the attributes. It also consider collusion attack among curious local authorities to derive users keys.

- Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data

exchanged after he drops the attribute, unless the other valid attributes that it is holding satisfy the access policy.

4.1.2 Disadvantages of Secure Data Retrieval

In subsection describes the disadvantages.[5]

- The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users 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.
- Issue is even more difficult, especially in systems, since each attribute is conceivably shared by multiple users (henceforth, It refer to such a collection of users as an attribute group)
- Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authoritys master secret keys to users associated set of attributes.
- The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attributes keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities.

4.2 Summary

In this chapter,The Advantages,Disadvantages,Application of Secure data retrival is presented and in the next chapter conclusion is presented.

Chapter 5

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. CPABE is a scalable cryptographic solution to the access control and secure data retrieval issues.It is an efficient and secure data retrieval method using CP-ABE for decentralized DTNs 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.[6]

The fine-grained key revocation can be done for each attribute group. It demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.Improve the storage capacity by introducing multiple Data storages where each storage belongs to particular type of users.[6]

Bibliography

[1] International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 2, February 2016

[2] Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM YEAR 2014

[3] Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks Arram Sriram Asst.Prof, IT Depatment, Anurag Group of Institutions V: Venkatapur, M: Ghatkesar, D: Rangareddy, Telangana, 501301.January 2016

[4] Securing Data Retrieval for Decentralized Disruption-Tolerant Military Networks (DTNs) using Cipher text- Policy Attribute-Based Encryption Umoh Bassey Offiong1, M. B. Mukeshkrishnan2 5 august 2015

[5] S. Roy and M. Chuah, Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs, Lehigh CSE Tech. Rep., 2009.

[6] Decentralized Interruption-Tolerant using Secure Data Rescue for Armed Force Networks Manjula HT1, Amreen Khanam1, Sumathi D.1 1Assistant Professor, Dept of CSE, HKBK College of Engineering, Bangalore

[7] R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures, in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 195203.

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

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

[10] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.

Index