ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

ATTRIBUTE BASED SECURE INFO RETRIEVAL FOR DTN

S.Kalpana
ME(AE)
Vivekanandha College of Engineering For Women
Namakkal, India
sadhakalpana@gmail.com

M.Udhayavani
Assistant Professor
Vivekanandha College of Engineering for Women
Namakkal, India
udhram@gmail.com

ABSTRACT: 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 allows wireless devices to communicate with each other and access the confidential information in military applications by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure text and video retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues The Multi authority CP-ABE and AES algorithm it provides secure retrieval of text and video respectively. The proposed system provides secure retrieval of text and video, using modified CP-ABE and AES algorithm the access control issues and Visual Cryptography Schemes (VCS) is a method of image encryption used to hide the secret information in video. Also, demonstrating how to apply the proposed mechanism to securely and efficiently manage the confidential information distributed in the disruption-tolerant military network. It implemented using Network Simulator-2.

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

INTRODUCTION

In many military network scenarios, the transmission of information through network is increasing rapidly, which provides instant access or distribution of digital information, wireless devices connection carried by soldiers can be 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. The different features of DTNs are Fault-tolerant methods and technologies, Electronic attack recovery, Degradation quality from heavy traffic loads and Minimal latency due to unreliable routers. For example, in a disruption-tolerant military network, a commander-in-chief may store confidential information at a storage node, which should be

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

accessed by members of "Battalion 1" who are participating in "Region 2". In DTN architecture where multiple authorities issue and manage their own attributes keys independently.

The concept of attribute-based encryption (ABE)[12] is a trained approach that fulfills the necessities for secure text retrieval in DTNs. ABE features a mechanism that facilitate an access control over encrypted text using access policies and ciphertext's. The attribute based encryption (ABE) in this scheme is having the access control for encryption of data only. Especially, ciphertext-policy ABE (CP-ABE)[3] provides a scalable approach of encrypting text such that the encryptor describes the attribute set that the decryptor desires to possess in order to decrypt the ciphertext. The Revocable multi authority (CP-ABE) is successful technique for encryption and decryption of data.

Visual cryptography is the technique used to transmit the secret information in images called secret image. Visual cryptography is a cryptographic method which allows visual information such as pictures to be encrypted in such a approach that decryption becomes a mechanical operation that does not require a computer. General access structure in VCS[2] for a set of *n* participants, certain qualified subsets of participants can visually recover the secret image, but other, forbidden, sets of participants have no information. The participants in a qualified set will be able to see the secret image without any considerate of cryptography and without performing any cryptographic computation. The advanced encryption scheme is the technique used to transmit the secret video in military application for easily understandable of soldier.

In this technique includes in Bit Stream Extractor (BSE) is used to the data to be found in a stream of bits used in a digital communication. Bit Stream is a series of bytes. Typically each byte is form a range of 256 distinct values. It may be encoded as a sequence of 8 bits in multiple different ways. The Bit Stream Decoder (BSD) is the entire text could then be stored as a bit stream, from which you read 5 bits at a time. The decoder is a device which does the reverse of an encoder, encoding so that the original information can be retrieved.

RELATED WORK

ABE approach in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE[7], the encryptor only gets to tag a ciphertext with a set of attributes. The key authority chooses a guideline for each user that determines which ciphertexts he can decrypt and issues the key to each user by embedding the policy into the user's key. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt secret text under the access structure via encrypting with the corresponding public keys or attributes. V Bozovic and D Socek[5] proposed decentralized CP-ABE designs in the multi-authority network surroundings. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times.
Wireless Sensor Networks have a wide range of applications including environmental monitoring. These networks consist of wireless sensor nodes which are densely deployed to

provide a wider coverage area. The dense deployment of the sensor node provides spatial correlation in the network. In this paper an efficient data gathering approach is implemented by combining the dual prediction and clustering algorithm. Clustering algorithm based on spatial correlation is used to cluster the sensor nodes. Then within the cluster, the nodes send their data to the sink using the Normalized Least Mean Square dual prediction algorithm. Simulation results show that the proposed algorithm reduces the average energy consumption of the network.

M. Naor and Shamir [13] explain the visual authentication and visual identification methods for human users based on visual cryptography. These methods are ordinary and easy to use and can be implemented using simple technology. A Parakh and Kak[1] analyzes the (k, n)-threshold VCS in which the restoration of black pixels is perfect. It provided a construction for (k, n)-threshold VCS for any assessment of n and k with $2 \leq k \leq n$ and it improves pixel expansion. The Proposed EVCS developed by Chang-Chou Lin, Wen-Hsiang Tsai[6] is a category of secret sharing scheme which allows the encoding of a secret image into shares spread to participants.

However, the problem of applying the ABE to DTNs introduces some security and privacy challenges. Since some users may modify their linked attributes at some point like moving their region, or some private keys might be compromised, key revocation or key update for each attribute is essential in order to compose systems secure. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be altered and reallocated to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying process or refuge degradation due to the windows of susceptibility if the earlier attribute key is not updated instantly. The drawback of applying visual cryptography methods is that the secret images can be protected in single information carrier. If it lost once, the information carrier is either damaged or destroyed.

In this paper, we have performed data aggregation on the basis of encryption. We have also proposed an energy efficient method for clustering the nodes in the network in order to retrieve the original image. Initially, sensors sensing the same category of data are placed within a distinct cluster. The remaining unclustered sensors estimate their divergence with respect to the clustered neighbors and ultimately join the least-divergent cluster. The overall performance of our proposed methods is evaluated using NS-2 simulator in terms of average packet drops, delay, and packet delivery ratio and transmission cost and network lifetime. Finally, the simulation results establish the validity and efficiency of our approach and retrieve the original information and video.

PROPOSED WORK

In this section, an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptor can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing 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 each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

We introduce a novel technique named attributes union, which can integrate a certain number of attributes into an attributes union. The core of attributes union is based on an arithmetic theorem. First, each attribute in the universe attributes set will be mapped with a unique prime element. Second, we can represent users' attributes set with the multiply product of all primes corresponding to the attributes in the set. Finally, the access structure can also be represented by attributes union based on the actual situation. We present an example CP-ABE construction with the attributes union, and proof that our construction is still secure against chosen plaintext attacks under the decisional Bilinear Diffie-Hellman assumption. Using attributes union we can also modify almost all existing CP-ABE algorithms and reduce their storage and computational overhead. The advanced encryption scheme is used to retrieve the original video by using the visual cryptography method in order to retrieve the original image, adding of all images in this form of video.

Issues such as scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. For improving the limitations of the above technique. We propose a new scheme called Revocable Multiauthority ciphertext policy attribute based encryption. Revocable Multiauthority ciphertext policy attribute based encryption scheme and AES scheme describes text and video retrieval with efficient revocation. This mechanism to securely and efficiently manage the confidential information distributed in the disruption-tolerant military network.

Fig. 1 shows the architecture of the DTN. The architecture consists of the following system entities.

Fig. 1. Architecture Diagram of Secure Data Retrieval

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

Storage Node : The user will upload some data's in the User Page. The system will calculate size of the file and sends through Storage node. Therefore storage node can get the data without traffic and also transmit the data in less time. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme. This is an entity that stores data from senders and provide corresponding access to users. Assume the storage node to be semi trusted, that is honest-but-curious.

Store Carry and Forward: 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. 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 ciphertext and obtain the data.

Decentralized User: Multiauthority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Communicate with every user in network.

The concept of CP-ABE is

• Private key assigned to "attributes"
• Cipher text associated with "access policy"
• Can decrypt only when attributes satisfy policy.

Central key Authority:

1. Choose a random exponent βϵ R Z*p.

Let h=g β

2. Masters (secret key)/public key

PKCA=h MKCA=β.

$PK_{CA}=h=g^{\beta}$ (1)

$MSK_{CA}=\beta$ (2)

Local Key Authority

1. Choose a random exponent αiϵ R Z*p.
2. Masters (secret key)/public key pair is

PKAi=e (g,g)αi,MK Ai=αi.

$PK_{AA} = e(g,g)^{\alpha}$ (3)

$MSK_{AA}= \alpha$ (4)

An efficient and secure data retrieval method using CP-ABE is used for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

hostile environment where key authorities local and central might be compromised or not fully trusted.

Key Generation: (MK, L): The key generation algorithm runs by CA. It takes as input the Master key of CA and the set of attributes L for user, then generate the secret key SK.

A).Algorithm for Key Generation: A trusted party chooses and publishes a (large) prime *p* and an integer *g*having large prime order in F*p
1. Select a large prime number p.
i. Choose a secret integer a.
ii. Compute A ≡ ga(mod p).
iii. Choose a secret integer b.
iv. Compute B ≡ gb(mod p).
2. Masters (secret key)
Compute the number Ba(mod p). Compute the number Ab(mod p).
The shared secret value is Ba ≡ (gb)a ≡ gab ≡ (ga)b ≡ Ab(mod p).
Data Encryption: Here when a sender wants to deliver its confidential data M, he defines the tree access structure T over the universe of attributes L, encrypts the data under to enforce attribute-based access control on the data, and stores it into the storage node.
The encryption algorithm takes as input the message M, public parameter PK and access structure A over the universe of attributes. Generate the output CT such that only those users who had valid set of attributes that satisfy the access policy can only able to decrypt. Assume that the CT implicitly contains access structure A. Data Decryption: When a user receives the ciphertext from the storage node, the user decrypts the ciphertext with its secret key. The decrypt algorithm run by user takes input the public parameter, the ciphertext CT contains access structure A and the secret key SK contain of user attribute set S. If S satisfies the access tree then algorithm decrypt the CT and give M otherwise gives "ϕ". Key Update (MK, SK, old value, new value): The key updating algorithm runs by CA. It takes as input the master key of CA, old SK and old attribute value old value, and then updates the secret key SK by updating (add/delete/update) old value with new value.

B). CP-ABE for Data Retrieval
We provide a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority Issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Data confidentiality on the stored the data against unauthorized users can be trivially guaranteed.

genkeys ($k_{A\ secret}$, $k_{A\ public}$)
genkeys ($k_{B\ secret}$, $k_{B\ public}$)
sharedsecret = curve25519($k_{B\ secret}$,$k_{M\ public}$)
k_{aes} = SH A256(sharedsecret)
AES_set_encrypt_key(k_{aes},256,$k_{aes\_expanded}$)
For(i = 0;i<40;i+ = 4)
Secretinfo[counter] = AES_encrypt(secretin fo[counter],$k_{aes\_expanded}$)

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

ENCRYPTION: When sender wants to convey its confidential data *M* to user, he defines the tree access structure *T* over the universe of attributes *L*, encrypts the data under to enforce attribute-based access control on the data, and stores it into the storage node. The encryption algorithm takes as input the message *M*, public parameter *PK* and access structure *A* over the set of attributes. Generate the output *CT* such that only those users who had valid set of attributes that satisfy the access policy can only able to decrypt. Assume that the *CT* perfectly contains access structure *A*.

$$Encrypt(PK, (T, \rho), M) \rightarrow CT$$

CT can be derived from following equation,

$$CT = \{T, C = M(\prod e(g,g)^{\alpha_d})^s, c' = h^s, c_x = h^{A_x}\left(T_{\rho(x)}\right)^{-r_x}, c'_x = g^{r_x} \quad \forall x \in \{1,2 \dots, l\}, \ \forall d \in \{1,2, \dots . D\}\} \qquad \textbf{(5)}$$

where *C* can be computed from

$$C = M(PK_{AA_1}, PK_{AA_2}, PK_{AA_3}, \dots ., PK_{AA_D})^s \qquad \textbf{(6)}$$

After the construction of *CT*, the sender stores it to the storage node securely. On getting any data request query from a user, the storage node reacts with *CT* to the user. It is essential to make a note of that the sender can describe the access policy under attributes of any chosen set of multiple authorities without any restrictions on the logic expressiveness as opposed to the previous multi-authority schemes.

DECRYPTION: When a user receives the ciphertext from the storage node, the user decrypts the ciphertext with its secret key. This deterministic algorithm runs by a user. Takes input as cipher-text *CT*, which was encrypted under attribute set *T* and decryption keys *SK* for an attribute set. The final output will be a message *M*. Without loss of generality, we suppose that a user *U* performs the decryption algorithm. If *x* is a leaf node, then define as follows.

$$Decrypt(PK, CT, S) \rightarrow M$$

M can be computed from

$$\prod_{d=1 \text{ to } D} \frac{\prod_{\rho(x)\epsilon s}\left(e(c_x, L_{UI,d}) e(c'_x, K_{\rho(x),UI,d})\right)^{w_x}}{e(c', K_{UI,d})} = \prod_{d=1 \text{ to } D} \frac{1}{e(g,g)^{\alpha_d s}} \qquad \textbf{(7)}$$

where constants $\{w_x\}$ satisfy

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

$$\sum_{x \in I} w_x A_x = (1,0, \dots 0)$$

The decryption algorithm begins by calling the function on the root node of access tree. Observe that $Decrypt(PK, CT, S) = e(g,g)^{\alpha_d s}$ if the tree T is satisfied by $\wedge$ for all $\lambda_x \epsilon \wedge$. When

set $A = Decrypt(PK, CT, S) = e(g,g)^{\alpha_d s}$, the algorithm decrypts the ciphertext by computing

$$\frac{C}{(e(c', K_{att,UI,d})/A)} = M \qquad \textbf{(8)}$$

KEY UPDATE: When a user comes to hold or drop an attribute, the corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively. The key update procedure is launched by sending a join or leave request for some attribute group from a user who wants to hold or drop the attribute to the corresponding authority. On receipt of the membership change request for some attribute groups, it notifies the storage node of the event. Without loss of generality, suppose there is any membership change (e.g., a user comes to hold or drop an attribute at some time instance).

It takes as input the *SK*, the old attribute value, the new attribute value and parameters of *CA*. It gives output as updated Secret Key of user. Then, the update procedure progresses as follows.

(1) User provides document for new attribute value and give his $SK_{CA.}$
(2) *CA* verifies the document and assigns the generation work of new *SK* for users to *AA*.
(3) AA checks for particular attribute in *SK*, if found at *i* then replace with new attribute and generate C_i, C'_i. Put them into *SK* of user and regenerate the new *SK*.
(4) If user wants to add new attribute then *AA* generate C_{new} and C'_{new} for that attribute value and generate *SK*.
(5) Finally, *AA* and *CA* outputs new *SK* for users.

$$CT' = \{T, C = M(\prod e(g,g)^{\alpha_d})^{s+s'}, c' = h^{s+s'}, c_x = h^{A_x}\left(T_{\rho(x)}\right)^{-r_x}, c'_x = g^{r_x} \quad \forall x \in \{1,2 \dots, l\}, \ \forall d \in \{1,2, \dots D\}\} \qquad \textbf{(9)}$$

When a user sends a request query for the data, the storage node responds with the newly updated and ciphertext encrypted under the reorganized keys.

A) VISUAL CRYPTOGRAPHY AND ADVANCED ENCRYPTION SCHEME

GENERATION OF SHARES: The algorithm initiates to find a solution for the given GAS by the access structure with an early set of participants and number of participants in Step 1 and 2.Here, n is the number of shares and n' is the number of participants.

INPUT: Set of participants P= $\{i_1, i_2, \dots, i_n\}$ and an access structure (T_{Qual}, T_{Forb})

OUTPUT: Constructed qualified shares $\{S_1, S_2, \dots, S_n\}$

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

METHOD:

STEP 1: Sender set the number of participants P= $\{i_1, i_2,\ldots,i_n\}$.

STEP 2: The qualified and forbidden set has to be declared.

STEP 3: The secret image is splitted into the number of shares as mentioned.

If $m=n_{max}$ then Stop and Output "No solution found" Else

$C \leftarrow C_{best}$

Until m←m-1

STEP 4: Until the number of shares 'n', the share synthesizer generates the shares

STEP 5: The generated share is sent to the embedding process.

After getting the secret image, share synthesizer generates the number of shares as per the number of participants and the password validation is used for the security concerns. Then, the protected shares are sent it to the embedding process.

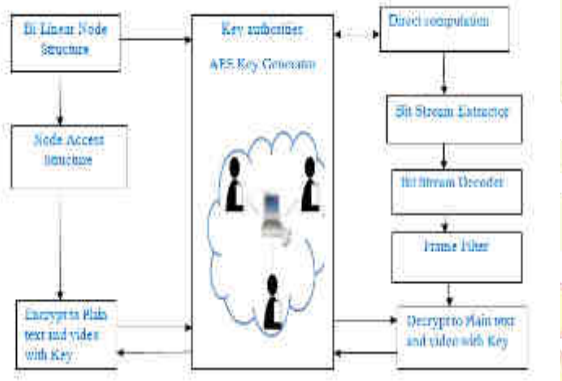

Figure 2. Architecture Diagram for secure video retrieval

The VCS includes, Embedding process involves embedding the binary image with the covering shares. For that, the covering shares can be divided into the blocks which contain the sub pixels each. The input for the embedding process is the covering shares assembled to the consequent VCS with the covering images necessary.

INPUT: Shares and covering images

OUTPUT: Embedded image

METHOD: Procedure Stamping (shares, cover images)and Advanced Encryption Scheme(AES)

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

In this Fig2 the bilinear node structure produces the bilinear form on a vector space. It can be extended to include modules over a commutative ring with linear maps. Node access structures are devices on a large network. The larger data structure such as linked with list data structure. The Advanced Encryption Scheme is includes in direct computation (DC),it supports the general purpose computing on graphics processing units.

An encoder is a device, circuit, transducer, and software program, algorithm that converts in formation from one format (or) code to another for the purposes of standardization, speed, secrecy and security.

SIMLULATION AND RESULTS

The proposed system Access control and Secure data retrieval based on CP-ABE implemented in NS2Simulator.
Here we perform access control and secure data retrieval by CP-ABE as well as the secure video retrieval in order to reduce the routing overhead, packet delivery ratio and End to End delay by using the Advanced Encryption Scheme(AES). and in Fig. 3 shows the plotted graph.

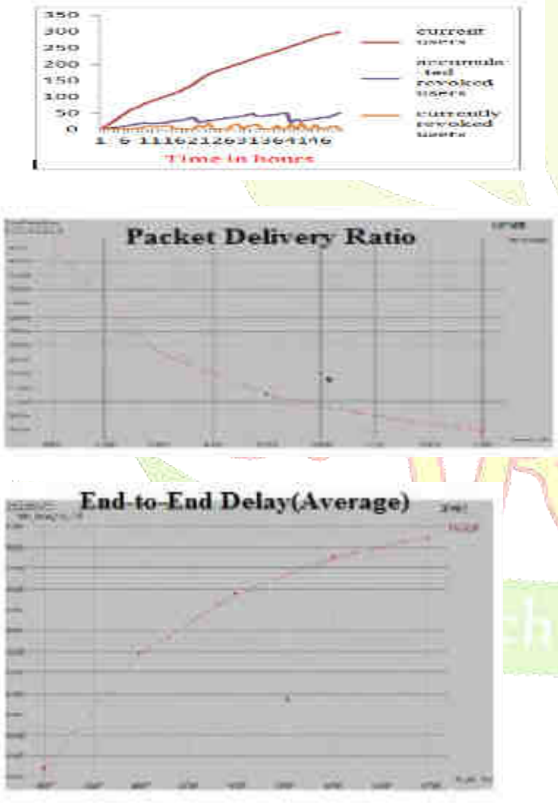

Figure 3.Number of users in an attribute group and performance graph

Since each attribute group can be shown as an independent network multicast group where the members of the group share a common attribute, we show the simulation result following this

probabilistic behavior distribution. The Packet Delivery Ratio (PDR) and End to End delay is reduced by using the Advanced Encryption Scheme (AES).

CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. Disruption Tolerant Network Technologies are challenging solution for end to end communication between wireless devices. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. The proposed Revocable Multiauthority Ciphertext Policy Attribute Based Encryption and Modified General Access Structure Algorithm is an efficient and secure information retrieval method for decentralized DTNs where multiple key authorities manage their attributes independently. In addition, the fine grained key revocation can be done for each attribute group and image also be retrieved by visual cryptography and advanced encryption schemes which is enhanced. In the proposed system, data confidentiality on the stored data in storage node against unauthorized users can be assured, which improves performance and reduce communication cost.

REFERENCES

1. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks IEEE transactions on networking vol:22 no:1 year 2014.

2. Changji Wang and Jianfa Luo,‖ An Efficient Key-Policy Attribute- Based Encryption Scheme with Constant Ciphertext Length‖, Received 21 January 2013; Accepted 16 March 2013.

3. JunbeomHur,"Improving Security and Efficiency in Attribute-Based Data Sharing", in IEEE Transactions on Knowledge And Data Engineering, VOL. 25, NO. 10, OCTOBER 2013.pp.2271-2282.

4. V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, "Multiauthority attribute-based encryption with honest-but-curious central authority" International Journal of Computer Mathematics, vol. 89,pp. 3,2012.

5. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2011.

6. [12] JunbeomHur and Dong Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems" IEEE Transactions On Parallel And Distributed Systems, Vol. 22, NO. 7, JULY 2011,pp.1214-1221.

7. Dr. M.Newlin Rajkumar, Ancy George, Brighty Batley C," An Overview of Multi-Authority Attribute Based Encryption Techniques".

8. Lewko, A., Waters, B.: ―Decentralizing Attribute-Based Encryption‖, In: CRYPTOLOGY ePrint Archive, Report 2010/351,2010.

9. M. Chase and S. S. M. Chow, "Improving privacy and security inmultiauthority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.

10. Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009.

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

12. Abhishek Parakh and Subhash Kak "A Recursive Threshold Visual Cryptography Scheme", CoRR abs/0902.2487: (2009).

13. S. S.M. Chow, "Removing escrow from identity-based encryption," in Proc. PKC, 2009, LNCS 5443, pp. 256–276.

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

15. J. Bethencourt and others. Ciphertext-policy attributebased encryption. In Proceedings of IEEE SP, Oakland, 2007.

16. Dr. M.Newlin Rajkumar, Ancy George, Brighty Batley C, An Overview of Multi-Authority Attribute Based Encryption Techniques‖2007.

17. M. Chase, "Multi-authority attribute based encryption," in Proc. TCC, 2007, LNCS 4329, pp. 515–534.