International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

Molkar Rajkumar
Assistant Professor, Department of Computer Science and Engineering, K G Reddy college of Engineering and Technology, Moinabad, Hyderabad, Telangana, India

ABSTRACT

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer fromm intermittent network connectivity and frequent partitions. Disruption-tolerant networks (DTN) technologies are developing to wind up best arrangements which permits the remote gadgets to be conveyed by the trooper keeping in mind the end goal to make correspondence with each other and access the data that are secret or orders are made solid by misusing the outside capacity hubs. There are the absolute most difficult issues exhibit in this situation, they are requirement of approval strategy and strategies that are refreshed for handling the information recovery in a safe way. Figure content arrangement quality based encryption (CPABE) is a huge answer for cryptography keeping in mind the end goal to get to the control issues. The issue of executing the CP-ABE is a de-concentrated DTNs causes numerous security and security challenges with respect to property renouncement key escrow, and co-ordinates of qualities given from various experts. In this paper, we propose a protected plan for recovery of information utilizing CP-ABE for de-incorporated DTNs where the experts of numerous key take care of their trait freely. We outline how to apply the proposed framework to deal with the private information with security and proficiency, appropriated in the Disruption-tolerant military systems.

Keywords: DTN, CP-ABE, Cipher Text, Attributes.

I. INTRODUCTION

In several military networks scenario, the soldiers may temporarily disconnected from the connection of wireless devices due to jamming, mobility and environmental factor, mainly when they access in hostile environments [1, 2]. Disruption-tolerant network (DTN) techniques are developing fruitful arrangement that grants the correspondence of for hubs inside them, which happens in the outrageous systems administration condition. At the point when the conclusion to-end association does not exist between a source and a goal match, the message from source to goal does not hold up in the middle of the road hubs for a considerable measure of time until the association is built up. DTN design is characterized as where various specialists offer and take care of their possess autonomous quality keys as de-unified DTN. ABE is a critical approach that fulfills their necessities for information recovery safely in DTNs. ABE highlights an instrument that birthplaces and access control over the encoded information utilizing achievement arrangement and credited traits on private and figure keys.

II. DISADVANTAGES

The issue of applying ABE to DTNs starting points numerous security and protection challenges. Since, the related trait might be changed by a few clients, at some client, sooner or later, or some private keys might be traded off, the key renouncement for each trait must be essential with a specific end goal to make the framework secure. This issue stays

significantly more troublesome for the most part in AES framework. Thus, every property is possibly shared by numerous clients.

III. PROBLEM DEFINITION

The issue definition characterizes that disavowal of any characteristic (or) single client in a property may offer the other client in the gathering. For instance, if a client is incorporated or isolated from the characteristic gathering, the key property must be changed over and re-dispersed to alternate individuals who are available in that same gathering for forward (or) in reverse mystery [3, 4] It brings about container neck amid rekeying method or debasement of security because of helplessness in windows, on the off chance that the past property key isn't refreshed all of a sudden.

IV. CHALLENGES

One of the most significant challenges is the key-escrow problem. In CP-ABE the private key of user is generated by key authority. This process takes place by applying the master secret key of authority to user's associated set of attributes. Thus every cipher text can be decrypted by the key authority. A potential threat to the data confidentiality or privacy for highly sensible data may happen, when the key authority is compromised by adversaries when deployed in the hostile environment. Indeed, even in the numerous expert frameworks the key escrow is a characteristic issue has the whole benefits keeping in mind the end goal to enable their own quality keys with their own lord privileged insights. Since such a instrument of key age relies upon single ace mystery is the general technique for some for a considerable lot of the hilter kilter encryption frameworks, for example, the identitybased or on the other hand the property based encryption conventions, erasing the escrow in a solitary (or) numerous expert, CP-ABE is a significant open problem.[5,6,7,8]. The last test is the coordination of traits given from various specialists. At the point when the numerous experts keep up and give credit keys to the clients autonomously with their own particular ace privileged insights, it is extremely hard to decide fine-grain get to strategies over the qualities issued from various experts. For illustration, if expert A deals with the traits "part 1" furthermore, "locale 1" and specialist B deals with the properties "part 2" and "locale 2". At that point, it isn't conceivable to deliver an entrance strategy (("part 1" OR "area 1") Also, ("part 2" OR "area 2") in the before plans since the OR rationale between characteristics given from different distinctive specialists can't be executed. This happens because of the way that the diverse experts create their own particular property keys utilizing their own free and individual ace mystery keys. Subsequently, get to strategy, for example, "out-of" rationale, can't be communicated in before plans.

V. EXISTING SYSTEM

5.1 Key-Policy attribute-Based Encryption (Kp- ABE)

In Kp-ABE, the encryption can only get to label a cipher text with set of attributes. The key authority selects a policy for every user that decides which cipher text he can decrypt and provide the key to every user by presenting the policy into the key of user [9,10,11].

5.2 Attribute Revocation

The arrangement is proposed so as to attach each characteristic a lapse date or time and give another set of keys to the clients who are thought to be legitimate after lapse.

5.3 Key Escrow

Numerous current ABE plans are based on the design where a solitary trusted specialist has the energy to give the entire private keys of client with its ace mystery data. Subsequently, the key escrow issue is innate such that the key specialist can be decoded and each figure content can be tended to to the clients in the framework by giving their mystery keys whenever [12,13,14]. A disseminated KP-ABE plot proposed will unravel the enter escrow issue in a multi specialist framework. In this approach, all

specialists of properties are participating in the key age convention in a dispersed way in such a route, to the point that, they can't pool their information and connection different credit sets having a place with a similar client.

5.4 De-Centralized Abe

A consolidated access arrangement over the characteristics given from different experts by just encoding the information numerous circumstances. The fundamental disadvantage of that method is the effectiveness and expressiveness of the entrance approach.

5.5 Disadvantages

The intermittent characteristic for ABE plans has two principle issues.

(I) The first and the premier one is the corruption of security regarding forward and in reverse mystery.

(ii) The following is the versatility issue. The key expert routinely passes on a key refresh material by unicast at inevitably space, with the goal that every one of the clients who are not denied can likewise refresh these keys. The single trait up-dation of circulates whole non-disavowed clients who may share the characteristic,

(iii) However, this arrangement will need in effectiveness execution.

(iv) Key Escrow framework needs high correspondence overhead on the framework set-up and furthermore the parts of rekeying stage other than the characteristic keys, where there is number of experts in the framework.

(v) Under the de-brought together ABE, the entrance rationale should just be AND, and they require activities of iterative encryption, where there is number of experts of traits. Here they are at any rate confined as far as access arrangement expressiveness what's more, require calculation and capacity cost.

VI. PROPOSED SYSTEM

(i) To propose an attribute based secure data for the transaction of data retrieval using digital signature.

(ii) (CP-ABE) is used for encryption and decryption.

(iii) Key-Issue Protocol generates and issues the secret key for user.

(iv) Key authorization is used for sharing the keys between the sender and the receiver.

(v) Digital Signature is used for Key Authorization.

(vi) In, the two PC protocol the key authority act as master secret for sharing information.

6.1 Advantages

There are three primary favorable circumstances of proposed work. They are,

(I) The above all else one is the prompt denial of trait that enhances the forward/in reverse mystery of secret information by bringing down the windows of weakness.

(ii) The second one is, scrambled can portray a finegrained get to approach by monotone access structure underneath traits given from any picked quality sets.

(iii) The third one is, the key Escrow issue which is dictated by a without escrow key giving convention that destructs the attributes of decentralized DTN design.

VII. RELATED WORK

ABE is comprised two flavors called key-policy ABE (KP-ABE) andmCipher text-policy ABE (CP-ABE)

7.1 Kp-Abe

In Kp-ABE, the encryption only obtains to label a cipher text along with set of attributes. The key authority selects a policy for each and every user that decides which cipher text that user can decrypt and provides the key to each user by enhancing the policy into user's key.

7.2 Cipher Text Policy Abe (Cp-Abe)

The encryption of figure content is done alongside an get to arrangement chose by an encyptor, however the key is ordinarily formed as for a trait set. The appointment of CP-ABE is more in DTNs than KPABE since it permits encyptors, for example,administrators to choose an entrance arrangement on the qualities and furthermore encodes classified information.

7.3 Attribute Revocation

Results that proposed to request to attach each trait a lapse date and issue another arrangement of key to the suitable substantial clients after the time of lapse. The trait of occasional revocable ABE process emerges of two principle issues. The principal issue is corruption of security regarding forward and in reverse mystery. The following is the adaptability issue. The key expert much of the time educates a key refresh material by unicast at each schedule opening and thus all non-disavowed clients can likewise refresh their keys. This impacts in the "I-influences "issue, which characterizes that the single characteristic updation will bother the whole non-denied clients who shared the characteristic. This may bring about blockage for both key-specialist and all the non-repudiated clients. The sudden key renouncement can by actualized by disavowing clients utilizing ABE that underpins negative conditions. So as to do it, one just incorporates conjunctively the ADD of nullification of renounced client identifiers. However, this outcome still flops in proficiency execution. This procedure will affectation slide assemble components aficionado to the extent of the private key over unique CP-ABE procedure of Bethen law court et al.; where there is most noteworthy size of repudiated characteristic set. Golle et al. likewise proposed a KP-ABE conspire which is client revocable, however this procedure will work just when the number of properties which is related with figure content is precisely a large portion of the span of the universe.

7.4 Key Escrow

Relatively a considerable lot of the current plans are based on the design where a solitary trusted specialist has the access keeping in mind the end goal to kick-begin the entire private keys of clients alongside its secret data. Consequently, the key escrow issue is inborn such that, by kick-beginning their mystery key whenever, the key specialist unscrambles each figure content routed to the clients display in the framework. Pursue et al, proposed a disseminated KP-ABE plot that uncovers the key escrow issue in a multi expert framework. In this plan, each property expert are participating in the key age convention in a appropriated way such that they can't gathering information and connection various ascribe sets which has a place with

a similar client. The principle disservice of this approach is the execution corruption. Since, the concentrated expert is absent in the ace mystery corruption, each quality expert should manage specialists introduce the framework with a specific end goal to create a clients' mysterykey. This keeps an eye on correspondence overhead on framework setup and rekeying stages parts additionally the trait keys, where the framework's number of specialists are available.

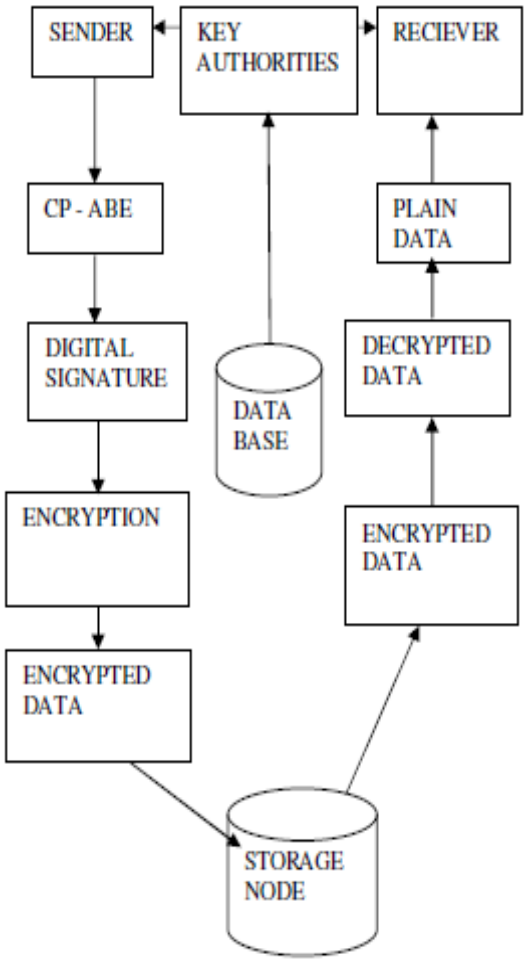

Fig 1. Architecture Diagram

7.5 Decentralized Abe

7.5 Decentralized Abe

Huang et al. furthermore, Roy et al. decided a decentralized CP-ABE conspire in multi expert system condition. They got a joined access arrangement over the characteristics given from different specialist by scrambling the information numerous number of times. The primary disadvantage of this plan is the effectiveness and expressiveness of access approach. For instance, when a secret mission is encoded by a leader to warrior under the arrangement, it can't by passed on, when each trait area is kept up by different specialist, since the various encoding approach can't be communicated by any broad. "Out-of-"rationales. For instance, let be the key experts, and be the traits stets they self-governingly achieve, separately. At that point the entrance approach which is communicated with is, can be controlled by scrambling the message with by, and after that encoding the ensuing figure content and after that scrambling the consequent figure content with by et cetera, this procedure goes ahead till multi encryption delivers the last figure content. Subsequently, the entrance rationale should just be AND, and they require iterative encryption tasks where the number of experts are available. In this way, marginally they are confined as far as expressiveness of the entrance strategy and need the cost of capacity and calculation. Despite the fact that, Pursue and Leweko et al. proposed a multi specialist KPABE what's more, CP-ABE plot, they will experience the key escrow issue.

VIII. CONCLUSION

The DTN strategies are developing to be the most successful arrangement in military applications that let the remote gadgets to communicate with each other and access the privately secure data reliably by abusing the outside capacity hubs. CP-ABE is an ascendable cryptographic answer for the entrance control what's more, recovery of secure information issues. In this paper, we proposed an efficient and secure information recovery technique utilizing CP-ABE for decentralized DTNs where the properties are self-governingly oversaw by different key experts. The trademark key escrow issue is resolved, with the end goal that the security of the put away information is ensured even in the threatening condition where the key experts might be bargained or untrusted. The renouncement for fine-grained key should likewise be possible for each property gather also. We illustrate how to apply the proposed framework so as to deal with the secret information conveyed in interruption resistance military system in a secured and effective way.

IX. REFERENCES

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

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

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

[4]. M. M. B. Tariq, M. Ammar, and E. Zequra, "Message ferry route de- sign for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37-48.

[5]. S.Royand,Chuah,"Secure data retrieval based on cipher text policy attribute-based encryption (CPABE)system for the DTNs," Lehigh CSE Tech. Rep.,2009.

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

[7]. A.LewkoandB.Waters,"Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

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

[9]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf.Comput.Commun.Security,2006,pp.89-98.

[10]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute- based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321-334.

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

[12]. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing withattributerevocation,"in Proc.ASIACCS,2010,pp.261-270.

[13]. A.Boldyreva,V.Goyal,andV.Kumar,"Identity-based encryption with efficient revocation,"in Proc.ACM Conf.Comput.Commun. Security, 2008, pp. 417-426.

[14]. RafaeliandD.Hutchison,"A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309-329, 2003

Mr.Molkar Rajkumar working as an Assistant Professor in Department of Computer Science and Engineering, KG Reddy college of Engineering and Technology, Moinabad, Hyderabad. He received the Master of Technology in ARYABHATA INSTITUTE OF TECHNOLOGY & SCIENCE- Jawaharlal Nehru Technological University, Hyderabad. He has 8+ years of teaching experience. His researches interests include Information security, Software testing, cloud computing, Data mining, Mobile Communication and Mobile ad-hoc networks.

Mr.Molkar Rajkumar working as an Assistant Professor in Department of Computer Science and Engineering, KG Reddy college of Engineering and Technology, Moinabad, Hyderabad. He received the Master of Technology in ARYABHATA INSTITUTE OF TECHNOLOGY & SCIENCE- Jawaharlal Nehru Technological University, Hyderabad. He studies Bachelor of technology in Nagarjuna Institute of Technology and Science. He studied diploma in Vemuganti Manohar Rao Polytechnic. He Studied till 10 class in Carmel Giri Convent High School, Devapur. His researches interests include Information security, Software testing, cloud computing, Data mining, Mobile Communication and Mobile ad-hoc networks