ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A TECHNIQUE TO PROVIDE SECURITY IN DECENTRALIZED MILITARY NETWORK FOR DATA SHARING

Ms. Priyanka S. Mehakare[*1] and Prof. Mayur Dhait[2]
[*1]Student,Dept. Of Computer Science and Engineering , ACE Nagthana, Wardha, Maharashtra,India.
[2]Professor,Dept. Of Computer Science and Engineering , ACE Nagthana, Wardha, Maharashtra,India.

ABSTRACT

Dynamic Portable center points in military circumstances, for instance, a forefront or a debilitating area are subject to encounter the evil impacts of unpredictable framework system and nonstop assignments. Intrusion tolerant framework (DTN) advances are getting the opportunity to be productive game plans that allow remote devices passed on by officers to compare with each other and access the arranged information or summon constantly by abusing external stockpiling center points. Unquestionably the most troublesome issues in this circumstance are the execution of endorsement techniques and the methodologies update for secure data recuperation. Figure content methodology characteristic based encryption (CP-ABE) is a promising cryptographic response for the passageway control issues. In any case, the issue of applying CP-ABE in decentralized DTNs presents a couple security and insurance challenges with regards to the property foreswearing, key escrow, and coordination of qualities issued from particular forces. In this paper, we propose a protected data recuperation arrangement using CP-ABE for decentralized DTNs where different key forces manage their qualities unreservedly. We demonstrate to apply the proposed instrument to securely and viably manage the private data scattered in the aggravation tolerant military framework.

Keywords: *Cluster Generation, Advanced Encryption standard (AES), disruption-tolerant network (DTN), multi authority, military system.*

1. INTRODUCTION

1.1 What is Disruption tolerant network?

In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. TN architecture may be referred as where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes.

Probably the most difficult issues in this situation are the implementation of approval approaches and the strategies upgrade for secure information recovery. Figure content approach quality based encryption (CP-ABE) is a promising cryptographic answer for the entrance control issues. On the other hand, the issue of applying CP-ABE in decentralized DTNs presents a few security and protection challenges with respect to the characteristic disavowal, key escrow, and coordination of traits issued from distinctive powers. In this paper, we propose a protected information recovery plan utilizing CP-ABE for decentralized DTNs where various key powers deal with their characteristics autonomously. We show how to apply the proposed system to safely and proficiently deal with the

ISSN 2348 – 8034
Impact Factor- 4.022

classified information conveyed in the interruption tolerant military system. Portable hubs in military situations, for example, a war zone or an unfriendly locale are prone to experience the ill effects of irregular system network and regular allotments. Interruption tolerant system (DTN) innovations are getting to be fruitful arrangements that permit remote gadgets conveyed by fighters to speak with one another and access the secret data or order dependably by misusing outer stockpiling hubs. Probably the most difficult issues in this situation are the requirement of approval arrangements and the strategies upgrade for secure information recovery.

1.2 What is Disruption Tolerant Network (DTN)?

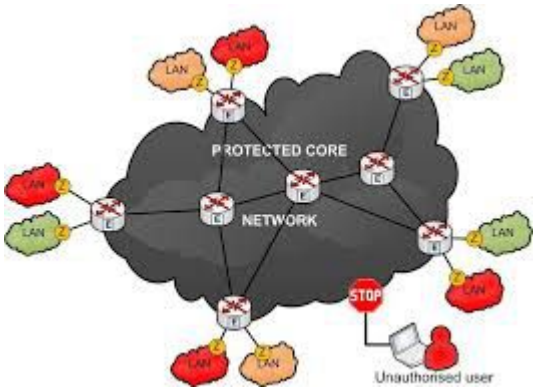

Fig 1. Military Networks

Interruption tolerant systems administration (DTN) is a way to deal with PC system engineering that looks to address the specialized issues in heterogeneous systems that may need constant system availability. Case of such systems are those working in versatile or compelling physical situations, or arranged systems in space. Interruption tolerant system (DTN) advancements are getting to be effective arrangements that permit hubs to speak with each other. Commonly when there is no limit to-end association between a source and a destination match, the messages from the source hub may need to sit tight in the middle hubs for a generous measure of time until the association would be in the end built up. After the association is in the long run set up, the message is conveyed to the destination hub.

As a case, in a combat zone DTN, a capacity hub may have some private data which ought to be gotten to just by an individual from „Battalion 6" or a member in „Mission 3". A few current arrangements take after the customary cryptographic-based methodology where the substance are encoded before being put away hubs, and the decoding keys are appropriated just to approved clients. In such methodologies, adaptability and granularity of substance access control depends vigorously on the fundamental cryptographic primitives being utilized. It is difficult to adjust between the multifaceted nature of key administration and the granularity of access control utilizing any arrangements that depend on the ordinary pair insightful key or gathering key primitives. Along these lines, regardless we have to outline a versatile arrangement that can give fine-grain access control. That is a DTN design where various powers issue and deal with their own trait keys freely as a decentralized DTN.

2. RELATED WORK

In this paper, maker propose an ensured data recuperation arrangement using CP-ABE for decentralized DTNs where different key forces manage their characteristics openly. We display how to apply the proposed instrument to securely and successfully manage the mystery data dispersed in the unsettling influence tolerant military network.[1]

In these frameworks organization circumstances DTN is outstandingly viable development The thought is Cipher content Policy ABE (CP-ABE).it gives a fitting strategy for encryption of data. The encryption consolidates the property set that the translating needs remembering the final objective to unscramble the figure content. In this manner, Many customers can be allowed to translate different parts of data as demonstrated by the security policy.[2]

In this paper, Author propose a secured data recuperation arrangement using CP-ABE for decentralized DTNs where various key forces manage their credits autonomously. We display how to apply the proposed framework to safely and competently deal with the assembled information scattered in the Interruption or unsettling influence tolerant network.[3]

In this methodology, each center separates other neighbor center points, which are arranged in the same subtask pack. While each subtask group pioneer (SGL) perceives diverse SGLs and centers in its subtask total and brought after with the appropriated trust appraisal is irregularly updated considering either organize discernments or indirect recognitions. The trial results exhibit that, the proposed ETMS procedure performs high efficiency and security with less complexity.[4]

CPABE is one such cryptographic framework which gives the response for the passageway control issues. Nevertheless, there exists a couple issues as for key escrow, trademark disavowal and coordination of attributes which are issued by assorted key forces while applying CP-ABE in decentralized DTNs. In this paper, more secured system for the recuperation of arranged data using CP-ABE for decentralized DTNs is proposed where sets of attributes will be delivered and regulated by various powers self-governingly and addresses a couple existing problem.[5]

In this paper we focus on an essential issue of value denial which is cumbersome for CP-ABE arranges. In particular, we re-settle this considering in order to test issue more conventional circumstances in which semi-trustable on-line go-between servers are open. At the point when stood out from existing arrangements, our proposed course of action enables the ability to repudiate customer attributes with immaterial e ort. We perform this by uncommonly planning the arrangement of mediator re-encryption with CP-ABE, and engage the ability to dole out most of troublesome endeavors to middle person servers. Formal examination shows that our proposed arrangement is provably secure against picked figure content strikes. In advancement expression, we exhibit that our method can in like manner be applicable to the Key-Policy Attribute Based Encryption (KP-ABE) counterpart.[6]

In this paper we demonstrate a system for recognizing complex access control on mixed data that we call Cipher content Policy Attribute-Based Encryption. By using our methods mixed data can be kept confidential paying little mind to the way that the stor-age server is untrusted; what's more, our schedules are secure against plot attacks. Past Attribute-Based Encryption systems used credits to delineate the mixed data and consolidated game plans with customer's keys; while in our structure credits are used to depict a customer's affirmations, and a social occasion encoding data stop burrows a methodology for who can unscramble. Thusly, our techniques are hypothetically nearer to standard access control procedures, for instance, Role-Based Access Control (RBAC). Also, we give a use of our sys-tem and give execution measurements.[7]

3. PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner:

In this paper, we propose a trademark based secure data recuperation arrangement using CP-ABE for decentralized DTNs. The proposed arrangement highlights the going with achievements. Regardless, fast trademark disavowal overhauls backward/forward puzzle of ordered data by lessening the windows of feebleness. Second, encryptors can portray a fine-grained access course of action using any monotone access structure under properties issued from any picked plan of forces. Third, the key escrow issue is dictated by a sans escrow key issuing tradition that enterprises

ISSN 2348 – 8034
Impact Factor- 4.022

the ordinary for the decentralized DTN building plan. The key issuing tradition makes and issues customer puzzle keys by performing an ensured two-party estimation (2PC) tradition among the key forces with their own master insider certainties. The 2PC tradition demoralizes the key forces from getting any master riddle information of each other such that none of them could make the whole plan of customer keys alone. In this way, customers are not expected to totally trust the instructing voices remembering the deciding objective to guarantee their data to be shared. The data mystery and security can be cryptographically maintained against any curious key forces or data stockpiling centers in the proposed arrangement.

- To propose a property based secure information recovery plan utilizing CP-ABE for decentralized DTNs.

- Cipher content strategy ABE (CP-ABE) gives a versatile method for scrambling information such that the encode or characterizes the trait set that the unscramble or needs to have with a specific end goal to decode the figure content.

- The key issuing convention creates and issues client mystery keys by performing a safe two-party calculation (2PC) convention among the key powers with their own particular expert mysteries.

- The 2PC convention deflects the key powers from getting any expert mystery data of one another such that none of them could create the entire arrangement of client key

Architecture Block Diagram of System

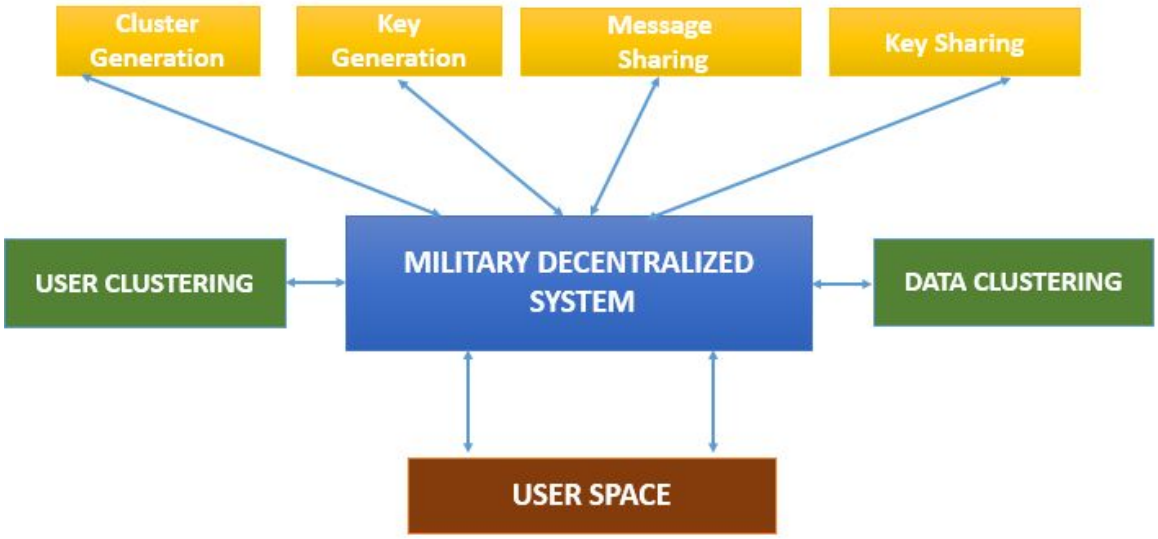

Fig -1: Basic System Architecture

- **Data confidentiality:** Unauthorized users who do not have enough credentials satisfying the access policy 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 may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone.

ISSN 2348 – 8034
Impact Factor- 4.022

- **Backward and forward Secrecy:** In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

AES algorithm is used as a strong encryption algorithm. As studies shows AES algorithm is much stronger as compared to other encryption schemes and also exploits security issues in Mobile Ad Hoc Networks. The two inter and intra cluster data passing is done in the form of messages. SHA and AES is used for key generation and data Security respectively. From the results we can verify the efficiency of proposed system in military networks and it proves to be efficient than existing schemes.

Following figure shows the flowchart of design:

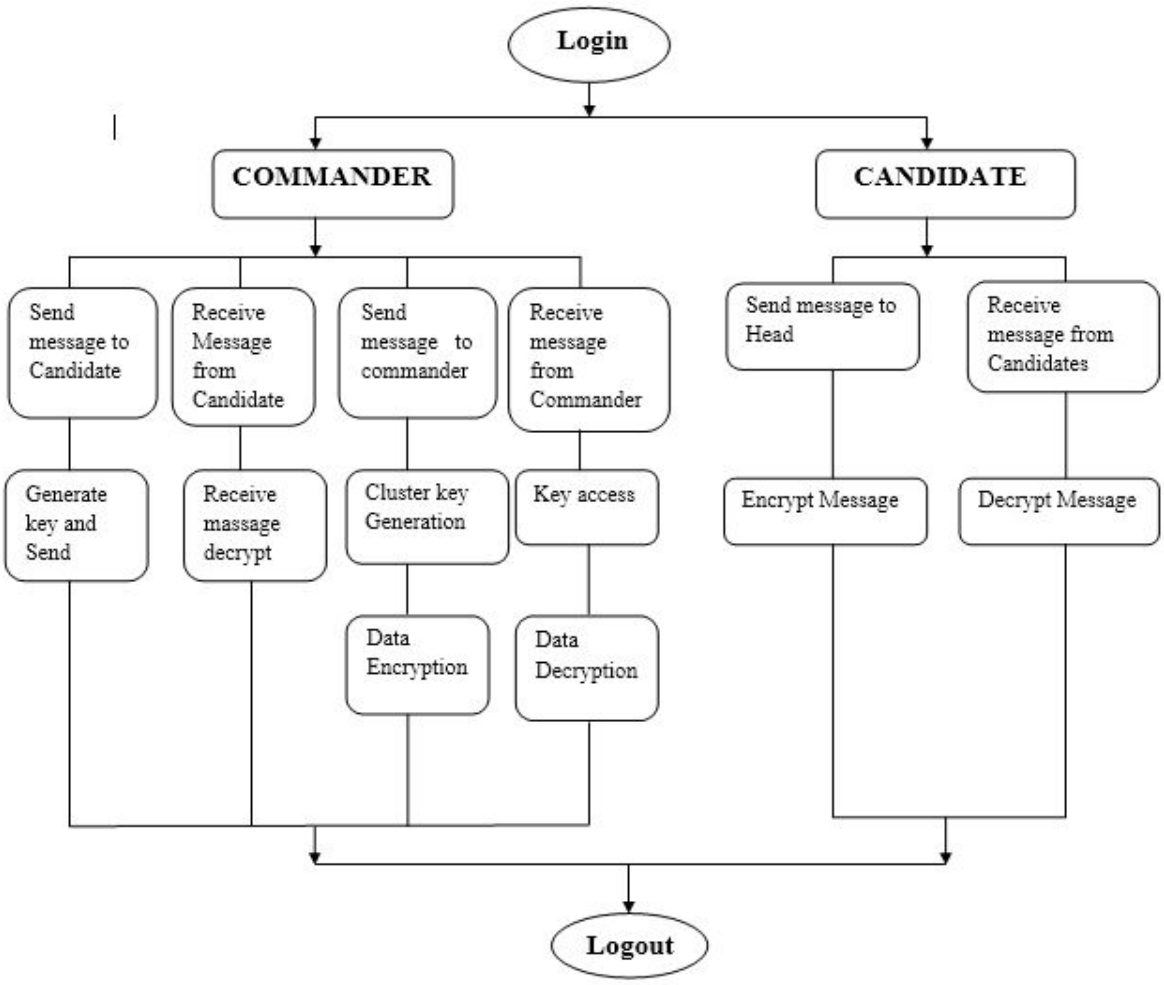

Fig -2: Flowchart of Design

ISSN 2348 – 8034
Impact Factor- 4.022

Use Case Diagram

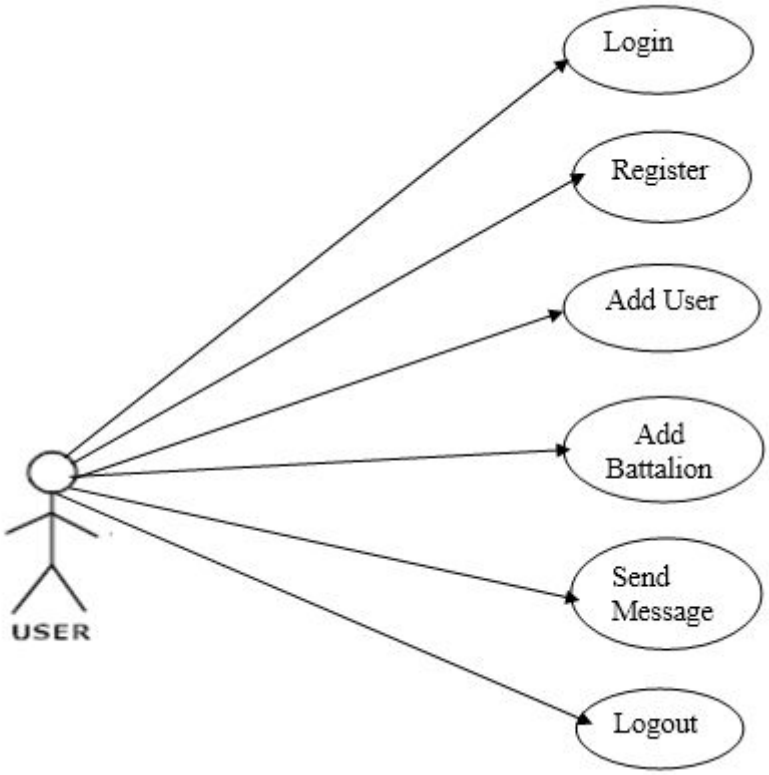

Fig.3 Use Case Diagram

Advantages of Proposed System

1. As in proposed system we will be using heavy encryption scheme along with compression, it will give better throughput with better efficiency.

2. Use of strong encryption scheme with hashing algorithm will provide better security to the message during the transmission.

3. Use of effective compression scheme will help to reduce the energy consumption during the transmission of data as well as will provide security to the encrypted message.

4. METHODOLOGY

MODULES:

1. **Cluster generation**
2. **Key Exchange**
3. **Text Sharing**
4. **File Sharing**
5. **Data Leakage Prevention**

ISSN 2348 – 8034
Impact Factor- 4.022

4.1 MODULES DESCRIPTION:

1. Cluster Generation:

Two clusters are formed separately, one for the battalion and one for the commandos so that the security level will increase and will have a desired output.

2. Key Exchange:

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.Text sharing:

This module is used for the text purpose.

4.File sharing:

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.

5. Data leakage Prevention:

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 cipher text and obtain the data**.**

4.2 Algorithms

- **AES Algorithm**

```
byte state[4,Nb]
state = in
AddRoundKey(state, keySchedule[0, Nb-1])
for round = 1 step 1 to Nr–1 {
        SubBytes(state)
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, keySchedule[round*Nb,(round+1)*Nb-1])
}
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, keySchedule[Nr*Nb, (Nr+1)*Nb-1])
```

out = state

Clustering in K-Means Algorithm

- For a given cluster assignment C of the data points, compute the cluster means m_k:

$$m_k = \frac{\sum_{i:C(i)=k} x_i}{N_k}, \; k = 1, \ldots, K.$$

- For a current set of cluster means, assign each observation as:

$$C(i) = \arg\min_{1 \le k \le K} \|x_i - m_k\|^2, \; i = 1, \ldots, N$$

- Iterate above two steps until convergence
- Algorithmically, very simple to implement
- *K*-means converges, but it finds a local minimum of the cost function
- Works only for numerical observations
- *K* is a user input; alternatively BIC (Bayesian information criterion) or MDL (minimum description length) can be used to estimate *K*
- Outliers can considerable trouble to *K*-means.

k-implies batching is a procedure for vector quantization, at first from sign taking care of, that is popular for gathering examination in data mining. k-suggests packing hopes to package n observations into k bunches in which each discernment has a spot with the gathering with the nearest mean, serving as a model of the group.

The issue is computationally troublesome (NP-hard); in any case, there are capable heuristic estimations that are consistently used and blend quickly to a close-by perfect. These are normally similar to the yearning growth estimation for mixes of Gaussian flows by method for an iterative refinement approach used by both figurings. Also, they both use bunch centers to demonstrate the data; in any case, k-infers bundling has a tendency to find clusters of equal spatial degree, while the yearning support part allows gatherings to have various shapes.

The computation has a free relationship to the k-nearest neighbor classifier, an understood machine learning technique for gathering that is consistently mixed up for k-infers by virtue of the k in the name. One can apply the 1-nearest neighbor classifier on the gathering centers gained by k-plans to arrange new data into the present packs. This is known as nearest centroid classifier or Rocchio computation.

5. DESIGN WORK

5.1 Source

Brief Overview about Problem Definition

In the large 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 regular medium. Portable nodes in military environments, for example, a front line or an antagonistic area are prone to experience the undergo of irregular system network and frequent partitions. Disruption-tolerant network (DTN) innovations are getting to be fruitful results that permit remote device conveyed by officers to speak with one another and access the confidential data or

ISSN 2348 – 8034
Impact Factor- 4.022

secret data or summon dependably by abusing outside capacity nodes or storage nodes. Thus a new methodology is introduced to provide successful communication between each other as well as access the confidential information provided by some major authorities like commander or other superiors. The methodology is called Disruption-Tolerant Network (DTN). This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases.

5.2 Algorithm / Procedure used

Procedure: Login (Username, Password)

Step 1: Read Username into a variable

unam = TextBox.getText()

Step 2: Read Password into a variable

pass = PasswordBox.getText()

Step 3: Connect to Database

Connection = MySQL. Connect ()

Step 4: Check for validation

If (Username and Password are present)

Go to MainPage

Else

Error" Some trouble is occur";

Step 5: Stop.

6. CONCLUSION AND FUTURE SCOPE

Information security assumes a critical part while managing in military based systems. Military systems work in decentralized which makes it harder to keep up information security and key administration in systems. To handle this issue we propose a structure that can give legitimate information and key security with the assistance of ON FLY key administration and solid symmetric AES encryption calculation. The proposed framework produces diverse bunches in view of military systems and gives legitimate ON FLY key administration to groups. The two entomb and intra bunch information passing is done as messages. SHA and AES is utilized for key era and information Security individually. From the outcomes we can check the proficiency of proposed framework in military systems and it turns out to be effective than existing plans.

In this paper we have proposed a framework that will give better security in cloud environment. We have proposed a security design which gives solid security utilizing AES calculation.

Future Scope

In future we plan to give more security to framework utilizing various encryption calculation at ones. We likewise plan to give record sharing component in the framework with the goal that client will have the capacity to share their document. We will likewise jump at the chance to give an additional element of information accessibility which will expand dependability of framework regardless of the possibility that one of the server crashes. Quicker key era for

better security and proficiency. Usage of same philosophy on unified systems. Ready to exchange various messages and flies at same time.

REFERENCES

[1] *Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", Member, IEEE, ACM, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014.*

[2] *L. Khairnar1 Gayatri V. Patil,Hemant D. Sonawane,"Attribute Based Secure Data Retrieval System for Decentralized Disruption Tolerant Military Networks", Sagar. International Journal on Recent and Innovation Trends in Computing and Communication 2014.*

[3] *S.Revathi 1, A.P.V.Raghavendra, "Advanced Data Access Scheme in Disruption Tolerant Network ", International Journal of Innovative Research in Computer and Communication Engineering.*

[4] *Miss. Arshiya Tabassum R.A.Khan,Miss. Ashwitha Reddy,"Secure Data Retrieval For Decentralized Disruption Tolerant MilitaryNetwork",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).*

[5] *Sneha and H. Harshavardhan,"CP-ABE in Decentralized Disruption-Tolerant Military Networks for Secure Retrieval of Data ",Proceedings of the International Conference , "Computational Systems for Health Sustainability"17-18, April, 2015.*

[6] *S. Yu, C. Wang, K. Ren, and W. Lou,"Attribute based data sharing with attribute revocation",in Birget, N. Memon Proc. ASIACCS, 2010.*

[7] *Bethencourt, A. Sahai, and B. Waters,"Cipher text-policy attribute based encryption", IEEE Symp. Security Privacy, 2007.*

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

[9] *M. Chase and S. S. M. Chow, "Improving privacy and security inmultiauthority attribute-based encryption", ACM Conf. Comput. Commun. Security, 2009.*

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

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

[12] *X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded cipher text policy attribute based encryption," in Proc. ASIACCS, 2009.*

[13] *M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in Proc. ACM Conf. Comput.Commun. Security, 2009*

[14] *M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute base systems," in Proc. ACMConf. Comput. Commun. Security, 2006*

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

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

[17] *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.*

[18] *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.*

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

ISSN 2348 – 8034
Impact Factor- 4.022

[20]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.
[21] 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.
[22]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.D.
[23] 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.