Privacy and Secure Data Retrival for Decentralized Military Network

Manmeet Kaur
Dept. of computer science and engineering,
Galgotia College of engineering and
technology, greaterNoida

Bhawna Mallick, PhD
Professor
Dept. of computer science and engineering,
GalgotiaCollege of engineering and
technology, greater Noida

ABSTRACT

Disruption-tolerant network (DTN) technologies are getting flourishing solutions that allow remote device sent by officers to talk with each other and access the confidential information or secret information by exploiting outside storage nodes. This technique provides economical state of affairs for authorization policies and also the policies update for secure information retrieval in most difficult cases. The foremost promising science resolution is introduced to regulate the access problems referred to as Cipher text Policy Attribute based mostly coding (CP-ABE). A number of the foremost difficult problems during this state of affairs square measure the social control of authorization policies and also the policies update for secure information retrieval. However, the matter of applying CP-ABE in decentralized DTNs introduces many security and privacy challenges with relevance the attribute revocation, key escrow, and coordination of attributes issued from totally different authorities. During this paper, we tend to propose a secure information retrieval theme exploitation CP-ABE for decentralized DTNs wherever multiple key authorities manage their attributes severally.We demonstrate the way to apply the planned mechanism to soundly and proficiently contend with the classified data spread within the Interruption or disruption tolerant network.

Keywords

Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multi-authority, secure data retrieval.

1. INTRODUCTION

Computer networking is that the follow of interfacing 2 or a lot of computing devices with one another for the aim of sharing knowledge. Laptop networks area unit engineered with a mixture of hardware and software package parts.

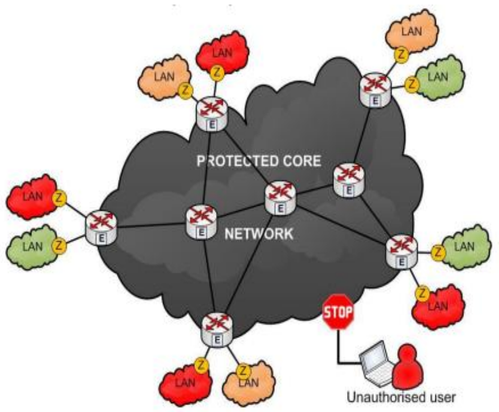
Computer networks are often categorised in many alternative ways. a method to reason the various sorts of network styles is by their scope or scale. For historical reasons, the networking business refers to just about each style of style as some reasonably space network. Common sorts of space networks are:

- LAN/NSN – native space Network
- WAN/WSN – Wide space Network
- WLAN/WNSN – Wireless native space Network
- MAN/MSN – Metropolitan space Network
- SAN/SSN –System space Network, Server space Network, or generally tiny space Network
- CAN/CSN– field space Network, Controller space Network, or generally Cluster space Network
- PAN/PSN – Personal space Network

LAN and WAN area unit the 2 primary and known classes of space networks, whereas the others have emerged with technology advances[7].

1.1 Military Network

In Military security, is a vital issue and within which heap of secret info and stuff square measure transfer, and for the secrecy we have a tendency to square measure cryptographically implemented it and within which the commander for the cluster is act because the key authority in before that the everybody within the mission is would like register within the portal for them a selected user id and arcanum is given and by that they will insect the knowledge for the ever user they're having the particular communication device and from that device they will send info within which for them for the particular region specific key authority square measure there and that they can get the key type them and because it is military setting the DTN technology is employed and it helpful even once the frequency isn't there if the soldier within the region ought to send the data he get the key type his key authority and send the knowledge to the storage node and type that needed information is ready to take by the user from the storage node Then the last challenge is that the coordination of the key authority and therefore the troopers WHO square measure holding account therein and within which previous the key written agreement downside is that there and currently it's reduced within which all the key authorities aren't ready to read the key and within which for the actual key authority can see their own cluster members and remaining cannot read and within which if the recent existing user take away account type the cluster which are going to be intimated to the key authority and therefore the account is invalid the unauthorized user ineffectual to look at square measure move into that For security purpose the coding policy is maintain during this that we have a tendency to square measure exploitation the CP-ABE coding technique the coding is totally completely different it's supported the attribute base and within which the required information that square measure taken which square measure encrypted type by obtaining the key from the authority and for the cluster of the members the individual authority is there and within which the key up date is there within the same algorithmic program is employed are the new algorithmic program is employed and within which the CP is stands for the cipher text and because it is the attribute primarily based coding the coding that's different for the individual attribute and create it's secure the member type the cluster is removed his distinctive id is removed and if the new member is joined means that constant id isn't given it's different from frequent[6].



1.2 Distributed Network

A distributed network may be a sort of electronic network that's adjoin completely different networks. This provides one digital communication network, which might be managed collectively or severally by every network. Besides shared communication among the network, a distributed network typically additionally distributes process.

Distributed networks square measure a part of distributed computing design, during which enterprise IT infrastructure resources square measure divided over variety of networks, processors and negotiator devices. A distributed network is supercharged by network management software package, that manages and monitors information routing, combining and allocating network information measure, access management and alternative core networking processes.

1.3 Attribute-Based Encryption

The concept of attribute-based cryptography was 1st projected in an exceedingly landmark work by Amit Sahai and goose Waters and later by Vipul Goyal, Omkant Pandey, Amit Sahai and goose Waters. Recently, many researchers have any projected Attribute-based cryptography with multiple authorities WHO together generate users' personal keys.

Attribute-based cryptography could be a kind of public-key cryptography within which the key key of a user and also the cipher text area unit dependent upon attributes (e.g. the country he lives, or the type of subscription he has). In such a system, the decipherment of a cipher text is feasible on condition that the set of attributes of the user key matches the attributes of the cipher text. a vital security side of Attribute-Based cryptography is collusion-resistance: Associate in Nursing someone that holds multiple keys ought to solely be ready to access knowledge if a minimum of one individual key grants access.

2. RELATED WORKS

2.1 Attribute Based Secure Data Retrieval System for Decentralized Disruption Tolerant Military Networks

According to Sagar L. Khairnar, Gayatri V. Patil, Pooja ,there are partitions in military environments like a parcel of land or a hostile region. they're probably to suffer from intermittent network property. They're having frequent partitions. Disruption-tolerant network DTN technologies square measure could be a true and simple solutions.DTN could be a Disruption-tolerant network. It permits devices that square measure wireless and carried by peoples in an exceedingly military to move with one another. These devices access the counselling or command dependably by exploiting storage device nodes. In these networking environments DTN is incredibly triple-crown technology. once there's no wired affiliation between a supply and a destination device, the knowledge from the supply node may have to attend within the intermediate nodes for an outsized quantity of your time till the affiliation would be properly established. one among the difficult approaches is associate ABE. that's attribute-based secret writing that fulfils the necessities for secure knowledge retrieval in DTNs. The conception is Cipher text Policy ABE (CP-ABE).It provides associate applicable approach of secret writing of information. The secret writing includes the attribute set that the coding must possess so as to decipher the cipher text. Hence, several users will be allowed to decipher totally different elements of information in keeping with the safety policy[1].

2.2 Privacy Preserving and Secure Data Retrieval in Sensor Network using Homomorphic Encryption Algorithm

According to S.Shanmugasundaram, S.Chitra, the Cipher text-policy Attribute primarily based coding for secure knowledge retrieval in suburbanized Disruption Tolerant Networks (DTNs) wherever multiple key authorities manage their attributes severally. Immediate attribute revocation enhances backward/forward secrecy of confidential knowledge by reducing the windows of vulnerability. Key written agreement downside is resolved by associate escrow-free key issue protocol that exploits the characteristic of the suburbanized Disruption Tolerant Networks design projected a suburbanized approach; their technique doesn't evidence users. Demonstrate a way to apply the projected mechanism to firmly and expeditiously manage the confidential knowledge distributed within the disruption-tolerant military network. Finally the Disruption-tolerant network (DTN) technologies are getting in solutions that enable wireless devices carried by troopers to speak with one another and access the confidential info or command dependably by exploiting secondary storage nodes. We have a tendency to propose associate economical system for preventing location leaks in detector Networks and conjointly it ensures the privacy-preserving theme against traffic analysis and flow tracing. With the quicker homomorphic coding algorithmic program technique, the projected theme offers 2 vital privacy conserving options, packet flow untraceability and message content confidentiality, which may expeditiously thwart traffic analysis/flow tracing attacks. Moreover, with homomorphic coding, the projected theme keeps the essence of random linear network committal to writing, and every sink will recover the supply messages by inverting with a really high likelihood. Our projected system works expeditiously in comparison to antecedently existing schemes[2].

2.3 Quick and Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

According to A. Vineth1, John Deva Prasanna they explain, The DTN technology is that the far-famed technology that employed in the military network it's disagree from the conventional peer to see network it's having the storage network if the affiliation isn't establish it'll store within the storage node the once the affiliation is establish then it transfer to the receiver to create it secure ABE CP is employed during which the transfer knowledge is encrypted during which the secret's needed to decode, for that key manager is ready up because it could be a localised network multiple key authority are localised new bundle protocol is employed for its potency and build it as traffic free session management is employed during which we have a tendency to are having quick and secure knowledge transfer[3].

2.4 Advanced Data Access Scheme in Disruption Tolerant Network

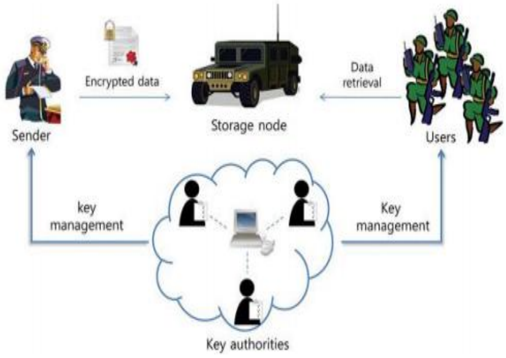
According to S.Revathi , A.P.V.Raghavendra they explain, Disruption- tolerant network (DTN) technologies are thought of to be the productive solutions, permit nodes to speak with one another within the extreme networking environments. a number of the foremost difficult problems during this state of affairs are the social control of authorization policies and also the policy change for secure knowledge retrieval. The construct of attribute-based coding (ABE) could be a promising approach that full fills the wants for secure knowledge retrieval in DTN. The prevailing system involves cipher text-policy attribute-based coding (CP-ABE) presentation, that provides a ascendible means of encrypting knowledge specified the encrypter defines the attribute set that the decrypted must method for decrypting the cipher text. However, the matter of applying CP-ABE in localized DTN ends up in many security and privacy challenges with regards to the attribute revocation, key escrow, and coordination of attributes issued from totally different authorities. So, a secure knowledge retrieval theme is required for exploitation CP-ABE for localized DTNs wherever multiple key authorities manage their attributes severally. However the most disadvantage is that the change of attributes isn't thus economical and high quality. so as to beat the higher than cited issues i am proposing a replacement technique “Efficient Trust management system (ETMS)”, for reducing quality and conjointly to enhance the protection in DTN. Additionally to it the geographical routing is additionally used for locating the situation of the nodes. During this technique, every node analyzes alternative neighbour nodes, that ar situated within the same subtask cluster. whereas every subtask cluster leader (SGL) identifies alternative SGLs and nodes in its subtask cluster and followed with the peer-to-peer trust analysis is sporadically updated supported either direct observations or indirect observations. The experimental results show that, the planned ETMS technique achieves high potency and security with less quality[4].

2.5 Secure Information Recovery for Decentralized Interruption

According to Korra Bichya they explains, Portable nodes in military environments, for instance, a front or Associate in Nursing antagonistic space area unit vulnerable to expertise the bear of irregular system network and frequent partitions. Interruption tolerant network (ITN) innovations are becoming to be fruitful results that let remote device sent by officers to talk with each other and access the key knowledge or summon faithfully by abusing outside capability nodes. most likely the foremost troublesome problems during this scenario area unit the need of approval arrangements and also the ways design for secure info recovery. Ciphertext-policy attribute-based coding (CP-ABE) could be a guaranteeing cryptographical account the proper to realize entrance management problems. In any case, the problem of applying CP-ABE in decentralized DTNs presents many securities and protection challenges on the property disclaimer, key escrow, and coordination of characteristics issued from distinctive powers. during this paper, we have a tendency to propose a secure info recovery set up utilizing CP-ABE for decentralized DTNs wherever varied key powers agitate their qualities autonomously. we have a tendency to show a way to apply the projected mechanism to securely and proficiently agitate the classified info spread in the Interruption tolerant network (ITN)[5].

3. PROPSED METHODLOLGY

In this we propose associate degree attribute-based secure information retrieval theme mistreatment CP-ABE for decentralised DTNs. The projected theme options the subsequent achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential information by reducing the windows of vulnerability. Second, encryptors will outline a fine-grained access policy mistreatment any monotone access structure beneath attributes issued from any chosen set of authorities. Third, the key written agreement drawback is resolved by associate degree escrow-free key issue protocol that exploits the characteristic of the decentralised DTN design. The key issue protocol generates and problems user secret keys by acting a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of every other such none of them could generate the full set of user keys alone. Thus, users aren't needed to completely trust the authorities so as to shield their information to be shared. The information confidentiality and privacy is cryptographically implemented against any curious key authorities or data storage nodes within the projected theme.



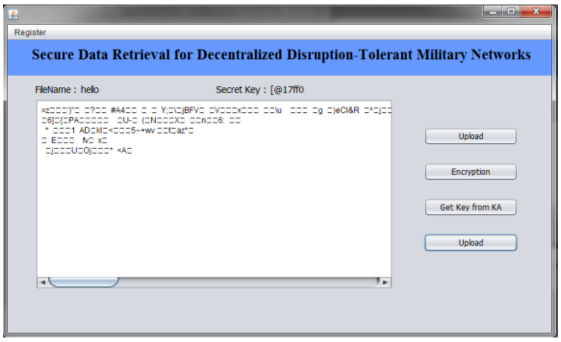
Advantages of Proposed System:

- **Data confidentiality:** Unauthorized users who didn't have enough credentials which satisfyies the access policy and it should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.
- **Collusion-resistance:** If multiple users collude, they might be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone.

Backward and forward Secrecy: In the context of ABE, backward secrecy means associatey user WHO involves hold an attribute (that satisfies the access policy) ought to be prevented from accessing the plaintext of the previous knowledge changed before he holds the attribute. On the opposite hand, forward secrecy means associatey user WHO drops an attribute ought to be prevented from accessing the plaintext of the next knowledge changed once he drops the attribute, unless the opposite valid attributes that he's holding satisfy the access policy[8].

4. IMPLEMENTATION

We have used Java programming language to implement the CP-ABE for DTN. within the remainder of this section, initial we are going to discuss the planned Disruption Tolerant military network then we have a tendency to mix our CP-ABE theme with decentralized DTN for secure knowledge retrieval. initial we've got designed the Disruption Tolerant Network (DTN) that introduces the construct of storage nodes whereby the confidential knowledge is replicated or keep such solely licensed mobile nodes will access the required info quickly and faithfully. The sender (commander) United Nations agency owns the confidential knowledge has the authority to register users (soldiers) and supply access privileges.



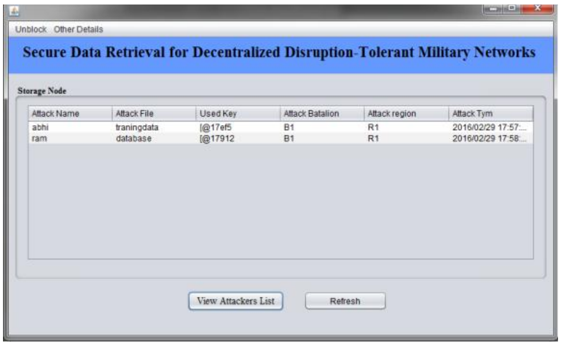
Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

FileName : hello   Secret Key : [@17ff0

```
=z□□□')"□ □?□□ #A4□□ □ □ Y;□\□jBFV□ □V□□□x□□□ □□\u  □□□ □g □)eCl&R □^□j□□
□6]□{□PA□□□□□  □U-□ (□N□□□X□ □□n□□6: □□
 * □□□1 AD□kl□<□□□5~+wv □□t□az*□
□ E□□□  fV□ x□
 □j□□□U□Oj□□□* <A□
```

Fig. 1. Sender Module

Fig. 1 shows the sender module implementation. The confidential data is encrypted before stored in the storage node. The key Authority generates a secret key for the user with respect to the attributes set. Sender encrypts the data and defines an access policy (i.e., Combination of battalion and region) which the user needs to possess in order to decrypt the data from the storage node. The cipher text is encrypted with an access policy chosen by an encryptor and then it is stored in the storage node.



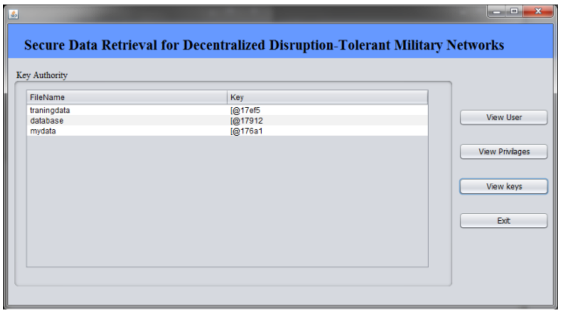
Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

Storage Node

Attack Name	Attack File	Used Key	Attack Batalion	Attack region	Attack Tym
abhi	traningdata	[@17ef5	B1	R1	2016/02/29 17:57:...
ram	database	[@17912	B1	R1	2016/02/29 17:58:...

Fig. 2. Storage Node-Attackers list

Fig. 2 shows the implementation of storage node. All the files stored can be viewed in here. All users who try to access the data from the storage node without satisfying the access policy will be blocked and will be added to the attackers list. Sender has the access to revoke any user at any point of time by unblocking them from the attackers list.



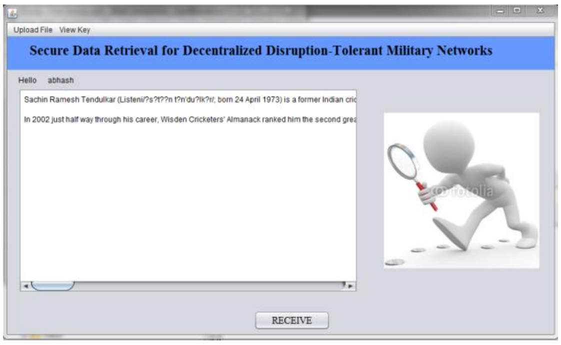
Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

Key Authority

FileName	Key
traningdata	[@17ef5
database	[@17912
mydata	[@176a1

Fig. 3. Key Authority

Fig. 3 shows the functionality of key authority. The key authority generates the secret keys to the user with respect to the attribute set. It can view the list of users, list of keys given to users and the privileges assigned to different users. 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. Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node. Meanwhile, they should be still able to issue secret keys to users. In order to achieve this the key authorities and sender engage in a secure two party computation such that end user (soldier) needs to satisfy the access policy defined by the commander and also must have enough privileges from sender to access the confidential data.



Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

Hello abhash

Sachin Ramesh Tendulkar (Listeni/?s?t??n t?n'du?lk?r/; born 24 April 1973) is a former Indian cric

In 2002 just half way through his career, Wisden Cricketers' Almanack ranked him the second grea

Fig. 4. Receiver Module

5. CONCLUSION

DTN technologies are getting roaring solutions in military applications that permit wireless devices to speak with one another and access the counsel dependably by exploiting memory device nodes. CP-ABE could be a scalable cryptanalytic resolution to access management and to secure knowledge retrieval problems. During this project, associate economical and secure knowledge retrieval methodology exploitation CP-ABE for decentralised DTNs wherever multiple key authorities manage their attributes severally has been enforced. The inherent key written agreement downside is resolved such the confidentiality of the hold on knowledge is bonded even underneath the hostile surroundings wherever key authorities may well be compromised or not absolutely trustworthy and additionally, the fine-grained key revocation are often in serious trouble every attribute cluster knowledge.

6. REFERENCES

[1] Sagar L. Khairnar, Gayatri V. Patil, Pooja , "Attribute Based Secure Data Retrieval System for Decentralized DisruptionTolerant Military Networks", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume: 2 Issue:2014.

[2] S.Shanmugasundaram, S.Chitra, "Privacy Preserving and Secure Data Retrieval in Sensor Network using Homomorphic Encryption Algorithm", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 12 Issue 3 –JANUARY 2015

[3] A. Vineth1, John Deva Prasanna, "Quick and Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Index Copernicus Value (2013): 6.14 | Impact Factor (2013).

[4] S.Revathi , A.P.V.Raghavendra, "Advanced Data Access Scheme in Disruption Tolerant Network", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 10, October 2014, ISSN(Online): 2320-9801 ISSN (Print): 2320-9798.

[5] Korra Bichya,"Secure Information Recovery for Decentralized Interruption Tolerant Defense Data Network" ,INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 1, ISSUE 3, SEPTEMBER 2014, PP 119-126, ISSN: 2349-7084.

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

[7] Miss. Arshiya Tabassum R.A.Khan, Miss. Ashwitha Reddy, "Secure Data Retrieval for Decentralized Disruption Tolerant Military Network", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences, (NCDATES- 09th & 10th January 2015).

[8] C. Rajeshwar Reddy, N.V. Sailaja, "Secure Data Retrieval Using CP-ABE for Decentralized Disruption Tolerant Military Networks , (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4201-4205, ISSN: 0975-9646.

[9] E K Girisan, Shidha S, "A Survey Of Secure Data Transfer In Disruption Tolerant Military Network, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 4, April 2015, ISSN (Online) 2278-1021 ISSN (Print) 2319-5940.

[10] Naveen K B, Pratibha Mishra, "Survey on Fault Tolerant Data Retrieval in Military Network, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 198-201, ISSN 2320–088X.

[11] Bhavyashree H D, M S Maheshan, "Secure Data Retrieval For Decentralized Disruption-Tolerant Military Networks Using Cp-Abe", International Journal For Technological Research In Engineering Volume 2, Issue 10, June-2015, ISSN (Online): 2347 – 4718.

[12] Seema S Balappanavar, Prof. Arati Shahapurk, "Secure and efficient management of confidential data in the decentralized disruption-tolerant militery networks", The International Journal Of Engineering And Science (IJES) || Volume || 4 || Issue || 5 || Pages || PP.01-05 || 2015 || ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805.

[13] Umoh Bassey Offiong, M. B. Mukeshkrishnan, "Securing Data Retrieval for Decentralized Disruption Tolerant Military Networks (DTNs) using Cipher text Policy Attribute-Based Encryption", International Journal of Engineering Trends and Technology (IJETT) – Volume 26 Number 5- August 2015.

[14] Girish Kumar B.C , S. N. Chandrashekara, Harshavardhana Doddamani, "Secure Data Retrieval Using CP-ABE for Decentralized Disruption-Tolerant Military Networks", International Journal of Engineering Science and Computing ISSN2321 3361 © 2015.