International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016

Available at http://internationaljournalofresearch.org

A Survey on: Secure Data Transfer in Disruption Tolerant Military Network

B V Ramakrishna [1]; G Pushpa Rajitha[2] & B Saritha[3]

[1]Associate professor, Dept. of CSE ST.Martin's Hyderabad,TS.

[2]Asst professor,Dept. of CSE ST.Martin's Hyderabad,TS

[3]Associate professor,Dept. of CSE ST.Martin's Hyderabad,TS.

Abstract

In the sizably voluminous number of outgrowing commercial environment each and everything depends on the other sources to transmit the data securely and maintain the data as well in the conventional medium. Portable nodes in military environments, for example, a front line or an antagonistic area are prone to experience the undergo of aberrant system network and frequent partitions. Disruption-tolerant network (DTN) innovations are getting to be fruitful results that sanction remote contrivance conveyed by officers to verbalize with one another and access the confidential data or secret data or summon dependably by abusing outside capacity nodes or storage nodes. Our project is not the unique one, but is an endeavor endeavor to have a precise scenario of what the terms "secure data retrieval for decentralized disruption tolerant network" is designated to be and its implementation as well on which we are currently working. As verbalized afore , our proposed system can enhance the security of military network by utilizing CP-ABE mechanism. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method utilizing CP-ABE for decentralized DTNs where multiple key ascendant entities manage their attributes independently.

Keywords: Interruption tolerant network (ITN); Ciphertext-policy attribute-based encryption (CP-ABE); Information Recovery

1. Introduction

In Numerous military system situations, sodalities of remote contrivances conveyed by officers may be briefly detached by sticking, ecological variables, and multifariousness, concretely when they work in hostil environments. Interruption tolerant system (DTN) advances are getting to be fruitful results that sanction hubs to correspond with one another in these compelling systems administration situations [1]–[3]. Mundanely, when there is no constraint to-end sodality between a source and a terminus match, the messages from the source hub may need to hold up in the middle of the road hubs for a munificent measure of time until the sodality would be in the cessation secured.

Roy [4] and Chuah [5] presented capacity hubs in DTNs where information is put away or duplicated such that just approved portable hubs can get to the essential data rapidly and efficaciously. Numerous military applications require expanded security of private information including access control routines that are cryptographically implemented [6], [7]. By and sizably voluminous, it is alluring to give dissevered access administrations such that information access approaches are characterized over client qualities or components, which are overseen by the key potencies. Case in point, in an interruption tolerant military system, a commandant may store relegated data at a stockpiling hub, which ought to be gotten to by components of "Legion 1" who are partaking in

"District 2." For this situation, it is a sensible supposition that numerous key powers are liable to deal with their element traits for warriors in their sentdistricts or echelons, which could be much of the time transmuted (e.g., the property verbalizing with current area of moving officers) [4], [8], [9]. We allude to this DTN structural engineering where sundry powers issue and deal with their trait keys liberatingly as a decentralized DTN [10]

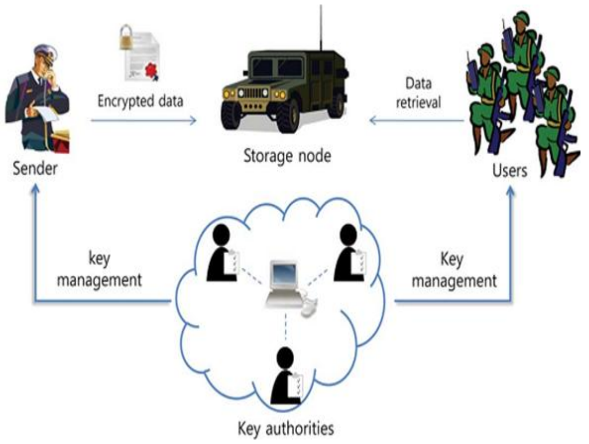


Fig 1: System Architecture.

The conception of characteristic predicated encryption (ABE) [11]–[14] is a assuring approach that gratifies the desiderata for secure information instauration in DTNs. ABE characteristics an instrument that empowers a right to gain ingression control over scrambled information utilizing access approaches and attributed qualities among private keys and ciphertexts. Especially, Ciphertext-policy attribute-predicated encryption gives an adaptable method for scrambling information such that the encrypt or characterizes the characteristic set that the decrypt or needs to have with a categorical end goal to unscramble the ciphertext [13]. Consequently, diverse clients are sanctioned to decode distinctive bits of information for every the security arrangement. On the other hand, theissue of applying the ABE to DTNs presents a few security and bulwark challenges. Since a few clients may transmute their cognate qualities eventually (for instance, moving their area), or some private keys may be traded off, key repudiation (or redesign) for each one characteristic is fundamental to make frameworks secure.

2. Related Work

2.1 Existing System:

The concept of attribute-predicated encryption (ABE) is a promising approach that consummates the requisites for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data utilizing access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are sanctioned to decrypt different pieces of data per the security policy.

2.2 Proposed System:

In this paper, we propose an attribute-predicated secure data retrieval scheme utilizing CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances rearward/forward secrecy of confidential data by reducing the windows of susceptibility. Second, encryptors can define a fine-grained access policy utilizing any monotone access structure under attributes issued from any culled set of ascendant entities. Third, the key escrow quandary is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol engenders and issues utilizer secret keys by performing a secure two-party computation (2PC) protocol among the key ascendant entities with their own master secrets. The 2PC protocol deters the key ascendant entities from obtaining any master secret information of each other such that none of them could engender the whole set of utilizer keys alone. Thus, users are not required to plenarily trust the ascendant entities in order to forfend their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key ascendant entities or data storage nodes in the proposed scheme.

Advantages:

- ✓ **Data confidentiality:** Unauthorized users who do not have enough credentials gratifying the access policy should be deterred from accessing the plain data in the storage node. In integration, unauthorized access from the storage node or key ascendant entities should be withal obviated.
- ✓ **Collusion-resistance:** If multiple users collude, they may be able to decrypt a ciphertext by cumulating their attributes even if each of the users cannot decrypt the ciphertext alone.
- ✓ **Rearward and forward Secrecy:** In the context of ABE, rearward secrecy denotes that any utilizer who comes to hold an attribute (that slakes the access policy) should be averted from accessing the plaintext of the antecedent data exchanged afore he holds the attribute. On the other hand, forward secrecy betokens that any utilizer who drops an attribute should be averted from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satiate the access policy.

3. Implementation

3.1 Key Mastery:

They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are 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 will honestly execute the assigned tasks in the system; however they would like to learn information of encrypted contents as much as possible.

3.2 Repository node:

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

3.3 Vendor:

This 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 (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

3.4 Customer:

This 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, then he will be able to decrypt the ciphertext and obtain the data.

4. Experimental Work

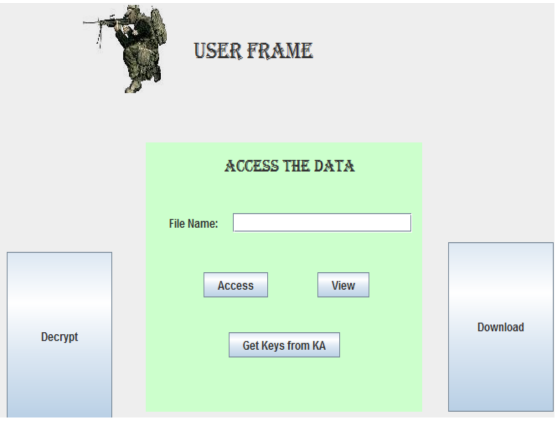
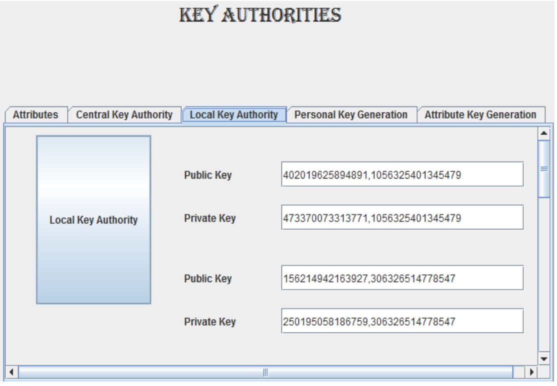


Fig 2: Customer Access Data Page.



Public Key 402019625894891,1056325401345479

Private Key 473370073313771,1056325401345479

Public Key 156214942163927,306326514778547

Private Key 250195058186759,306326514778547

Fig 3: Public and Private Key Generation.

5. Conclusion

We have proposed a novel approach which uses sound signature to recall graphical password click points. No antecedently developed system utilized this approach this system is subsidiary when utilizer is logging after a long time. In future systems other patterns may be utilized for recalling purport like touch of smells, study shows that these patterns are very utilizable in recalling the associated objects like images or text. In this paper, we proposed an efficient and secure data retrieval method utilizing CP-ABE for decentralized DTNs where multiple key ascendant entities manage their attributes independently. The intrinsical key escrow quandary is resolved such that the confidentiality of the stored data is ensured even under the bellicose environment where key ascendant entities might be compromised or not plenarily trusted. In additament, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

6. References

[1] Birget, J.C., D. Hong, and N. Memon. GraphicalPasswords Based on Robust Discretization. IEEE Trans.Info. Forensics and Security, 1(3), September 2006.

[2] Blonder, G.E. Graphical Passwords. United StatesPatent 5,559,961, 1996.

[3] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. ASecond Look at the Usability of Click-based GraphicalPasswords. ACM SOUPS, 2007.

[4] Cranor, L.F., S. Garfinkel. Security and Usability.O'Reilly Media, 2005.

[5] R. N. Shepard, "Recognition memory for words,sentences, and pictures," Journal of Verbal Learning andVerbal Behavior, vol. 6, pp. 156-163, 1967.

[6] A. Perrig and D. Song, "Hash Visualization: A NewTechnique to Improve Real-World Security," in Proceedingsof the 1999 International Workshop on CryptographicTechniques and E-Commerce, 1999.

[7] D. Weinshall and S. Kirkpatrick, "Passwords You'llNever Forget, but Can't Recall," in Proceedings of
Conference on Human Factors in Computing Systems(CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.