International Journal of Engineering in Advanced Research Science and Technology

VOLUME-3
ISSUE-1

Secure Data Transmission in DTNs for Key Escow Process

K.Siddartha[1] , S. Sailaja[2]

[1]Mtech Student ,Department of C.S.E, RISE Krishan Sai Gandhi Group Of Institutions, JNTU-K,Valluru,ONGOLE,
[2]Associate Professor,Department of C.S.E, RISE Krishan Sai Gandhi Group Of Institutions, JNTU-K,Valluru,ONGOLE

Abstract: Military faces a number of challenges in handling classified and unclassified information. Major challenges include the money, time and effort it takes to develop and deploy new devices or networks and finally integrating them with the existing infrastructure cohesively currently in use and not readily replaceable. To meet military needs for securing data storage with respect to the new state of the art Disruption-tolerant network's (DTN) that allows DTN nodes carried by soldiers to communicate with each other and access and share private information even in the event of network delays. But security breach is a major concern in such DTN's. Although an attribute based encryption scheme is found viable in such store and forward networks, the latency issues with respect to key generation and maintenance is quite complex when using the traditional list based structures. So we propose a new optimized solution to improve to attribute extraction process of data and sort, revalidate and formulate a key generation process that can reduce the latencies involved and store and forwarding process of DTN's [4]. A real time network application developed in this regard highlights our proposed claim and its efficiency.

Index Terms: Secure Data Retrieval, Disruption-tolerant network's, multiauthority, Q-Tree, Multi-Attribute Based Range Query.

INTRODUCTION

Some of army system circumstances, relationships of wireless devices taken by army may be momentarily disconnected by performing, ecological aspects, and flexibility, especially when they function in aggressive surroundings. Disruption- tolerant system (DTN) technological innovation is becoming successful solutions that allow nodes to connect with each other in these excessive social media surroundings [3]. Generally, when there is no end-to-end relationship between a source and a place couple, the information from the resource node may need to delay in the advanced nodes for a significant amount of time until the relationship would be gradually recognized. Many army programs need improved protection of personal information such as accessibility management methods that are cryptographically required. In many situations, it is suitable to offer classified accessibility solutions such that data accessibility guidelines are described over customer features or positions, which are handled by the key regulators.

Copyright @ 2015 IJEARST. All rights reserved.

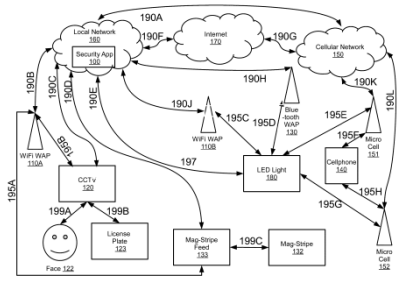

Figure 1: System process for developing security in DTNs.

For example, in a disruption-tolerant army system, a leader may shop a personal information at a storage space node, which should be utilized by associates of "Battalion 1" who are taking part in "Region 2." As show in above figure. In this case, it is a affordable supposition that several key regulators are likely to handle their own powerful features for army in their implemented areas or echelons, which could be regularly modified (e.g., the feature comprising present place of shifting soldiers).

However, the problem of implementing the ABE to DTNs introduces several security and comfort difficulties [4][5]. Since some users may modify their associated features at some point (for example, moving their region), or some personal important aspects might be compromised, key cancellation (or update) for each feature is necessary to help make techniques protected. However, this issue is even more challenging, especially in ABE techniques, since each attribute is possibly distributed by several customers (henceforth, we refer to such a selection of customers as an feature group).

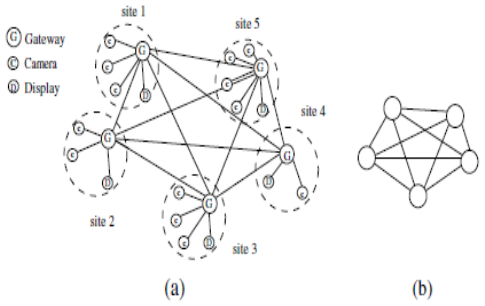

Figure 2: Tele-immersive atmosphere. (a) Tele immersive setup (b) Corresponding Overlay.

This implies that cancellation of any feature or any individual customer in an attribute team would impact the other customers in the team. For example, if a customer connects or results in an feature team, the associated attribute key should be modified and reassigned to all the other members in the same team for in reverse or ahead secrecy. It may outcome in bottleneck during rekeying process, or security degradation due to the ms windows of weaknesses if the previous attribute key is not modified instantly.

As shown in fig 2, with the improve in their range with regards to variety of gadgets and elements linked at each website, it has become really hard to deal with and observe the whole TI program from only one management point. Queries in such techniques are not like the conventional data source concerns with only one key value, instead they are given in a advanced level information which are modified into multi-attribute blend variety concerns. Some of the consist of "which website is extremely congested?", "which elements are not working properly?" etc. To response the first one, the question is modified into a multi-attribute blend variety question with constrains (range of values) on CPU usage, storage expense, flow amount, data transfer usage, wait and bundle loss amount [8]. The later one can be

Copyright @ 2015 IJEARST. All rights reserved.

responded to by building a multi-attribute variety question with constrains on fixed and powerful features of those elements. Queries can also be made by interpreting different multi-attribute varies clearly.

We recommend Q-Tree, a multi-attribute variety based question remedy considering all these specifications. One of the important qualities of our strategy is that it inserts only one question to the overlay for any dimension blend multi-attribute concerns without any pre-processing and still guarantees the maximum variety of node traversal. It can handle significant amount of feature turn in the TI program and also machines with the variety of information products. Our strategy is a new P2P variety index structure. It provides actual solutions to variety and aggregated queries (MAX, MIN, COUNT, AVG, SUM) by in-network gathering or amassing and performs for several information products using only one overlay framework.

I. RELATED WORK

ABE comes in two tastes known as key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to brand a cipher written text with a set of features [10]. The key energy selects a cover each customer that decides which cipher texts he can decrypt and problems the key to each customer by embedding the plan into the user's key. However, the positions of the cipher text messages and important factors are changed in CP-ABE.

In CP-ABE, the cipher written text is secured with an accessibility plan selected by an encryptor, but a key is basically designed with regard to an features set. CP-ABE is more appropriate to DTNs than KP-ABE because it allows encryptions such as a leader to select an accessibility plan on features and to secure private details under the accessibility framework via encrypting with the corresponding community important factors or features.

The immediate key cancellation can be done by revoking customers using ABE that facilitates adverse conditions. To do so, one just contributes conjunctively the AND of negation of suspended customer details (where each is regarded as an feature here). However, this remedy still somewhat does not have efficiency performance. This plan will cause expense team elements1 additively to the dimension the cipher written text and multiplicatively to the dimension personal key over the unique CP-ABE plan of Bethencourt et al, where the highest possible dimension is suspended features set . Golle et al. also proposed a customer revocable KP-ABE plan, but their plan only performs when the variety of features associated with a cipher written text is exactly 50 percent of the galaxy dimension.

Key Escrow: Most of the current ABE techniques are constructed on the framework where only one reliable energy has the energy to produce the whole personal important factors of customers with its master key details. Thus, the key escrow issue is natural such that the key energy can decrypt every cipher written text resolved to customers in the program by producing their key important factors whenever you want.

Decentralized ABE: Huang et al. and Roy et al. suggested decentralized CP-ABE techniques in the multi authority system atmosphere. They obtained a mixed accessibility plan over the features released from different regulators by basically encrypting information many periods [11]. The

Copyright @ 2015 IJEARST. All rights reserved.

primary drawbacks of this strategy are performance and expressiveness of accessibility plan. For example, when a leader encrypts a key mission to military under the plan ("Battalion 1" AND ("Region 2" OR 'Region 3")), it cannot be indicated when each "Region" feature is handled by different regulators, since basically multiple encrypting techniques can certainly not show any common " -out-of- " logics (e.g., OR, that is 1-out-of-).

II. DTN ARCHITECTURE

In this area, we explain the DTN structure and determine the protection design. Fig. 3 reveals the structure of the DTN. As proven in Fig. 3, the structure includes the following program organizations.

1) Key Authorities: They are key creation facilities that generate public/secret factors for CP-ABE. The key authorities consist of a main power and several local authorities. We believe that there are protected and reliable communication programs between a main power and each regional power during the preliminary key installation and generation phase [6]. Each regional power controls different attributes and problems corresponding feature important factors to customers. They allow differential accessibility privileges to personal users based on the users' features. The key regulators are assumed to be honest-but-curious. That is, they will honestly execute the allocated projects in the program, however they would like to understand details of secured material as much as possible.

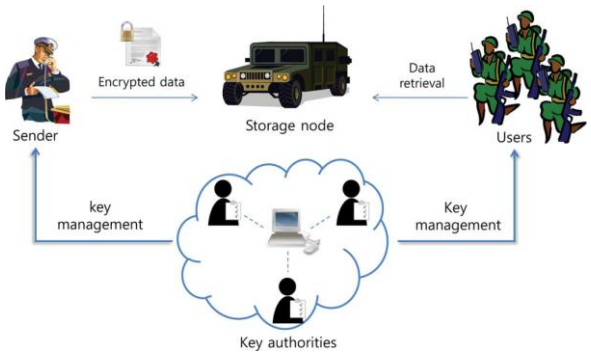

Figure 3: Architecture of secure data retrieval in a disruption-tolerant military network.

2) Storage space node: This is an enterprise that shops details from senders and offer corresponding accessibility customers. It may be mobile or fixed. Just like the past techniques, we also believe the storage node to be semi-trusted that is honest-but-curious.

3) Sender: This is an enterprise who operates private messages or details (e.g., a commander) and desires to shop them into the exterior details storage node for convenience of discussing or for reliable distribution to customers in the excessive social media surroundings. An emailer is accountable for interpreting (attribute based) access plan and implementing it on its own details by encrypting the details under the plan before saving it to the storage node.

4) User: This is a cellular node who wants to accessibility the data stored at the storage node (e.g., a soldier) [9]. If a customer possesses a set of features fulfilling the accessibility plan of the encrypted details described by the remailer, and is not revoked in any of the features, then he will be able to decrypt the cipher written text and acquire the details.

Since the key regulators are semi-trusted, they should be deterred from obtaining plaintext of the details in the storage node; meanwhile, they should

Copyright @ 2015 IJEARST. All rights reserved.

be still able to problem key important factors to customers. In purchase to recognize this somewhat contrary need, the central power and the regional regulators take part in the arithmetic 2PC method with expert key important factors of their own and issue separate key elements to customers during the key issuing phase [11]. The 2PC method stops them from knowing each other's expert tricks so that none of them can generate the whole set of key important factors of customers independently. Thus, we take an supposition that the main power does not collude with the regional regulators (otherwise, they can think the key keys of every customer by discussing their expert secrets).

III. MULTI-ATTRIBUTE BASED QUERY PROCESSING

Q-Tree intends to offer a multi-attribute centered query solution for hierarchically grouped surroundings. In this section, we first determine the program style effectively. Then, we existing the program framework of Q-Tree along with its metadata style.

System Model

We style our program style considering the TI interactive systems. There is a set of websites where multi-media and computing gadgets are linked with a entrance at each website. Gateway keeps details of regional gadgets as well as other system features of the regional nodes. Each Gateway can contact other gateways across websites, and so we signify each site by its entrance in the overlay1, as proven in figure 1 [12]. One realistic example of TI program is TEEVE (Tele immersive Environment for Everyone). It makes TI 3D multi-camera space surroundings both regionally and slightly. These kinds of atmosphere signify a next creation of TI where the greatest objective is to provide the wider viewers a 3D tele-immersive encounter over their available computing and interaction facilities.

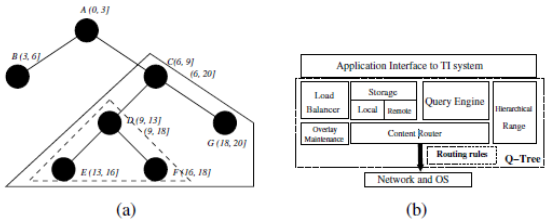

Figure 4: (a) Example (b) Q-Tree system architecture.

The program has very little turn and failing is fairly limited which can be immediately managed by the system administrator. Two kinds of details features are usually found in TI system: fixed and powerful. Static features (such as static digital parameters) do stay pretty the same over an whole TI period, whereas powerful details features (such as frame rate, end-to-end wait, CPU usage, bandwidth etc.) changes regularly [9]. Any irrelevant website may initiate a question either offering a advanced stage details of the query or clearly interpreting any mixture of (attribute, value/range) couple. The actual need of offering concerns is to retrieve data products from nodes. Q-Tree arranges gateways in an overlay shrub framework and designates varies to nodes in some framework. Data products are published into the overlay to be saved slightly in some other nodes according to the value. When a question is created for products specifying the range for certain features from any irrelevant node, a distributed search is started across the overlay.

Copyright @ 2015 IJEARST. All rights reserved.

```
Input: x: Node to which assignment is being made;
a: Attribute;
l, h: real numbers, range bound,
Δa(x) ← (l, h];
δa(x) ← (l, l + 1
N];
l ← l + 1N ;
for all c in C(x) do
nc ← c.size; /* size of the subtree at child c */
h ← l + nc/N ;
Assign Range(a, l, h);
l ← h;
end for
```

Algorithm 1: Assign range Query processing in nodes secure arrangement.

Algorithm 1 reveals how varies are allocated to nodes. The task is started by the main by invoking Assign- Range root(0.0, 1.0). Then, personal node designates variety to itself and to nodes in its sub trees, just like a preorder traversal of the shrub. We believed that all principles within the whole range (0.0, 1.0] of an feature are similarly likely. So, each node gets a self-range of equivalent dimension $|f\hat{A}a(x)| = 1$ N for each feature. This guarantees that each node shops nearly the same amount of information products. But if it happens that certain feature follows some submission other than consistent, the variety should be partitioned based on that submission operate (if known before-hand). For any given submission operate Fa(v) for an feature a, we need each node to get the equivalent number of information products to shop, that is P{v □ , $f\hat{A}a(x)$} = 1/N .

IV. SIMULATION RESULTS

In this area, we first evaluate and evaluate the performance of the suggested plan to the past multi-authority CP-ABE schemes in theoretical factors. Then, the performance of the proposed plan is confirmed in the system simulator in terms of the interaction cost [13]. We also talk about its efficiency when applied with particular factors and evaluate these results to those acquired by the other techniques.

We consider DTN programs using the Internet secured by the attribute-based security. Almeroth and Anmar confirmed the team actions in the Internet's multicast central source system (MBone). They revealed that the number of customers becoming a member of a team follows a Poisson submission with rate , and the account length time follows an exponential submission with a mean length . Since each attribute team can be proven as an separate system multicast group where the associates of the team discuss a common feature, we display the simulator outcome following this probabilistic actions submission. We assume that customer be a part of and keep activities are independently and in the same way allocated in each feature team following Poisson submission. The account length here we are at an feature is believed to adhere to an rapid submission.

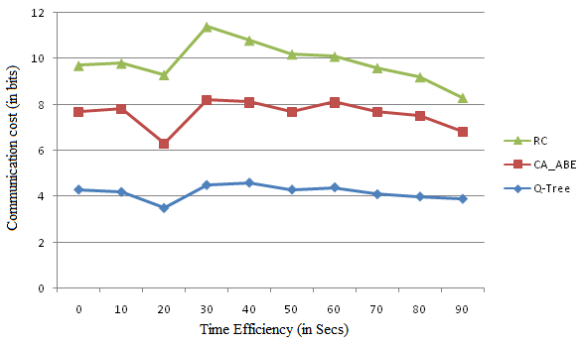

Figure 5: Communication cost in the multi authority CP-ABE systems with respect q-tree.

We imitate Q-Tree in an copied system installation on top of a unique system occasion simulation created in Coffee. We replicate a 'virtual' system with node-to-node latencies obtained from 4 time Planet Lab records which includes 250 unique nodes. This track gives us the connectivity

Copyright @ 2015 IJEARST. All rights reserved.

information and rtt setbacks among the nodes. We use this information to imitate question aircraft for TI techniques. As an overlay option, we consider MST and k-MST (degree bounded MST) [11]. The purpose behind this is that we always want to develop a latency-optimal shrub, though our solution would perform for any other shrub development techniques.

We are enthusiastic about mainly three efficiency metrics: query latency, interaction price, and overhead in meta-data servicing. We consider concerns of three kinds, namely equal-to (EQ), multi-attribute blend range queries (R), and multi-attribute multicast concerns (M). EQ represents question specified by an 'attr = value', for example 'cameras with frame rate=20', R identifies boundaries on attribute values, such as 'cameras with framerate between (10, 15) and obtain > 100'. Variety concerns (for both fixed and dynamic attributes) may also additionally be with any of the total features like MIN, MAX, COUNT, SUM and AVG, for example 'what is the MAX framerate in current TI session?'. For each run, we develop the overlay by taking nodes arbitrarily from the records and imitate the same event for 100 circumstances and take their regular. Unless mentioned, each site has 10 gadgets and each system has 10 features. To evaluate the efficiency of fill controlling criteria, we place information products via a right manipulated distribution (beta(4,2)) for 100 nodes in the program.

V. CONCLUSION

DTN technological innovation are becoming effective alternatives in military applications that allow wi-fi gadgets to communicate with each other and accessibility the private information reliably by taking advantage of exterior storage space nodes. The natural key escrow problem is settled such that the privacy of the saved information is assured even under the aggressive atmosphere where key regulators might be compromised or not completely reliable. We have developed and analyzed Q-Tree, a multi-attribute question structure for querying powerful TI techniques. Our efficiency results show that our program machines with the number of local gadgets and information items and allows adequate feature churns. Q-Tree web servers any complicated multi-attribute variety question in low latency and lowest expense. Beyond TI, any program that needs multi-attribute variety concerns in time-sensitive, light-weight and joyful way, will get benefits from Q-Tree.

VI. REFERNCES

[1] Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", proceedings in IEEE TRANSACTIONS ON NETWORKING VOL:22 NO:1 YEAR 2014.

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

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

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

[5] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

Copyright @ 2015 IJEARST. All rights reserved.

[6] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[7] 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.

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

[9] Md Ahsan Arefin, Md Yusuf Sarwar Uddin, Indranil Gupta, Klara Nahrstedt, "**Q-Tree: A Multi-Attribute Based Range Query Solution for Tele-Immersive Framework**", in *Proc. of ACM SIGCOMM*, 2009, pp. 379–390.

[10] S. Ko, S. Yalagandula, I. Gupta, V. Talwar, D. Milojicic, and S. Iyer, "Moara: Flexible and scalable group-based querying system," in *Proc. of ACM/IFIP/USENIX Middleware*, 2008.

[11] MONET, http://cairo.cs.uiuc.edu/projects/teleimmersion/.

[12] Z. Yang, Y. Cui, B. Yu, J. Liang, K. Nahrsterdt, S. H. Jung, and R. Bajscy, "Teeve: The next generation architecture for tele-immersive environments," in *Proc. of ISM*, Irvine, CA, USA, 2005, pp. 112–119.

[13] M. Arefin, M. Uddin, I. Gupta, and K. Nahrstedt, "Q-tree: A multi-attribute rnage based query solution for tele-immersive framework," in *Technical Report, UIUCDCS-R-2009-3042, UIUC*, 2009.

Copyright @ 2015 IJEARST. All rights reserved.