International Journal of Research
Available at http://internationaljournalofresearch.org/

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 01 Issue 09
October 2015

Secure Data Retrieval Schemes using CP-ABE for Decentralized DTNs

Nakkala Radhamma[1], Md.Asim[2]

[1]Student,Dr.K.V.Subba Reddy College of Engg for Women, Kurnool, Andhra Pradesh
[2]Asst.Professor, Dr.K.V.Subba Reddy College of Engg for Women, Kurnool, A.P

Abstract:

Compact centre points in certain circumstances, for instance, a forefront or a hostile region are obligated to experience the evil impacts of broken framework system and ceaseless bundles. Intrusion tolerant framework (DTN) progressions are getting the opportunity to be productive plans that allow remote contraptions passed on by troopers to talk using individually and give permission to private evidence or charge unfailingly abuse outside limit centre points. Irrefutably the most troublesome issues in this circumstance are the approval of endorsement methodologies and their courses of action redesign for secure data recuperation. Figure content methodology property gives encryption promise rejoinder to channel mechanism topics. Regardless, of topics to apply for CP-ABE in decentralized Intrusion tolerant framework (DTN) presents a couple security and insurance difficulties concerning the quality disavowal, fake, and direction of qualities allotted from unmistakable forces. We recommend an ensured data recuperation arrangement using the skill for distributed DTNs anywhere various key forces fare their dangers self-sufficiently. We provide security to the data that we have sent using distributed data. It is used in secure transmission of data for nations defence.

Keywords: *Attribute Based Encryption, disruption tolerant networking, information retrieval, performance evaluation .*

1. INTRODUCTION

With the advances in technology, we have many wireless computing devices e.g. PDAs, sensors etc. Such devices can form infrastructureless ad hoc networks and communicate with one another via the help of intermediate nodes. Such ad hoc networks are very useful in several scenarios e.g. battlefield operations, vehicular ad hoc networks and disaster response scenarios. Many ad hoc routing schemes have been designed for ad hoc networks but such routing schemes are not useful in some challenging network scenarios where thenodes have intermittent connectivity and suffer from frequent partitioning. Recently, disruption tolerant network technologies [1],[2] have been proposed to allow nodes to communicate with one another in such extreme networking environments. Several DTN routing schemes [3],[4],[5],[6] have been proposed. Although routing is an important design issue for such sparsely connected networks, the ability to access information rapidly is also an important feature that a DTN should have since the ultimate goal of having such a network is to allow mobile nodes to access information quickly and efficiently. For example, in a battlefield, soldiers need to access information related to detailed geographical maps, intelligence information about enemy locations, new commands from the general, weather information etc. In addition, a particular data item may be of interest to multiple soldiers, so it makes sense to replicate the data item, and store them at multiple nodes so that it can be accessed by other nodes. This allows us to save battery power, bandwidth consumption and the data item retrieval time. Such data caching also means that the source of the data items need not know the identities of the nodes that need to access the data items. Research on data access and dissemination techniques in ad hoc and sensor networks is not new. For example in [7], the authors consider the storage node placement problem aiming at minimizing the total energy cost for gathering data to the storage nodes and replying queries. In [8], the authors study the optimal number of replicas for a set of objects in large two-dimensional wireless mesh networks such that the access cost can be minimized. Their approach is not directly applicable to mobile networks since they assume stationary nodes in their environments. They also do not consider how a node can discover the replicas of the data items. In [9], the authors propose three distributed caching techniques for well-connected ad hoc networks, namely CacheData, CachePath and HybridCache. However, their techniques are only useful for well-connected ad hocnetworks.

Two key technologies enhance our ability to access information efficiently on the Internet [19]. The first is the indexing and search infrastructure e.g. Google's search engine that enables one to access

information by collecting and maintaining mappings of content to location. The second is a caching infrastructure that maintains a mapping from the content location to a cache location. These technologies, however, assume that the network devices are strongly connected to the Internet and hence are not tolerant to disruption. In addition, current technologies do not take into consideration that nodes move in some scenarios (e.g. mobile devices carried by human beings riding in vehicles). For a content-based information retrieval system to work in challenging network scenarios, data items need to be replicated and cached at different nodes. Questions like how many copies of each data item need to be replicated and which nodes should be selected to cache the replicated data items need to be answered. In addition, queries may need to be disseminated and cached by some intermediate nodes to increase the chances of them being answered in a timely manner. Again, the issue as to how a querying node selects other nodes to store its queries needs to be explored. In this paper, we design a content-based information retrieval system for disruption tolerant networks. Our design focuses on answering questions related to *data caching*, *query disseminations* and *message routing*. For data caching, we explore two data caching schemes, namely (i) *random caching*, and (b) *intelligent caching*. With *random caching*, each node generating a data item creates K tokens (representing K copies) and spread half of the tokens to the nodes that they first encounter. With *intelligent caching*, each node generating a data item only spreads the K tokens to carefully selected nodes that they encounter. The node selection is based on a friendliness metric: a node will be selected if it can meet many other nodes. The value for K can be fixed for all data items or varied depending on the access frequencies of each data item. For *query dissemination*, we explore two possible schemes, namely (a) *W-copy selective query spraying (WSS),* and (b) *L-hop neighborhood query spraying (LNS)*. In the *WSS* scheme, a querying node carefully selects W nodes based on a friendliness metric to cache replicated copies of the same query. In the *LNS* scheme, the querying node disseminates each query to its L-hop neighborhood. This is done by setting the TTL of its query message to L and any intermediate node that receives a query with a TTL more than one will rebroadcast the query after decrementing the TTL value. For *message routing*, we use an *enhanced Prophet* [3] scheme that only forwards messages to a next-hop node with an estimated delivery probability to the destination that exceeds a certain threshold. Other routing schemes can also be used.

2. RELATED WORK

ABE comes in two flavors called key-arrangement ABE (KP-ABE) and cipher text-strategy ABE (CP-ABE). In KP-ABE, the encryptor only gets the opportunity to mark a ciphertext with an arrangement of attributes. The key power picks a strategy for every client that determines which figure writings he can unscramble and issues the way to each user by implanting the approach into the client's key. However, the parts of the figure messages and keys are turned around in CP-ABE.

1) Characteristic Revocation: Bethencourt et al. [13] and numerous times. The primary detriments of this approach are effectiveness and expressiveness of access approach. The 2PC protocol deters the key powers from getting any expert secret information of one another such that none of them could generate the entire arrangement of client keys alone. Hence, clients are not required to completely believe the prevailing voices so as to ensure their data to be shared. The information classifiedness and security can be cryptographically enforced against any inquisitive key powers or data storage hubs in the proposed plan.

2) Key Escrow: Most of the existing ABE plans are constructed on the structural engineering where a solitary trusted power has the ability to create the entire private keys of clients with its ace mystery data. Consequently, the key escrow issue is intrinsic such that the key power can decrypt each cipher text tended to clients in the framework by generating their mystery keys whenever.

3) Distributed ABE: Huang et al. [9] and Roy et al. [4] proposed decentralized CP-ABE plots in the multiauthority system environment. They accomplished a consolidated access strategy over the traits issued from distinctive powers by just encoding information various times.

3. NETWORK ARCHITECTURE

In this section, we describe the DTN architecture and define the security model.

International Journal of Research
Available at http://internationaljournalofresearch.org/
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 01 Issue 09
October 2015

Figure. 1. Architecture of secure data retrieval using CP-ABE in a disruption-tolerant military network.

A composition overview is a grouping of substance that wants to review the segregating purposes of current learning and/or methodological approaches on a particular topic. For through examination of the system it needs to experience each and every specific piece of the related material all around. In this segment it delineates the outline of related progressions and abstract of related work done already.

Principally shared exactly at a floor level. We add to another cryptosystem for sharing of mixed data that we call KP-ABE. In our technique, figure compositions are named with crowds of qualities and in our permission of data minding which figure messages a customer has the limit translate. We demonstrate the instinctive nature of our improvement to allotment of survey log material and film encryption. Our improvement provisions assignment of secrets which subsumes HIBE. Decentralizing worth-Based Encryption [2] they propose a Multi-Authority Attribute-Based Encryption (ABE) structure.

In any case, in our structure each section will start from a perhaps particular force, where we acknowledge no coordination between such powers. We make new techniques to tie key sections together and check game plan attacks between customers with unmistakable overall identifiers. IBE with Effectual Reversal [3] Personality based encryption (IBE) is an empowering particular choice for open key encryption, as IBEC forgoes the prerequisite for a PKI. Any set, PKI- or identity based C must give an expects to repudiate customers from the structure.

Viable revocation is an all that much focused on C issue with the customary PKI setting. Nonetheless, in the setting of IBE, there has been little C wear down focusing on the dissent instruments. The most even minded plan requires the senders to furthermore use time periods when encoding, and all the beneficiaries (paying little personality to whether their keys have been exchanged off or not) to redesign their private keys reliably by coming to the trusted force. We observe that this plan does not scale well – as the amount of customers fabricates, the work on key overhauls transforms into a bottleneck. Message Ferry Route Design for Sparse Ad hoc Networks with Mobile Nodes [4] Message delivery is a frameworks organization standard where an unprecedented centre point, called a message boat, energizes the mix in a versatile uncommonly named framework where the centres are sparsely passed on. One of the key challenges under this perfect model is the layout of boat courses to fulfil certain properties of end to-end system, for instance, concede and message adversity among the centre points in the exceptionally named framework. This is a troublesome issue when the centre points in the framework move subjectively. As we can't make sure of the territory of the centres, we can't arrange a course where the boat can con act the centre points with affirmation.

In view of this inconvenience, prior work has either considered ship course layout for extraordinarily selected frameworks where the centre points are stationary, or where the centres and the boat move expert successfully to meet at particular regions. Such systems either oblige long-range radio or aggravate centre points' compactness outlines which can be coordinated by non-correspondence endeavours. Point convenience model. Each time that the boat explores this course, it contacts each adaptable centre with a certain base probability.

A. Architecture Description

Figure.1 shows the architecture of the DTN. As shown in Figure. 1, the architecture consists of the following system entities.

1) Key Authorities: They are key era focuses that generate public/mystery parameters for CP-ABE. The key authorities consist of a focal power and numerous local authorities. We accept that there are secure and reliable communication channels between

2) Storage node: This is an element that stores information from senders and give relating access to clients. It might be versatile or static [4], [5].

3) Sender: This is a substance that possesses private messages or information (e.g., a commandant) and wishes to store them into the outside information stockpiling hub for simplicity of sharing or for solid conveyance to clients in the compelling systems administration situations. A sender is in charge of characterizing (property based) access approach and authorizing it all alone information by scrambling the

information under the arrangement before putting away it to the capacity hub.
4) User: This is a portable hub that needs to get to the information put away at the capacity hub (e.g., a trooper). In the event that a client has an arrangement of qualities fulfilling the entrance strategy of the scrambled information characterized by the sender, and is not repudiated in any of the properties, then he will have the capacity to unscramble the cipher-text.

B. Threat Model and Security Requirements

1) Data privacy: Unauthorized clients who don't have enough qualifications fulfilling the entrance approach ought to be dissuaded from getting to the plain information in the capacity hub. Furthermore, unapproved access from the capacity hub or key powers ought to be likewise averted.
2) Agreement resistance: If different clients plot, they possibly ready to unscramble a cipher-text by consolidating their attribute seven if each of the clients can't decode the cipher-text alone [11]–[13]. For instance, assume there exist a client with properties {"Battalion 1", "District 1"} and another client with qualities {"Battalion 2", "Area 2"}. They may succeed in decoding a cipher-text scrambled under the entrance arrangement of ("Battalion 1" AND "Area 2"), regardless of the possibility that each of them can't unscramble it independently. We don't need these colluders to have the capacity to unscramble the mystery data by joining their traits. We additionally consider agreement assault among inquisitive neighborhood powers to determine clients' key.
3) Backward and forward Secrecy: In the setting of ABE, in reverse mystery implies that any client who comes to hold a trait (that fulfills the entrance arrangement) ought to be kept from getting to the plaintext of the past information traded before he holds the characteristic. Then again, forward mystery implies that any client who drops a characteristic should be kept from getting to the plaintext of the resulting information traded after he drops the trait, unless the other substantial properties that he is holding fulfill the entrance strategy.

3. PROPOSED SCHEME

In this section, we provide a multiauthority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Bethencourt *et al.* [13], dozens of CP-ABE schemes have been proposed [7], [15]–[16].
The subsequent CP-ABE schemes are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to achieve the expressiveness of the Bethencourt *et al.*'s scheme, which described an efficient system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic formula over attributes. Therefore, in this section, we develop a variation of the CP-ABE algorithm partially based on (but not limited to) Bethencourt et al.'s construction in order to enhance the expressiveness of the access control policy instead of building a new CP-ABE scheme from scratch.

A. ANALYSIS

In this segment, we first examine and think about the proficiency of the proposed plan to the past multi authority CP-ABE conspires in hypothetical perspective. At that point, the productivity of the proposed plan is shown in the system reenactment regarding the correspondence cost. We additionally talk about its productivity when actualized with particular parameters and contrast these outcomes with those acquired by alternate plans.

B. EFFICIENCY

In the authority architecture, logic expressiveness of access structure that can be defined under different disjoint sets of attributes (managed by different authorities), key escrow, and revocation granularity of each CP-ABE scheme. In the proposed scheme, the logic can be very expressive as in the single authority system like BSW [13] such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [9] and RC [4] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, attributes of users can be revoked at any time even before the expiration time that might be set.

C. SIMULATION

In this reproduction, we consider DTN applications utilizing the Internet secured by the quality based encryption.
Almeroth and Anmar [3] exhibited the gathering conduct in the Internet's multicast spine system (MBone). They demonstrated that the quantity of

clients joining a gathering takes after a Poisson distribution with rate, and the enrollment length of time takes after an exponential conveyance with a mean span. Since every quality gathering can be indicated as a free system multicast bunch where the individuals from the gathering share a typical characteristic, we demonstrate the reenactment result taking after this probabilistic conduct circulation [17].We assume that client join and leave occasions are independently and indistinguishably dispersed in every trait bunch following. Poisson dissemination. The enrollment span time for an attribute is expected to take after an exponential dispersion. We set the inter-arrival time between clients as 20 min and the normal participation term time as 20 h. Figure. 2 speaks to the quantity of current clients and renounced clients in a characteristic gathering.

D. IMPLEMENTATION

Next, we analyze and measure the computation cost for encrypting (by a sender) and decrypting (by a user) a data. We used a Type-A curve (in the pairing-based cryptography (PBC) library [3]) providing groups in which a bilinear map is defined. It shows the computational time results. For each operation, we include benchmark timing. Each cryptographic operation was implemented using the PBC library ver. 0.4.18 [3] on a 3.0-GHz processor PC. The public key parameters were selected to provide 80-bit security level. The implementation uses a 160-bit elliptic curve group based on the super singular curve over a 512-bit finite field. The comparatively negligible hash, symmetric key, and multiplication operations in the group are ignored in the time result. In this analysis, we assume that the access tree in the ciphertext is a complete binary tree.

4. CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. 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 using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, 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.

5. REFERENCES

[1] 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.

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

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.

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

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

[6] 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.

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

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

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

[10] 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.