Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 4, April -2015

ESTABLISHING A TRUST AND SECURE DATA RETRIEVAL IN MILITARY NETWORKS

R.Yokeshwaran [1], Mr.R.Purushothaman [2]

[1] PG Scholar, M.E CSE (with specialization in computer networks), GKMCET, Chennai
[2] Assistant Professor, Department of CSE, GKMCET, Chennai

Abstract-*Networks in the military environment used mobile node for communication, which are then replaced by the storage nodes as the communication through the storage nodes are far more secure than the mobile nodes. Disruptions being an important challenge in the military environment, Disruption-Tolerant military networks are being used for the communication between the storage nodes. CP-ABE algorithm is used to encrypt the confidential information to overcome the authorization challenges in the storage node, where the decryption could be done when its access policy satisfies with the attribute key. The CP-ABE algorithm being implemented is semi-trusted, thus here we propose a CP-A^{2}BE scheme with additional user specific information to provide a trusted Disruption-Tolerant Military Network.*

Keywords-*Accountability, access control, cipher text policy attribute based encryption (CP-ABE), Disruption Tolerant Networks (DTN).*

I. INTRODUCTION

In battlefield or hostile environments many difficulties are occur while using wireless nodes in extreme military networks. Soldiers carried a connection of wireless devices that may be disconnected by jamming, environmental factors and mobility. Delay-/Disruption-Tolerant Networking is an overlay architecture intended to operate above the protocol stacks of the distinct ICNs and enable gateway functionality between them through the use of storage capacity, a variety of protocol techniques, replication and parallel forwarding, forward error correction and many other techniques for overcoming communication impairments. Mobile nodes in some challenging network scenarios suffer from intermittent connectivity and frequent partition e.g. battlefield and disaster recovery scenarios. In the above scenarios, an end-to-end path between a source and destination may not always exist where the links between intermediate nodes may be opportunistic, predictable connectivity or periodically connected. To allow nodes to communicate with each other in these extreme network environments recently research community has proposed a new architecture called the Disruption-Tolerant networks (DTN). The connectivity problem that are solved and successfully access information from mobile nodes over the disruption tolerant networks. At the same time due to the delay of confidential data that are accessing an unauthorized person or entrusted party in a networks. So avoid the vulnerabilities of secret data and we encrypt the secret data by using recent crypto algorithms to store the encrypted data in storage node. When unauthorized person access or compromise the information they will not access fully. Even though compromise the data then access denied because authority define the access control policy who owned the secret data then only appropriate user revealing the secret data.
In existing ABE schemes there is a one critical functionality missing which is key abuse problem. The key that shared an unauthorized person while accessing a confidential data or information. Attribute based encryption algorithm based access control system has semi trust and misbehavior of the semi trusted attribute authority including illegal key re-distribution. To the best of our knowledge, such key abuse problems exist in all current ABE schemes as the attribute private keys assigned to the users are never designed to be linked to any user specific information except the commonly shared user attributes. To avoid this key abuse problem by using **accountability of user information** that embedding in user's secret key. The accountability for user is achieved by embedding additional user specific information in the attribute private key issued to the user. To overcome the entrusted user shares his data to others.

II. CONTRIBUTION

In this paper, we define the different following achievements. It reduces by windows of vulnerability using immediate attribute revocation. Encrypt the confidential data as a cipher text if compromise without access. The proposed methodologies for CP-A^{2}BE algorithm define the access policy and set of attributes of who owned the confidential data. The data should encrypt to store storage node and when user want to decrypt the cipher text satisfy the access policy and specified attributes then only access or decrypt the cipher text using a secret key of users. The

accountability of user specific information that is embeds to the corresponding secret key to overcome the key abuse problem in military environments

A. Network architecture

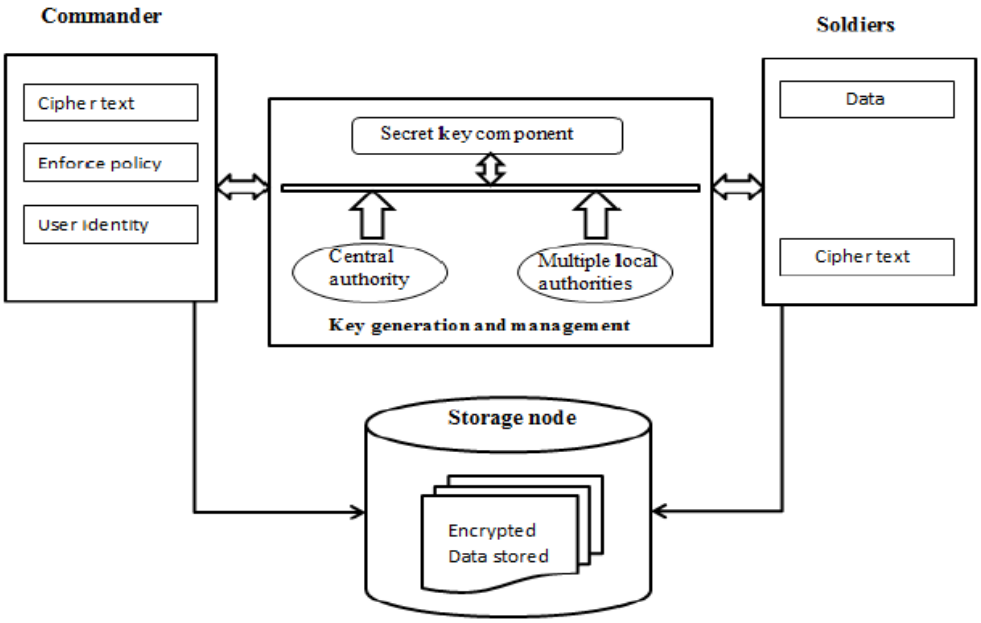

Figure 1. Architecture for proposed system

The overall architecture of the proposed system that shown figure 1, commander encrypt the secret data as a cipher text and enforce policy for who owned data. The secret data contain a secret key and identity of user or soldiers. The encrypted data that are send and store into the storage node by sender. In key generation phase have two authorities are there such as Central authority and multiple local authorities. The central authority generates a secret key and multiple local authorities define attributes for each user or soldiers. The attributes and access policy that are match then only the relevant user decrypt the cipher text by using secret key. Users want to retrieve the secret data that are accessing the request to send the secret data from the storage node. The user receives a secret data and decrypt by matching the access structure and attributes.

In encryption process, the secret data that are encrypt as a cipher text format and then the commander define the access policy enforcing corresponding secret data. The identity of the user data that are also embed to the secret data and it is used to find the dishonest user in the battlefield. Dishonest user means who sharing his secret key or attribute key to unauthorized members.

In key generation and management, the secret key components that contain the personalized key and attribute key for each user. The component of secret key that are generated by key authorities using arithmetic 2 party computation protocol. The protocol is used to avoid the coordination of two authorities and the master secret key that are not collude of two different authorities in key issuing phase. The secret key component sends to the commander and receives then enforcing a policy and encrypts identity of the user to store into storage node. In military network communication without any disruption to accessing secret key using technique such that disruption tolerant networks. It is used to store and forward when the end to end path does not exists. When the dishonest user sharing his secret key or decryption key that will identified by the user identity and avoid key abuse problem using accountability of user information.

In storage node, the encrypted data that are stored and when the user send the request to the storage node and send to the appropriate user in the networks. The attribute key those are hold or drop in the one region to another region while the key that invalid at the time of decryption of non-valid attribute key in another region. The key component of attributes that are update in the storage node by key authorities in key generation phase. Updated key that are send to the appropriate attribute group member in the region.

III. CP-A^ BE CONSTRUCTION

3.1. Setup

To generate system parameters, a trusted authority selects random generators g, g2, g3, u0, u1, . . ., un € G1, picks a random α € Zp, and sets g1 = g^{α}. He also defines a cryptographic hash function H: {0,1}* Z p. The system parameter is param = (g, g 1, g 2, g 3, u 0, u 1, · · ·, un, H), and the master secret key is g_2^{α}.

3.2. Key Gen

To issue an attribute private key for a user with identity ID and an attribute list L = [L1,L2, · · · , Ln], the attribute authority picks up a random r € Zp and computes (d0, d1)=(g_2^{α} (u_0^{ID} $u_1^{H(L1)}$ · · · $u_1^{H(Ln)}$ g3)^r, g^r) as the attribute private key. The validity of (d0, d1) can be verified through the following equation: $e^{\wedge}$(d0, g) = $e^{\wedge}$(g1, g2) $e^{\wedge}$(u_0^{ID} $u_1^{H(L1)}$ · · · $u_1^{H(Ln)}$ g3, d1). Finally, the user retains the decryption key $sk_{ID,L}$ = (d0, d1, d2, d3) on decryption device, where d2 = ID and d3 = L.

3.3. Enc

To encrypt a message M € G2 under cipher text-policy W = [W 1, W 2, · · ·, Wn], pick up a random value s € Zp and set C0 = M $e^{\wedge}$(g1, g2)^s, C1 = g^s, C2 = (πW_i ≠* $u_i^{H(Wi)}$ · g3)^s, Ti = {u_i^s} W_i =*, E = u_0^s. The cipher text for M on W is C = (C0, C1, C2, {Ti} W_i =*, E).

3.4. Dec

To decrypt the cipher text C = (C0, C1, C2, {Ti} W_i =*,E), the recipient with identity ID and attribute list L first checks W to know whether R(L,W) = 1. If R(L,W) = 1, he proceeds as follows: Let = $sk_{ID,L}$ (d0, d1, d2, d3) be the decryption key deposited in decryption device, where d2 = ID and d3 = L. He computes C0 2 = C2 πW_i =*, T $_i^{H(Li)}$ E^{d2} and decrypts with $sk_{ID,L}$ to get M = C0 $e^{\wedge}$(d1, C0 2)/ $e^{\wedge}$ (d0, C1).

3.5. Trace

Let $sk_{ID,L}$ = (d0, d1, d2, d3) be a valid decryption key in an illegal decryption device, where d3=[L1,L2, · · · , Ln]. It means that $e^{\wedge}$(d0, g) = $e^{\wedge}$(g2, g 1) $e^{\wedge}$(u_0^{ID} u $_1^{H(L1)}$ · · · $u_1^{H(Ln)}$ g3, d1). Then, just reveal d2 as the identity of the dishonest user who shares the decryption key.

IV. SYSTEM ENTITIES

4.1. Encryption Using CP-ABE

This describes how the confidential data that are encrypted by cipher text and define the access policy under attributes. When a sender (commander) wants to deliver its confidential data, he defines the access structure over the attributes and encrypts the data under access structure to enforce attribute-based access control on the data and stores it into the storage node.

4.2. Key Generation & Distribution Using Key Authorities

Key-Generation**:** The Key Gen(MK, PK, A) algorithm takes as input the master key values MK, the public parameters PK and the attribute set A of the user, and outputs for the user a set of decryption keys SK which confirms the users possession of all the attributes in A and no other external attribute.

The users ask for secret key to revealing a secret document and CA (Central Authority) asks for require document of user in key generation phase. CA verifies the user document and define the access structure of who owned data it contain set of attributes generated by multiple Local Authority (LA). The set of attributes and access policy satisfy then only user will reveal secret information from encrypted data from CA. CA takes as randomized algorithm to generate secret key of encrypted data and encryption file that contain the secret key of user and key contain access structure and set of attributes.

4.3. Decryption Process

This describes how the user (soldiers) decrypts the cipher text by using his secret key. The decryption process performs in a recursive way. Recursive algorithm denotes Decrypt *Node (CT, SK, and x)*.This takes as inputs a cipher text *CT*, a secret key *SK*, which is associated with set of attributes and node *x* from the tree.
The decryption algorithm **Dec** (CT, SK, and PK) takes as input the cipher text CT, the user secret keys SK and the public parameters PK, and it outputs the encrypted message M, if and only if the attributes A embedded in SK satisfy the access structure T which was used while Encrypting the cipher text CT. i.e. If T (A) = 1 then message M is output else, it outputs.

4.4. Managing Encrypted Data & Key Update In Storage Node

This describe the how manage confidential or encrypt data in storage node and how key update procedure progress. When a user comes to hold or drop an attribute, the corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively. The key update procedure is launched by sending a join or leave request for some attribute group from a user who wants to hold or drop the attribute to the corresponding authority. On receipt of the membership change request for some attribute groups, it notifies the storage node of the event. Without loss of generality, suppose there is any membership change in (e.g., a user comes to hold or drop an attribute at some time instance).

Key update: The key Update (SK, old attr, *PP*) algorithm define as input of user secret key and old attribute of previous region and parameters of CA. This input data use to generate the new value of attribute key of user. To check the particular secret key of user attributes to generate new key to update in storage node. Storage node keeps the updated attribute key of the users. When user attributes are satisfy with access structure of secret data while decrypt the secret data if only valid update key.

4.5. Embedding User Identity Using Identity Based Encryption

This describes the how user additional specific information that is embeds with secret key from key authority. Cipher text encrypt as a public parameter pp, identity ID, secret key SK construct as identity based encryption IBE Enc(pp;ID;SK) and One wants to encrypt a message to some identity ID. He also wants to ensure that the user can only decrypt if he not only has identity ID, but also satisfies some additional conditions. For example, the cipher text can be created for ID with additional attributes “Gen Op” and “technical dept.”. However, in traditional IBE, a message can only be encrypted to some user with ID, without other conditions. From the above scheme, such conditional IBE can be constructed as follows.
To encrypt a message M € G2 for identity ID with cipher text-policy W=[W1,W2,…,Wn], pick up a random value and the cipher text is C=(C0,C1,C2,{Ti} wi=*), the user with identity ID and attribute list L=[L1,L2,….,Ln] can check W to know whether R(L,W)=1. Decrypt the cipher text and his secret key (SK), L = (d0, d1).

Trace: The tracing algorithm denote as, L = (d0, d1, d2, d3) be a valid decryption key in an illegal decryption device, where d3=[L1,L2,….,Ln]. It means that $e^{\wedge}(d0, g) = e^{\wedge}(g2, g1)\ e^{\wedge}(u_0^{ID} u_1^{H(L1)} \cdots u_1^{H(Ln)}\ g3, d1)$. Then, just reveal d2 as the identity of the dishonest user who shares the decryption key.

V. CONCLUSION

It discussed the problem of key abuse existed in access control that is based on CP-ABE and semi-trusted of key authority and user in military networks. Considered the accountability for users and accountability for the semi-trusted attribute authority in network, It showed how to construct CP-ABE scheme such as key generation and distribution, how user satisfy the access structure and set of attributes, how encrypt a secret file and store in storage node, retrieve from storage node and decrypt by using a secret key in military networks. It remove key abuse problem in military networks and identify the dishonest user by embed user additional specific information corresponding to the user secret key. To establish a trust and securely data retrieve in military networks without any disruption over Disruption-Tolerant Networking.

VI. FUTURE WORK

It presents a future work for applying Disruption Tolerant Network in less reliability of storage data due to delay network connectivity in large commercial organization and more efficient access control technique applying to the decentralized systems.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang,"Secure Data Retrieval for Decentralized Disruption-Tolerant Military Network",IEEE/ACM Transaction in networking VOL. 22, NO. 1, February 2014.
[2] 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.
[3] Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrintArchive: Rep. 2010/351, 2010.
[4] M. Chuah and P. Yang, "Node density-based adaptive routing schemefor disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006.
[5] Jin Li, Kui Ren, and Kwangjo Kim "A2BE: Accountable Attribute-Based Encryptionfor Abuse Free Access Control"
[6] Nishant Doshi and Devas Jinwala "Updating attribute in CP-ABE: A New Approach A Survey of Delay- and Disruption-TolerantNetworking Applications",IEEE/ACM Transaction in networking Vol. 5, No. 1, June 2012
[7] Xiaohui Liang, Rongxing Lu, Xiaodong Lin, and Xiamen (Sherman) Shan "Ciphertext policy attribute based encryptionwith efficient revocation"
[8] J. Khabbaz, Chadi M. Assi, and Wissam F. Fawaz "Disruption-Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges "Maurice"
[9] Abel Joy, Akhila H, Annie Chacko"Survey of Management of PHR by Secure Cipher Text Policy Attribute Based Encryption Scheme", International Journal of Scientific & Technology Research Vol 3, Issue 4, APR 2014.
[10] Venkateshprasad, D.Haritha "CIPHER-Text Policy Attribute Based Access to Cloud", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014,
[11] Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Euro crypt*, 2005, pp.457–473.
[12] John Bethencourt, Amit Sahai and Brent Waters, "Cipher text policy attribute based encryption"
[13] DTN research group http://dtnrg.org.
[14] L.Wood, W.M. Burleigh "E-Book for DTN: Bundle problem" pg. 245-389.
[15] Abdul Shabbir, Anasuri Sunil Kumar (Jan2012) "An Efficient Authentication Protocol for Security in MANETs", IJCCT.
[16] AMSAT http://www.amsat.org.
[17] J.Jackson "Crypto analysis and security" pg.177-197.
[18] Mooi-Choo Chuah, Peng Yang, Brian D. Davison, Liang Cheng "Store-and-Forward Performance in a DTN"

