Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Multiple Attribute Based Encryption for Secret Key Generations in Disruption Tolerant Networks

N. Lakshmi Vasantha
P.G Student, Dept of CSE, Intell Engg College,
Affiliated to JNTUA University,
Andhra Pradesh, India

T. Venkata Naga Jayudu
Asst. Professor , CSE Dept, Intell Engg College,
Affiliated to JNTUA University,
Andhra Pradesh, India

Abstract: ***In military network conditions, links of wireless devices used by soldiers may be momentarily disconnected by environmental forces, mobility, jamming, particularly when they operate in aggressive environments. DTN (Disruption tolerant network) technologies are appropriate and unbeaten solutions that allocate nodes to communicate with each other in these tremendous networking environments. Usually, when there is no end to end link among a source pair and a destination pair, the messages from the source node may need to remain in the in between nodes for a considerable amount of time until the connection is eventually established. Using the two party computations, secret keys are issued on both sides but it needs extra computation cost as well. So in order to reduce the computation cost this paper will utilize another level of Attribute based encryption to the related work. Using this extra level there is no need to implement a two party computation rather two parties can use this ABE.***

Keywords: Encryption, Disruption Tolerant Military Networks, Attributes, Storage.

I. INTRODUCTION

In various armed forces method circumstances, interactions connected with remote control gadgets presented by means of reps may be in brief indifferent by means of sticking, ecological issues, and usefulness, particularly when these people operate in hostil conditions. Being interrupted tolerant method (DTN) advancements are generally addressing end up being worthwhile effects in which permit hubs for you to concur with 1yet another in these types of persuasive methods management circumstances [1]–[3]. Commonly, if you find simply no restriction to-end organization involving the resource as well as a terminus fit, the particular mail messages from your resource hub needs to manage down the middle of the road hubs for just a good measure of time till the organization would be ultimately guaranteed. Roy [4] and Chuah [5] introduced potential hubs in DTNs wherever information is usually put away or maybe copied in a way that simply just approved convenient hubs will get on the important files swiftly and properly. A lot of armed forces programs require expanded protection connected with private information which includes accessibility command routines that are cryptographically implemented [6], [7]. Mostly, it's elegant to give divided accessibility organizations in a way that information accessibility strategies are generally recognized more than buyer traits or maybe elements, that happen to be overseen through the important properties. Great example, in the disruption tolerant armed forces method, the commandant might keep categorized files at the stockpiling hub, which often must for being gotten to by means of elements of "Legion 1" who definitely are taking part in "District two. " For this scenario, this is a reasonable supposition that lots of important properties are generally at fault to manage his or her factor traits for a warrior into their delivered areas or maybe echelons, that may end up being most of the time altered (e. h., the particular property speaking with present section of going officers) [4], [8], [9]. All of us allude for this DTN structural architectural wherever various properties difficulty and handle his or her characteristic keys readily being a decentralized DTN [10].

The concept of attribute centered encryption (ABE) [11]–[14] can be a insuring approach that complies with the particular basics for safeguarded information recovery with DTNs. ABE qualities a musical instrument that allows a right to realize entry ways handle above scrambled information using access approaches and also ascribed characteristics amongst non-public recommendations and also ciphertexts. Specifically, Ciphertext-policy attribute-based encryption presents the flexible method for battling information such that the particular encryptor characterizes the particular attribute arranged which the decryptor needs to possess with a unique end goal for you to unscramble the particular ciphertext [13]. Thus, assorted customers usually are permitted for you to decode distinctive items of information for any the particular security design. difficulty regarding utilizing the particular ABE for you to DTNs reveals several security and also security challenges. Since several customers may perhaps transform the related characteristics sooner or later (for example, transferring the area), or even many non-public recommendations can be exchanged off, important repudiation (or redesign) for each a single attribute can be basic to create frameworks safeguarded. For the additional side, this challenge can be a lot more worrisome, particularly with ABE frameworks, due to the fact each one of these

characteristic can be maybe imparted by several customers (from now about, most of us allude for you to a real getting regarding customers being a excellent gathering). This kind of infers that renouncement regarding virtually any excellent or even virtually any single purchaser in a very attribute getting might have an effect on alternative customers inside the getting. Great example, if the purchaser ties together or even foliage an outstanding getting, the particular related attribute important ought to be modified and also redistributed towards the parts inside the similar getting for regressive or even forward puzzle. It may well produce bottleneck among rekeying process or even security file corruption due to house windows regarding powerlessness if the earlier house important isn't overhauled promptly. Different examination is the important escrow difficulty. In CP-ABE, the important thing Electric power produces non-public recommendations regarding customers through the use of the particular power's professional puzzle recommendations for you to consumers' related arranged regarding components. In this fashion, the important thing energy can easily decode each ciphertext maintained for you to unique customers by providing the characteristic recommendations. For the off possibility which the important energy can be exchanged off by predators as soon as submitted the particular antagonistic situations, this could be some sort of likely threat towards the information classifiedness or even security especially when the info can be exceptionally sensitive.

II. RELATED WORK

The previous technique recommended a capability centered protected files access structure using CP-ABE (Cipher text message insurance plan capability dependent encryption) with regard to decentralized Interruption Tolerant Sites. The previous technique possesses about three capabilities: the 1st an example may be the quick capability revocation improves forward/backward secrecy associated with classified files by minimizing the actual house windows associated with susceptibility. Minute an example may be the encrypters can identify a new fine-grained everyone insurance plan through any monotone admittance construction under attributes provided from any selected list of regulators. Last but not least, the important thing escrow trouble is usually rectified by a escrow-free critical problem project which exploits the actual characteristics from the decentralized Interruption Tolerant Sites architectural mastery. The main element making project problems user exclusive tips by calculating a new protected 2PC (two celebration computation) relating to the critical regulators having help of their very own get good at techniques.

The concept of Feature centered encryption (ABE) can be a making certain tactic that satisfies the actual specifications with regard to safe facts retrieval with DTNs. ABE characteristics something that encourages a right to obtain access manage in excess of scrambled facts utilizing access strategies and also added attributes amid personal secrets and also ciphertexts. The concern involving using the actual ABE to DTNs gifts a number of safety measures and also safeguard problems. Since a number of customers may transform the connected attributes faster as well as in the future (for instance, shifting the district), as well as many personal secrets could be exchanged away from, key repudiation (or redesign) per one characteristic is standard keeping in mind the final target to create frameworks safe. This particular infers that renouncement involving any kind of home as well as any kind of one client in a characteristic accumulating could affect alternative customers from the accumulating. Situation inpoint, if your client connects to as well as leaves a feature assemble, the actual connected characteristic key must be modified and also redistributed towards parts from the same accumulating with regard to retrograde as well as frontward secret. It may result in bottleneck among rekeying process as well as safety measures file corruption due to the house windows involving powerlessness in the event the previous characteristic key seriously isn't overhauled quickly.

Limitations

i) The situation involving using the particular ABE to DTNs gifts a number of protection and also protection problems. Because a few buyers may perhaps alter their own related qualities quicker as well as afterwards (for case, relocating their own area), as well as a few non-public secrets may be bargained, essential renouncement (or upgrade) for each 1 characteristic is fundamental having a unique end goal for making frameworks secure.

ii) On the other hand, this issue is a lot more troublesome, specially with ABE frameworks, since every feature is probably imparted through different buyers (hereafter, all of us allude to such a accumulating involving buyers being a excellent gathering)

iii) Another examination is the essential escrow matter. Inside CP-ABE,the important thing electric power produces non-public secrets involving buyers throughusing the particular power's pro mystery secrets to users'related group of qualities.

iv) One more examination is the coordination involving traits grantedthrough distinctive capabilities. In the level when a variety ofcapabilities oversee and also matter ascribes secrets to buyerswidely using pro mysteries, it can be complicated todefine fine-grained access agreements overtraits granted through distinctive capabilities.

III. PROPOSED WORK

Using the 2 party calculations, key tips tend to be granted upon equally facets nevertheless it requirements further calculation expense at the same time. Thus in order to reduce the calculation expense this suggested program may utilize one higher level of Feature dependent encryption towards active program. Employing this further amount there is no need to help implement any 2 party calculations instead 2 events incorporates the use of that ABE.

Figure 1: System Architecture

Functioning of the Architecture

Multi Authority CP-ABE: There're crucial age centers that creates open/mystery parameters regarding CP-ABE. The real key capabilities comprise of the focal strength and numerous community capabilities. All of us agree to that you have secured and dependable letters routes among the focal strength and each and every community strength among the particular starting up crucial build and age period. Each and every community strength runs different attributes and difficulties relevant credit tips in order to clientele. They offer differential entry legal rights in order to person clientele centered across the consumers' features. The real key capabilities are thought to be truthful even so inquisitive. That is certainly, they are going to seriously perform the particular allocated undertakings inside framework; nevertheless that they may want to discover information involving scrambled substance even so considerably while could fairly end up being estimated.

Storage Node: This can be a substance that merchant's info from senders and allow comparing entry to clientele. It could be convenient or perhaps static. Like the past options, many of us in addition expect the proportions switch to become semiassumed that is certainly fair still inquisitive.

Sender: That is an element whom statements private announcements or perhaps info (e. h., the commandant) and would like in order to retail store these individuals into your exterior info stockpiling switch regarding simpleness involving imparting or perhaps regarding dependable conveyance in order to clientele inside remarkable techniques administration predicaments. Some sort of sender manages characterizing (characteristic based) entry layout and authorizing all this by yourself info through scrambling the information underneath the approach previous to storing up the item in order to the particular stockpiling switch.

Receiver: This can be a flexible switch that should be able to the information place away at the stockpiling switch (e. h., the fighter). If perhaps a client possesses a few components rewarding the best to gain access strategy from the encoded info seen as a the particular sender, and it is not disavowed within from any of the qualities, then he may have the proportions in order to decode the particular ciphertext and have the information.

IV. ANALYSIS

The main aspect of this paper is to reduce the time taken to compute the keys regarding the file size, means while the size increases the computation of 2pc has to be reduced.

The below figure clearly depicts the time variations between the related work and the proposed work.

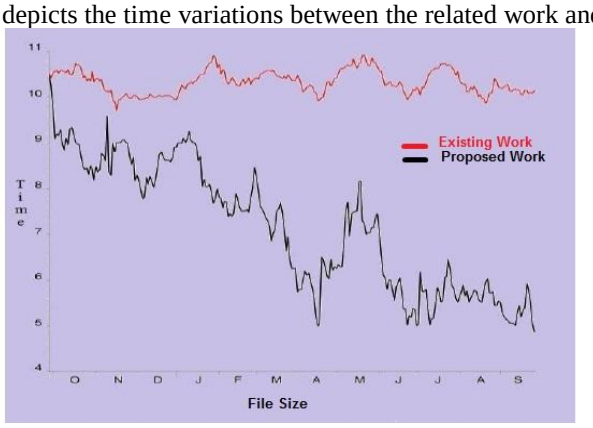

Figure 2: Time Comparison

As the figure above clearly depicts that the proposed work takes much less time as the file size keeps on increasing. It clearly explains that at initial it takes more time once the keys are computed then further it takes much lesser time.

V. CONCLUSION

With this Paper we all tend to deal with a risk-free facts collection theme victimization CP-ABE pertaining to suburbanized DTNs anywhere multiple essential government bodies manage his or her capabilities severally. We now have a tendency in order to incontestable ways to apply the particular planned device in order to strongly and with productivity manage the particular confidential facts dispersed inside the disruption-tolerant armed forces network. Disruption tolerant network (DTN) technologies have become flourishing solutions in which help wireless products taken simply by troopers in order to converse with each other in addition to admittance the particular breeze or even command consistently simply by discovering memory device nodes. most of the primary challenging difficulties during this circumstance rectangular measure the particular cultural manage connected with consent procedures in addition to meaning that the procedures bring up to date pertaining to risk-free facts collection. Ciphertext-policy attribute-based encoding (CP-ABE) is actually a offering cryptanalytic decision on the admittance administration difficulties. Nevertheless, the matter connected with making use of CP-ABE inside suburbanized DTNs presents numerous safety measures in addition to solitude issues using meaning the particular feature revocation, essential escrow, in addition to coordination connected with capabilities granted from completely different government bodies.

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] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309– 329,2003.

[3] T V Naga Jayudu and R Raja Sekhar, "D-LAROD: A Density Based LAROD for Geographical Routing in Intermittently Connected MANETs", in International Journal on Electronics and communication Technology (IJECT) in 2012.

[4] S. Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 1997, pp. 277–288.

[5] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in Proc. Symp. Identity Trust Internet, 2008,pp. 26–35.

[6] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE,"in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456– 465.

[7] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591.

[8] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in Proc. ASI ACCS, 2009, pp. 343–352.

[9] S. S. M. Chow, "Removing escrow from identity-based encryption," in Proc. PKC, 2009, LNCS 5443, pp. 256–276.

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

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"CryptologyePrint Archive: Rep. 2010/351, 2010.

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

[13] 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.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

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

[16] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

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

[18] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in *Proc. ACMConf. Comput. Commun. Security*, 2006, pp. 99–112.

[19] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *Comput. Surv.*, vol. 35, no. 3, pp. 309–329, 2003.

[20] S. Mittra, "Iolus: A framework for scalable secure multicasting," in *Proc. ACM SIGCOMM*, 1997, pp. 277–288.

[21] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in *Proc. Symp. Identity Trust Internet*, 2008, pp. 26–35.

[22] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

[23] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.

ABOUT THE AUTHORS

T. Venkata Naga Jayudu, received his **B.Tech** degree in computer science and information technology from Jawaharlal Nehru Technological University, Hyderabad, India, in 2005. **M.Tech** degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Ananthapur, India, in 2011. Currently **pursuing PhD** in computer science at Jawaharlal Nehru Technological University, Anantapur, India. His interesting research area is wireless sensor networks, Mobile Ad-Hoc Networks, Network Security and Operating Systems.

N.Vasantha Lakshmi received **B.Tech** degree in computer science and engineering from Srinivasa Ramanujan institute of technology, Anantapur, India, in 2013.Currently pursuing **M.Tech** in computer science and engineering at Intell engineering institute of technology, Anantapur, India.

