ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Key Escrow Removal Using Random Oracle in CP-ABE for Security in Military Networks

Hiral Patel[1], M. A. Lokhandwala[2]

PG Research Scholar, Electronics & Communication, Parul Institute of engineering & Technology, Vadodara, India[1]

Assistant Professor, Electronics & Communication, Parul Institute of engineering & Technology, Vadodara, India[2]

Abstract: In this paper, Confidential Data Security Methodology has been modified by using random key authority generation replacing two-party computation protocol to remove the disadvantage KEY ESCROW, with recent adoption and spreading of data sharing. One or more trusted parties supply information to decrypt ciphertext. Trusted parties are known as central authorities provide information in form of data recovery keys. Key escrow refers to the safeguarding of those data recovery keys. In this paper random key distribution in CP-ABE is explained and simulated to secure the confidential data. The definitive approach CP-ABE provides the addition of access policies and its updates. It has been demonstrated how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Keywords: Access Control, Attribute Based Encryption (ABE), Disruption-Tolerant Networks (DTN), multiauthority, secure data retrieval.

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 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.

Disruption **T**olerant **N**etworking is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would 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.

DTN works using different kind of approach than TCP/IP for packet delivery that is more resilient to disruption than TCP/IP. DTN is based on a new experimental protocol called the Bundle Protocol (RFC 5050). The Bundle Protocol (BP) sits at the application layer of some number of constituent internets, forming a store-and-forward overlay network. BP operates as an overlay protocol that links together multiple subnets (such as Ethernet-based LANs) into a single network.

The basic idea behind DTN network is that endpoints aren't always continuously connected. In order to facilitate data transfer, DTN uses a store-and-forward approach across routers that is more disruption-tolerant than TCP/IP. However, the DTN approach doesn't necessarily mean that all DTN routers on a network would require large storage capacity in order to maintain end-to-end data integrity.

A common technique used to maximize the probability of a message being successfully transferred is to replicate many copies of the message in the hope that one will succeed in reaching its destination. This is feasible only on networks with large amounts of local storage and internodes bandwidth relative to the expected traffic. In many common problem spaces, this inefficiency is outweighed by the increased efficiency and shortened delivery times made possible by taking maximum advantage of available unscheduled forwarding opportunities. In others, where available storage and internodes throughput opportunities are more tightly constrained, a more discriminate algorithm is required.

II. CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION

One of the most challenging issues in confidential data sharing systems is the enforcement of data access policies and the support of policies updates. Cipher text policy attribute based encryption (CP-ABE) is becoming a promising cryptographic solution to this kind of problem. It enables data owners to define their own access policies over their user attributes and enforce the policies on the data to be distributed.

However, the advantage of the system comes with a major drawback which is known as a key escrow problem. The key generation center could decrypt any kind of messages addressed to specific users by generating their private keys. This is not suitable for data sharing typical scenarios

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

where the data owner would like to make their private data only accessible to designated users.

III. BACKGROUND

A Before we explain the details of our scheme, we first introduce the background of our work, including bilinear maps and CP-ABE algorithm.

A. Bilinear Maps

We introduce some related facts of groups with efficiently computable bilinear maps.

Let G1 and G2 be two multiplicative cyclic groups of prime order p. Let g denote the generator of G1 and e be a bilinear map,

e : G1 ×G1 → G2

The bilinear map e satisfies the following requirements:

Bilinear: for all u, v ∈ G1 and a, b ∈ Zp, we have
e(ua, vb) = e(u, v)ab

Non-degeneracy: e(g, g) _ 1.

Computable: There is a polynomial time algorithm to compute the group operation in G1 and the bilinear map
e : G1 × G1 → G2

Notice that the map e is symmetric since
e(ga, gb) =e(g, g)ab = e(gb, ga)

B. CP-ABE Algorithm

In CP-ABE system, the access policy is determined by DO, so it is suitable for access control applications. In this paper, the cryptographic access control is achieved by CPABE. The CP-ABE scheme [4] consists of four probabilistic polynomial-time algorithm and its formal model is as follows.

Setup(λ). This is a randomized algorithm that takes security parameter λ as input. It outputs the public parameters PK and a secret master key MK.

Encrypt(PK, M, A). This algorithm takes public parameters PK, a message M, and an access structure A over the universe of attributes as input. The encrypting procedure produces a ciphertext CT such that only a user own a set of attributes that satisfies.

A will be able to decrypt the message. We will assume that the ciphertext implicitly contains access policy A.

KeyGen(MK, S). This key generation algorithm takes as input the master key MK and a set of attributes S. It outputs a private key SK described by S.

Decrypt (PK, CT, SK). This algorithm takes as input the public parameters PK, a ciphertext CT, and a private key SK. If the attributes set contained in SK satisfies the access policy A in CT, this algorithm will decrypt the CT and return a message M.

C. Related Work

Attribute Based Encryption (ABE) is derived from Identity-Based Encryption(IBE), where IBE can be viewed as a special case of ABE actually. Sahai and Waters introduced fuzzy identity-based encryption as a primitive work of ABE. And later the ABE systems are divided into KP-ABE and CP-ABE by Goyal et al. In KP-ABE systems, an encrypted ciphertext is associated with a set of attributes, and a user's private key represents the access structure over attributes. Contrary to KP-ABE, in CP-ABE systems a user's private key is associated with attributes and an encrypted ciphertext will reflect the access policy. Both in KP-ABE and CP-ABE systems, a user will be able to decrypt ciphertext if and only if the attributes set satisfies the access policy.

To date, a number of different constructions of ABE have been proposed. Most of their constructions are based on Secret Sharing Schemes (SSS); the exception is constructed through AND gates. In these SSS-based systems, a randomness (or the system's master key, is divided into shares by using SSS; and then these shares are embedded into user secret keys (KP-ABE) or ciphertext components (CP-ABE). In the AND gates based system, the master key is embedded into private key and ciphertext components directly. Generally speaking, the SSS based scheme is more expressive than the other one. The SSS based ABE algorithm usually takes access tree, or LSSS matrix as the access structure. Because SSS are limited to expressing monotonic access structures (since a participating party can always choose not to contribute his share), the corresponding ABE scheme can not support negative constraints.

IV. SECURITY

A. 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.

B. Collusion-resistance:

If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone. For example, suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion2","Region2"}. They may succeed in decrypting a ciphertext encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them can not decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive users' keys.

C. Backward and forward Secrecy:

In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

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 he is holding satisfy the access policy.

V. PROPOSED BLOCK DIAGRAM

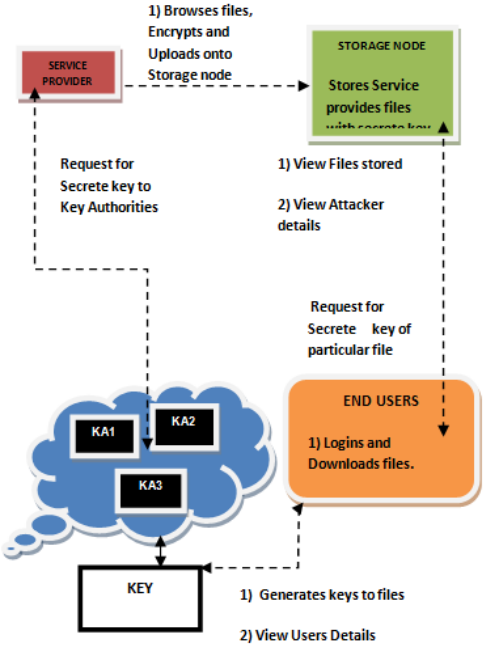


Figure 1: Proposed Block Diagram of System

The Service provider /Sender are responsible for registering the Users by providing their details, including Battalion and Region.

The Service Provider/Sender Browses the data File, encrypts it and generates the key from Key Authority Server (KA1, KA2, and KA3) and uploads file to the destination.

The DTN Router stores the encrypted data file and their details in the Storage Node.
The End User Request to the storage node using their credentials like file Name, secret key, Battalion and Region.

Then storage node connects to the respective Key authority server. If all credentials are correct then user is authorized to receive the file.

If the user gives wrong credentials file name, secret key, Battalion, Region, then the end user will considered as non authorized user.

VI. MAIN ISSUE

There are possibilities of threats to data like offensive use of the data by the storage server or illegal access by outer users. Users may wish to visible their private data to specified persons by giving some credentials. A potential cryptographic advance that achieves an elegant data access control is Attribute-based encryption. Depending on the attributes of the requester and data object it defines access policies. Particularly, cipher text policy attribute-based encryption allows encryption of attribute set and decryption needs to have in order to decrypt the ciphertext, and impose it on the data. Therefore, each user with a diverse set of attributes is permitted to decrypt dissimilar pieces of data for each security policy. To prevent unauthorized data access our CP-ABE reduces the need to depending on data storage server (DSS).

On the other hand, the advantage of the CP-ABE comes with a most important disadvantage which is known as a KEY ESCROW or written agreement problem. By generating their attribute keys the KGC will decrypt every ciphertext addressed to specific users which is a potential hazard to the data privacy or secrecy in the distributed data sharing systems. One more challenge in Distributed data sharing system is the key revocation. In order to make systems secure, update of each attribute is necessary as a few users may alter their attributes at some time or few private keys might be negotiated. This matter is still more complicated particularly in ABE, as each attribute is possibly shared by multiple users. The cancellation of any attribute or single user from an attribute group or set of users will influence all users in that group. As a consequence, there may be a constrained access during rekeying procedure or security ruin due to the windows of defenselessness.

VII. BACKGROUND

The usual method of splitting key K into two keys K0 and K1 given to two parties for the purpose described follow
Generate K1 randomly of the same size as K
Set K0 = K XOR K1

Joining K0 and K1 into K is simply K = K0 XOR K1. This construct is such that each of two parties gain absolutely no advantage by getting its split key Kj
Unless it also gets the other, it is just random and unrelated to K

This can be generalized to n>2 parties that must all collaborate to reconstruct K
Generate K1 to K_{n-1} randomly of the same size as K
Set K0 = K XOR K1 XOR …. XOR K_{n-1}
Ofcourse after joining K = K0 XOR K1 XOR XOR K_{n-1}

VII. SIMULATION SOFTWARE

The Network simulator tool is a generic tool which has large use base and support. It can be utilized for many purposes. Almost all new research on computer Networks uses the tool. NS has significantly more global appeal and research base. NS has a "Real Time Emulation" feature by virtue of which nodes in a NS simulation can be interfaced with real time applications and data.

IX. SIMULATION RESULTS

This section presents the simulation results of the parameters of Energy, Delay and Throughput in system.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Here are some images of the screen shots of this system which got after successful execution of the entire system. This system works efficiently with the lowest time delay. This is because of CP-ABE algorithm and DTN network. The processed confidential data uploaded to DTN network and transmitted through wireless device so that user input key to corresponding sender for particular data and then the confidential data is provided to used after deciphering as shown in below Figure 2. Figure 3(c) shows **Throughput** is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node.

$X = C/T$

Where X is the throughput, C is the number of requests that are accomplished by the system, and T denotes the total time of system observation.

Figure 3(b) shows **End-to-End delay** signifies how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time.

$D_{end\text{-}end} = N(d_{trans} + d_{prop} + d_{proc} + d_{queue})$

Where delay end-end= end-to-end delay, d_{trans} = transmission delay, d_{prop}= propagation delay, d_{proc}= processing delay, d_{queue}= queuing delay, N= Number of links.

Figure 3(a) shows **Energy**, The metric is measured as the percent of energy consumed by a node with respect to its initial energy. The initial energy and the final energy left in the node, at the end of the simulation run are measured. The percent energy consumed by a node is calculated as the energy consumed to the initial energy.

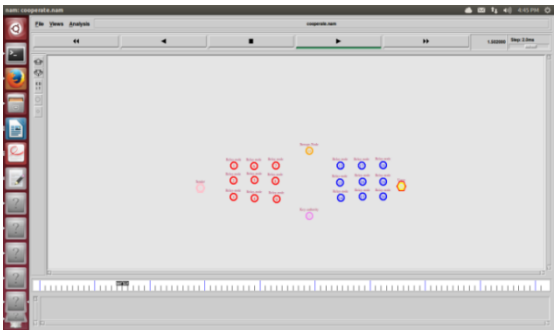
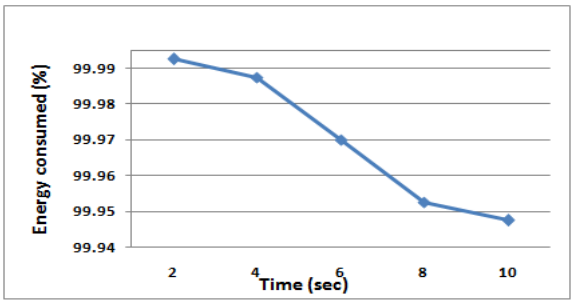
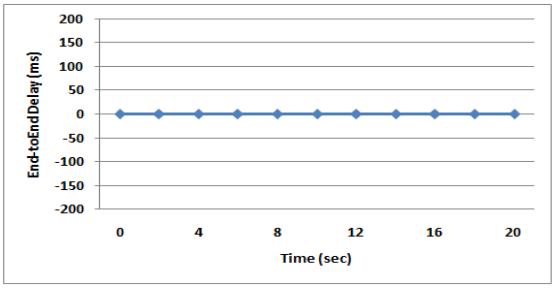


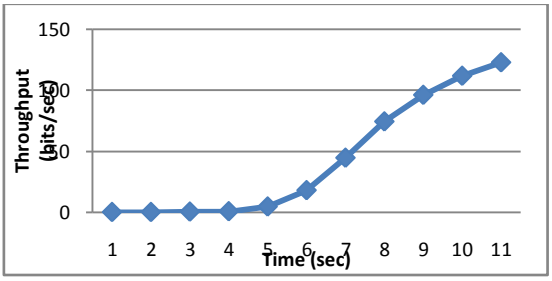
Figure 2: Nodes created to provide confidential data from sender to user



(a)



(b)



(c)

Figure 3: (a) Energy Consumption (b) End-to-End Delay (c) Throughput

And finally the percent energy consumed by all the nodes in a scenario is calculated as the average of their individual energy consumption of the nodes.

X. CONCLUSION

The CP-ABE scheme reduces the problem of KEY-ESCROW. It will be attracted a lot, because the attribute based encryption help a lot to improve the security of the data. The key escrow problem could be solved by random key issuing in multi-authorities in central authority center, which can issue keys randomly to user and keys will be constructed between key generation center and the data storing center. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.he version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained.

ACKNOWLEDGEMENT

Special thanks to **Prof. M. A. Lokhandwala** who helped me in this research and secondly i would like to thank my parents and friends who helped me a lot in finalizing this research within limited time frame.

REFERENCES

[1] Secure Data Retrieval for Decentralized Disruption Tolerant Military Networks. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM transactions on networking, vol. 22, no. 1, February 2014

[2] Attributes Union in CP-ABE algorithm for large universe cryptographic access control, Yong Cheng, Jiangchun Ren,

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Zhiying Wang, Songzhu Mei, Jie Zhou School of Computer Science and Technology, National University of Defense Technology Changsha, China Second International Conference on Cloud and Green Computing, IEEE 2012

[3] Ciphertext-Policy Attribute-Based Encryption, John Bethencourt, Amit Sahai, Brent Waters, IEEE Symposium on Security and Privacy(SP'07), 2007

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

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

[6] Delay and Disruption-Tolerant Networking (DTN): An alternative solution for future Satellite Networking applications. Carlo caini, Haitham Cruickshank, Stephen Farrell, and Mario Marchese, Proceeding of the IEEE/Vol.99, No. 11 November 2011

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

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

[9] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Medi-ated ciphertext-policy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

[10] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryp-tion," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[11] "The Pairing-Based Cryptography Library," Accessed Aug. 2010 [On-line]. Available: http://crypto.stanford.edu/pbc/

BIOGRAPHY

Hiral Patel is persuing the Masters of Engineering in Electronics and communication from Gujarat technological University in 2013-15 batch.