An Approach for Security in Data Sharing Application for Decentralized Military Network

Ms. Priyanka S. Mehakare[1]
[1]Student,
Dept. Of Computer Science and Engineering , ACE
Nagthana, Wardha, Maharashtra,India.
[1]priyata.mehakare@gmail.com

Prof. Mayur Dhait[2]
[2]Professor,
Dept. Of Computer Science and Engineering , ACE
Nagthana, Wardha, Maharashtra,India.
[2]mayursdhait@gmail.com

Abstract- Portable hubs in military situations, for example, a front line or a threatening locale are liable to experience the ill effects of irregular system network and continuous allotments. Interruption tolerant system (DTN) advances are getting to be fruitful arrangements that permit remote gadgets conveyed by officers to correspond with one another and access the classified data or summon dependably by misusing outer stockpiling hubs. The absolute most difficult issues in this situation are the implementation of approval strategies and the approaches redesign for secure information recovery. Cipher text-approach trait based encryption (CP-ABE) is a promising cryptographic answer for the entrance control issues. Be that as it may, the issue of applying CP-ABE in decentralized DTNs presents a few security and protection challenges as to the property denial, key escrow, and coordination of characteristics issued from distinctive powers. In this paper, we propose a safe information recovery plan utilizing CP-ABE for decentralized DTNs where various key powers deal with their qualities freely. We show how to apply the proposed instrument to safely and effectively deal with the private information dispersed in the disturbance tolerant military system.

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

*****

1. INTRODUCTION

What is Disruption tolerant network?

In numerous military system situations, associations of remote gadgets conveyed by fighters might be incidentally disengaged by sticking, natural components, and portability, particularly when they work in unfriendly situations. Disturbance tolerant system (DTN) advances are getting to be effective arrangements that permit hubs to speak with each other in these amazing systems administration situations. Commonly, when there is no limit to-end association between a source and a destination combine, the messages from the source hub may need to sit tight in the middle of the road hubs for a generous measure of time until the association would be in the long run built up. TN engineering might be alluded as where different powers issue and deal with their own trait keys freely as a decentralized DTN.

Portable hubs in military situations, for example, a combat zone or an antagonistic locale are prone to experience the ill effects of irregular system availability and successive parcels. Interruption tolerant system (DTN) innovations are getting to be fruitful arrangements that permit remote gadgets conveyed by officers to speak with each other and access the private data or charge dependably by abusing outside capacity hubs.

Probably the most difficult issues in this situation are the requirement of approval approaches and the strategies upgrade for secure information recovery. Figure content arrangement trait based encryption (CP-ABE) is a promising cryptographic answer for the entrance control issues. Nonetheless, the issue of applying CP-ABE in decentralized DTNs presents a few security and protection challenges with respect to the trait repudiation, key escrow, and coordination of properties issued from various powers. In this paper, we propose a safe information recovery plan utilizing CP-ABE for decentralized DTNs where different key powers deal with their qualities autonomously. We show how to apply the proposed system to safely and proficiently deal with the secret information circulated in the interruption tolerant military system. In various military framework circumstances, relationship of remote contraptions passed on by officers might be by the way isolated by staying, common segments, and compactness, especially when they work in debilitating circumstances. Unsettling influence tolerant framework (DTN) developments are getting the chance to be productive courses of action that allow center points to talk with each other in these convincing frameworks organization circumstances.

1.2 What is Disruption Tolerant Network (DTN)?

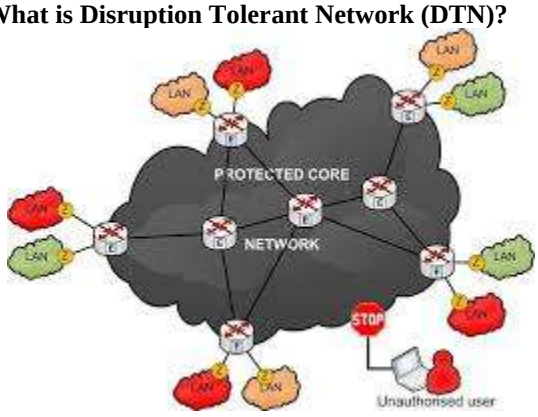

Fig 1. Military Networks

Disruption-tolerant networking (**DTN**) is a way to deal with PC system engineering that looks to address the specialized issues in heterogeneous systems that may need persistent system availability. Case of such systems are those working in portable or amazing physical situations, or arranged systems in space. Interruption tolerant system (DTN) innovations are getting to be effective arrangements that permit hubs to speak with each other. Ordinarily 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 of the road hubs for a significant measure of time until the association would be in the end built up. After the association is in the end built up, the message is conveyed to the destination hub.

2. RELATED WORK

In this technique, each center separates other neighbor center points, which are arranged in the same subtask cluster. While each subtask bundle pioneer (SGL) perceives diverse SGLs and center points in its subtask total and brought after with the appropriated trust evaluation is irregularly updated considering either facilitate observations or indirect recognitions. The trial results exhibit that, the proposed ETMS method performs high profitability and security with less complexity.[4]

CPABE is one such cryptographic framework which gives the response for the passageway control issues. In any case, there exists a couple issues as for key escrow, trademark renouncement and coordination of characteristics which are issued by different key forces while applying CP-ABE in decentralized DTNs. In this paper, more secured procedure for the recuperation of grouped data using CP-ABE for decentralized DTNs is proposed where sets of characteristics will be delivered and supervised by various powers self-rulingly and addresses a couple existing problem.[5]

In this paper we focus on a fundamental issue of value denial which is massive for CP-ABE arranges. In particular, we re-settle this considering in order to test issue more rational circumstances in which semi-trustable on-line delegate servers are open. At the point when stood out from existing arrangements, our proposed course of action engages the ability to deny customer qualities with irrelevant effort. We fulfill this by incredibly organizing the arrangement of middle person re-encryption with CP-ABE, and enable the ability to dole out most of troublesome endeavors to mediator servers. Formal examination exhibits that our proposed arrangement is provably secure against picked figure content ambushes. In advancement word usage, we show that our system can in like manner be germane 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 systems mixed data can be kept confidential paying little heed to the way that the stor-age server is untrusted; furthermore, our schedules are secure against plot strikes. Past Attribute-Based Encryption structures used credits to delineate the mixed data and fused game plans with customer's keys; while in our system credits are used to depict a customer's confirmations, and a social event encoding data stop burrows a technique for who can unscramble. Thusly, our techniques are hypothetically nearer to standard access control procedures, for instance, Role-Based Access Control (RBAC). In addition, 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 information recovery game plan utilizing CP-ABE for decentralized DTNs. The proposed plan highlights the running with accomplishments. In any case, quick trademark repudiation updates in reverse/forward riddle of requested information by reducing the windows of weakness. Second, encryptions can depict a fine-grained get to strategy utilizing any monotone access structure under properties issued from any picked arrangement of strengths. Third, the key escrow issue is directed by a sans escrow key issuing custom that undertakings the common for the decentralized DTN building arrangement. The key issuing convention makes and issues client riddle keys by playing out a guaranteed two-party estimation (2PC) custom among the key powers with their own lord insider sureness's. The 2PC convention dampens the key strengths from getting any expert question data of each other such that none of them could make the entire arrangement of client keys alone. Along these lines, clients are not anticipated that would thoroughly believe the educating voices recollecting the choosing goal to ensure their information to be shared. The information secret and security can be cryptographically kept up against any inquisitive key powers or information stockpiling focuses in the proposed course of action.

- 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.
- **Backward and forward Secrecy:**With regards to ABE, in reverse mystery implies that any client who comes to hold a characteristic (that fulfills the entrance arrangement) ought to be kept from getting to the plaintext of the past information traded before he holds the property. Then again, forward mystery implies that any client who drops a quality ought to be kept from getting to the plaintext of the consequent information traded after he drops the characteristic, unless the other substantial properties that he is holding fulfill the entrance strategy.

AES calculation is utilized as a solid encryption calculation. As studies shows AES calculation is much more grounded when contrasted with other encryption plans furthermore abuses security issues in Mobile Ad Hoc Networks. 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 confirm the effectiveness of proposed framework in military systems and it ends up being productive than existing plans.

Following figure shows the flowchart of design:

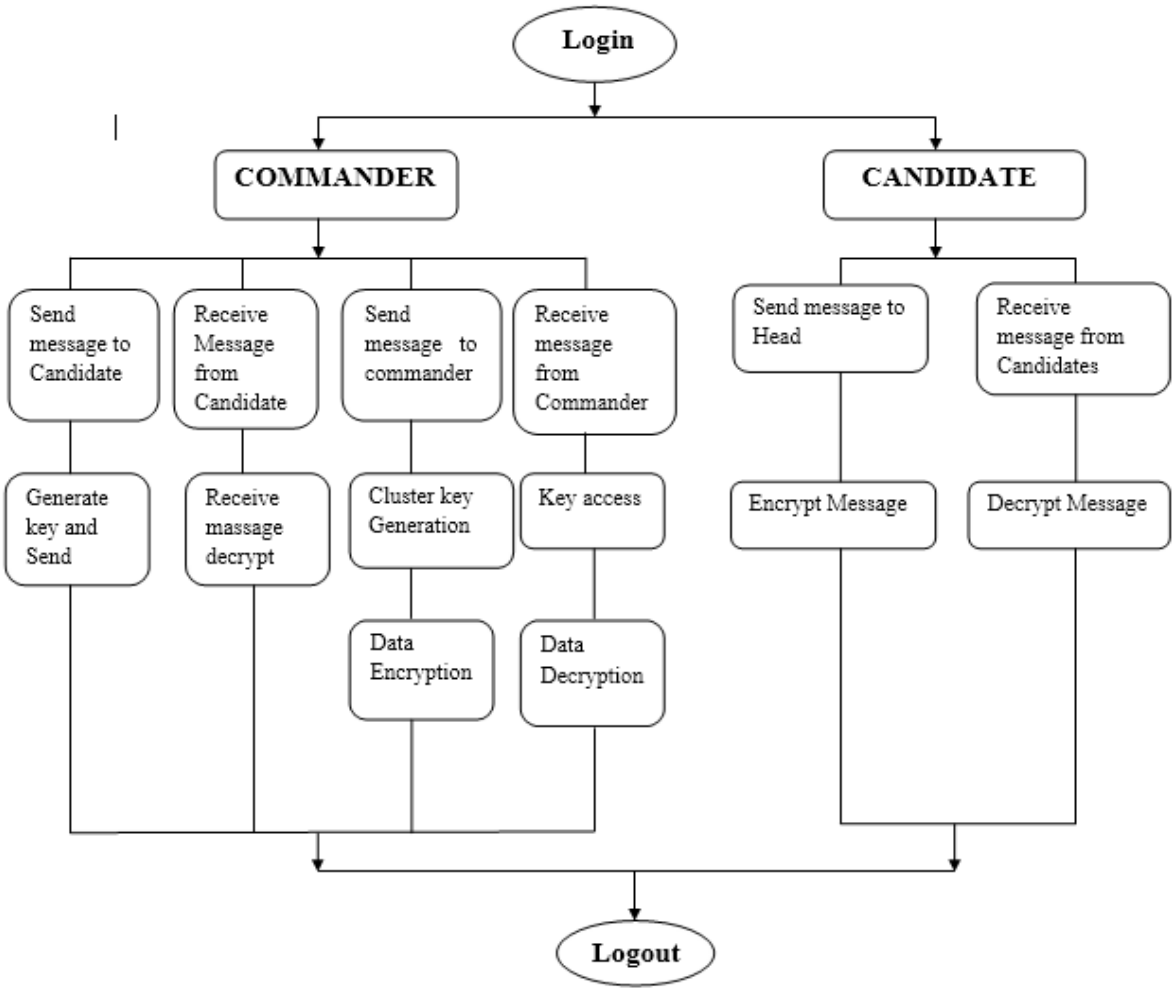

Fig -2: Flowchart of Design

Use Case Diagram

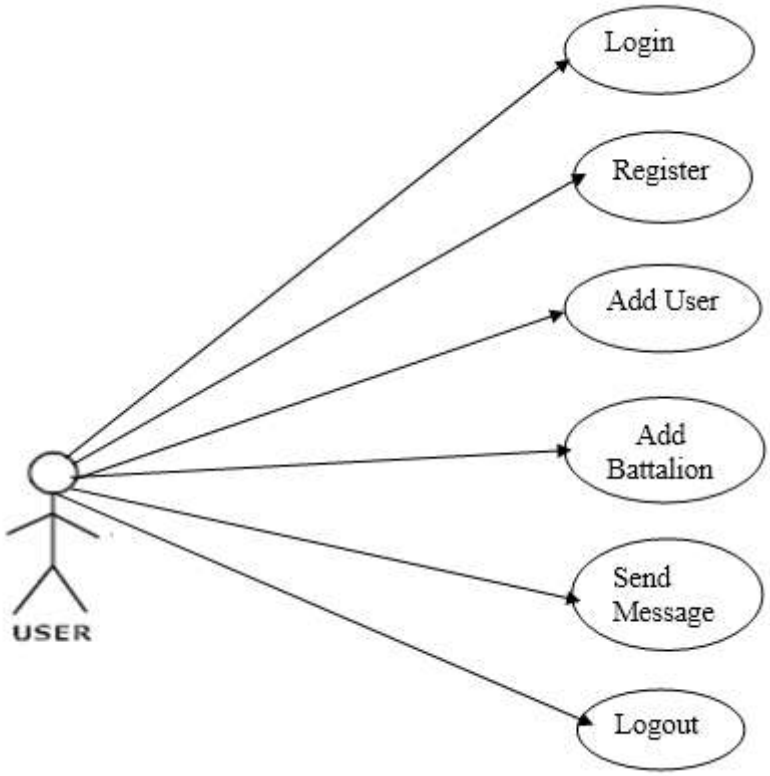

Fig.3 Use Case Diagram

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**

5.3.1 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 era focuses that produce open/mystery parameters for CP-ABE. The key powers comprise of a focal power and numerous nearby powers. We accept that there are secure and solid correspondence channels between a focal power and every neighborhood power amid the underlying key setup and era stage. Every nearby power oversees diverse traits and issues relating credit keys to clients. They concede differential access rights to individual clients taking into account the clients' properties. The key powers are thought to be straightforward however inquisitive. That is, they will sincerely execute the allotted assignments in the framework; nonetheless they might want to learn data of encoded substance however much as could be expected.

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**.**

4.6 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 method for vector quantization, at first from sign taking care of, that is acclaimed for gathering examination in data mining. k-suggests bundling hopes to package n recognitions into k bunches in which each discernment has a spot with the gathering with the nearest mean, serving as a model of the cluster.

The issue is computationally troublesome (NP-hard); in any case, there are capable heuristic figurings that are routinely used and consolidate quickly to a close-by perfect. These are regularly similar to the longing growth computation for mixes of Gaussian courses by method for an iterative refinement approach used by both counts. In addition, they both use bunch centers to demonstrate the data; in any case, k-suggests clustering has a tendency to find bundles of equal spatial degree, while the longing help part allows gatherings to have differing shapes.

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

5. RESULTS AND DISCUSSION

Main Page

Fig.4 Login Form

This is the home page of the system. Using the login screen user can login to the system and if not register user can then click on the register button to open the registration form.

1.4.2 Forgot Password Form

Fig.5 Forgot Password Form

Using this form user can generate a new password for provided email id. The system generates a new password for the given mail id and then sends it to user email Id.

6.4.3 Send messages to Battalion

Fig.6 Message sending to system administrator

1.4.6 Publish Message

Fig.7 Massage is published

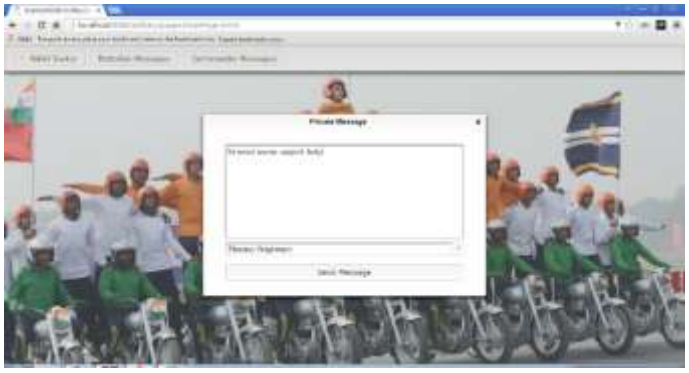

Fig.8 Private massage sent to commander

Fig.9 View commander massage

Time Required For Encryption

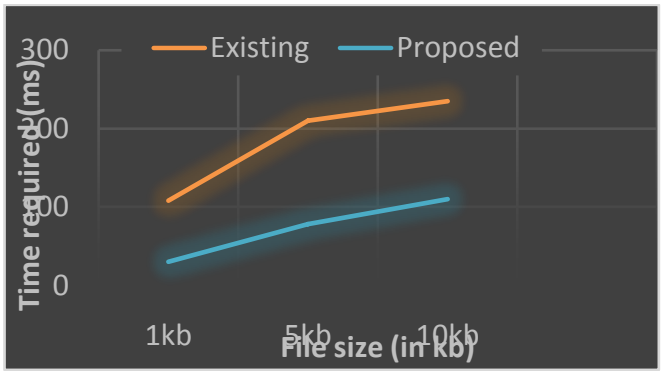

Fig -10: Time Required for Encryption

The above graph shows comparison between proposed system and existing system with respect to File Size (KB) and Transmission Time (ms).

Time required for Decryption

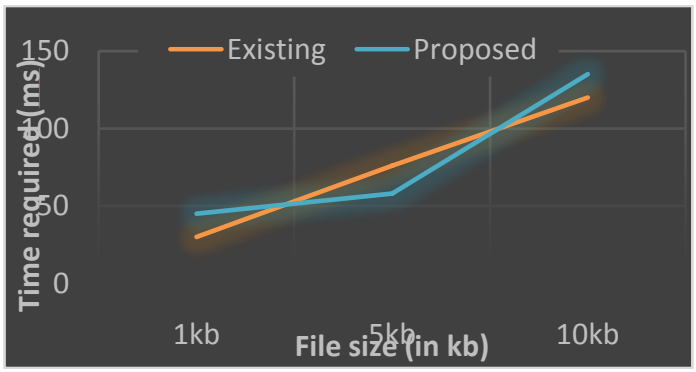

Fig -11: Time required for Decryption

The above graph shows comparison between proposed system and existing system with respect to File Size (KB) and Saved Energy (Joules).

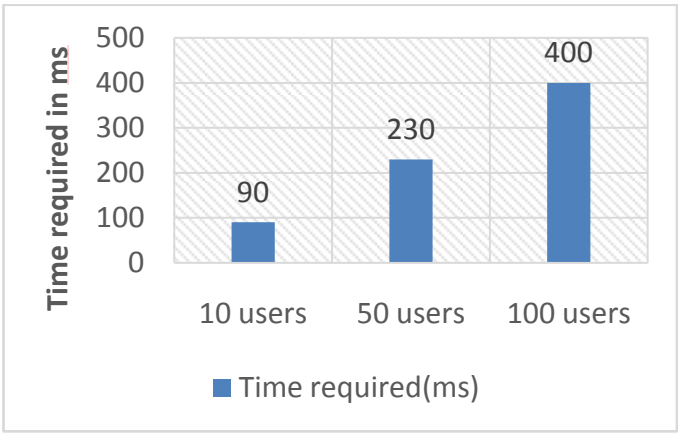

Fig -12: Data Broadcasting

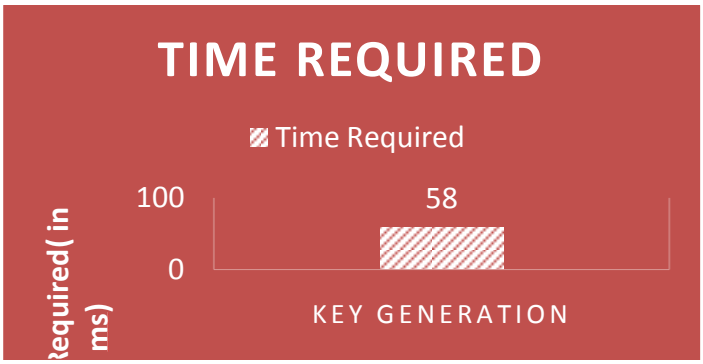

Fig -13: Time required for key generation

6. CONCLUSION AND FUTURE SCOPE

Information security assumes an essential 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 system 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 creates distinctive groups in view of military systems and gives legitimate ON FLY key administration to bunch. The two entomb and intra group 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 productivity of proposed framework in military systems and it ends up being 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 engineering which gives solid security utilizing AES calculation.

Future Scope

In future we plan to give more security to framework utilizing different encryption calculation at ones. We likewise plan to give record sharing element in the framework with the goal that client will have the capacity to share their document. We will likewise get a kick out of the chance to give an additional component of information accessibility which will build unwavering quality of framework regardless of the fact that one of the server crashes. Speedier key era for better security and proficiency. Execution of same philosophy on concentrated systems. Ready to exchange numerous messages and flies at same time.

REFERENCES

[1] JunbeomHur 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.

[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.