Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 297-302, 2016
ISSN 1990-9233;

DOI: 10.5829/idosi.mejsr.2016.24.TAET23541

Retrieving Data Securely in Disruption Tolerant Military Networks

[1]R. Saranya, [2]L. Malathi and [3]S. Sneha

[1]PG Scholar, Department of CSE,
Vivekanandha College of Engineering for Women, Tamilnadu, India
[*2]Assistant Professor, Department of CSE, Vivekanandha College of
Engineering for Women, Tamilnadu, India
[*3]PG Scholar, Department of CSE, Vivekanandha College
of Engineering for Women, Tamilnadu, India

Abstract: Disruption Tolerant Network technologies allow wireless devices carried by soldiers in military networks and access the confidential information by storage nodes. Data to be stored and retrieved from storage nodes, since the data handled by the soldiers are different, it is necessary to implement the security policy and access control policy to them. The authorization policies and secure data retrieval by soldiers are the key issues in DTN. Ciphertext Policy Attribute Based Encryption is a cryptographic resolution to the access control issues and fulfills the necessities for secure text retrieval in DTNs. To transmitting the secret image in DTN, Visual Cryptography Schemes are used. These schemes are used to hide the secret information in images. To support both text and image retrieval in DTN, the proposed algorithm can be enhanced. However, previous approach suffers attribute revocation problem in information, pixel expansion and noise problem in images. The proposed system provides secured retrieval of text and image, using Multiauthority CP-ABE with Data Revocation and customized GAS algorithm for decentralized disruption tolerant military network respectively. On demonstrating the proposed system, the private information is secured and efficiently managed in Disruption Tolerant Military Network.

Key words: Access control · Attribute-based encryption (ABE) · Disruption-tolerant network (DTN) · Multi-authority · Secure information retrieval

INTRODUCTION

Recently, the transmission of information through network is increasing rapidly, which provides direct access or distribution of digital information. The outgrowing commercial environment such as military, each and everything based on the sources to televise the information strongly and maintain the information as well in the regular standard.. The shield of confidential data in military relevance is mandatory including access control methods.

Disruption-tolerant network (DTN) is a technology for transferring texts and images in military network. Roy and Chuah [1] introduced storage nodes in DTNs where data is stored or imitated such that only specialized mobile nodes can right to use the essential data rapidly and efficiently. In many cases, data access policies are defined over user attributes, which are organized by the key authorities. In DTN[2] architecture where multiple authorities issue and handle their own attribute keys autonomously. The conception of attribute-based encryption (ABE) [3, 4] is a qualified approach that executes the necessities for secure text retrieval in DTNs. ABE features a mechanism that assist an access control over encrypted text using access policies and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) [5, 6] 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.

Visual Cryptography [7] 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.

Corresponding Author: R. Saranya, PG Scholar, Department of CSE,
Vivekanandha College of Engineering for Women, Tamilnadu, India.

General access structure in VCS [8, 9] 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 can see the secret image without any considerate of cryptography and without performing any cryptographic computation.

Although DTNs were originally imagined for interplanetary use, they may have a far greater number of applications on Earth. The possible applications are Space Agencies, Military and Intelligence, Public Service and Safety, Personal Use, Environmental Monitoring, Engineering and Scientific Research. The real time applications of VCS are biometric security, printing and scanning applications, Bank customer identification, Steganography, etc.

Related Work: DTN provides connectivity in Heterogeneous networks which lack continual connectivity due to disruptions or considerable delays in mobile or extreme terrestrial environments or planned network in military [10, 11].

ABE [12, 13] approach in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE [14], the encryptor only gets to tag a ciphertext with a set of attributes. The key authority chooses a guideline for each user that determines the ciphertexts that to be decrypt and issues are embedded the policy into the user's key. CP-ABE 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 [15, 16] proposed decentralized CP-ABE designs in the multi-authority network surroundings. By encrypting data for multiple times, a combined access policy is achieved over the attributes issued from different authorities.

M. Naor and B. Pinkas [17, 18] explain the visual authentication and visual identification methods for human users based on visual cryptography. Parakh and Kak[19] analyzes the (k, n)-threshold VCS in which the restoration of black pixels is perfect which provides a construction for (k, n)-threshold VCS for any assessment of n and k with 2 = k = n and it improves pixel expansion. The Proposed EVCS developed by Feng Liu and Chuankun Wu is a category of secret sharing scheme allows an 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. The user may modify their linked attributes such as region moving or can be compromised with some private keys, key revocation or key update for each attribute is essential compose secure systems which imply the revocation of any attribute. For any single user, an attribute group affects the other users in the group. The drawback of applying visual cryptography methods is that the secret images can be protected in single information carrier. If one is lost, then the information carrier is either damaged or destroyed. Generally, meaningless shares are used in VCS, it might invite the adversary concern. Each share of image gets affected in terms of visual effect by the content of other shares.

Proposed System: In this section, the proposed scheme concentrates on both text and data retrieval in DTN. To securely transmit a text, Multiauthority CP-ABE with Information Revocation is proposed to overcome attribute revocation problem. For transmitting images, C-GAS Algorithm is proposed to overcome pixel expansion and noise problem in DTNs. Each local authority issues a partial personalized and an attribute key components to a user with secure 2PC protocol along with the central authority. Each attribute key of a user can be updated individually and immediately shows in Fig 1. The proposed scheme features includes achievements such as an immediate attribute revocation enhances backward/forward secrecy of confidential data by decrease of windows vulnerability. Then, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the 2PC protocol detects the key authorities with the obtained master secret information of each other. Among that none of them generates the whole set of user keys alone. Forth, images send by sender stored in storage node can be retrieval by general Access Structure with Stamping and Synthesizing Algorithm. The data confidentiality and privacy are enforced cryptographically against any curious key authorities or data storage nodes in the proposed scheme. Thus, in the proposed method, the scalability and security are enhanced.

Text Retrieval – Mcpabe with Ir

Key Setup:

Central Key Authority: This key authority chooses a random exponent $\alpha \in_R Z_p^*$. It generally sets $h=g^{\alpha}$. The public key (PK) and master secret key (MSK) of central key authority is given by

$PK_{CA}=h= g^{\text{▾▾}}$ (1)

MSK_{CA} = ▾▾ (2)

Attribute Key Authority: Each *AA* chooses a random exponent ▾▾ $\square_R Z^*_p$. The public key (PK) and master secret key (MSK) of attribute key authority is given by

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

MSK_{AA}= ▾▾ (4)

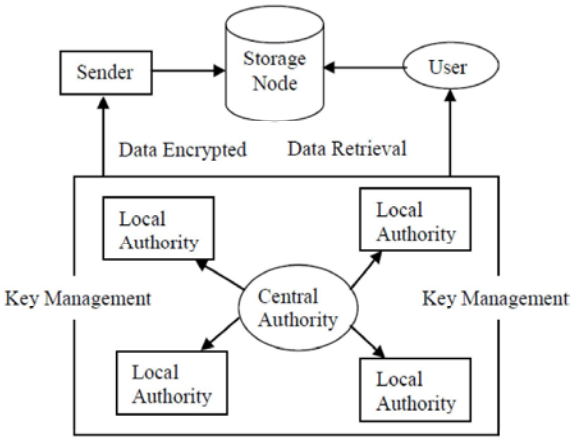

Fig. 1: Information Retrieval Architecture

Key Generation and Distribution: In CP-ABE, single personalized key and multiple attribute key are derived from user secret components. To preventing collusion attack among users, personalized key is exclusively determined for each user with different attributes.

Central Key Generation: This randomized algorithm runs by a central authority. Takes input as master secret key MSK_{CA} and a user's information *UI* and output as secret key *SK* for the user.

$CKeyGen(UI,d) \rightarrow (K_{UI,d}, L_{UI,d})$ (5)

From the equation **(5)**, the following terms are derived

$K_{UI,d} = g^{\alpha_d} h^{r_{UI,d}} R_0$

$L_{UI,d} = g^{r_{gid,d}} R'_0$

Attribute Key Generation: This randomized algorithm runs by an attribute authority. Takes input as authority's secret key MSK_{AA}, the authority's value σ, a user's information *UI*. Output as secret key SK_{AA} for user.

$AKeyGen(\{L_{UI,d}, \sigma_{UI,d} | d = 1,2,\dots D\}, att) \rightarrow \{K_{att,UI,d}\}$ (6)

From the equation (6), the following terms are derived

$K_{att,UI,d} = L_{UI,d}^{s_{att}} R_{att,UI,d}, \quad d = 1,2,\dots,D$

$K_{att,UI,d} = (g^{r_{gid,d}} R'_0)^{s_{att}} R_{att,UI,d}$

Encryption: The input message M is taken for the encryption algorithm, 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,

$CT = \{T, C = M(\prod e(g,g)^{\alpha_d})^s, c' = h^s, c_x = h^{A_x}(T_{\rho(x)})^{-r_x}, c'_x = g^{r_x} \quad \forall x \in \{1,2\dots,l\}, \forall d \in \{1,2,\dots.D\}\}$ (7)

where *C* can be computed from

$C = M(PK_{AA_1}, PK_{AA_2}, PK_{AA_3}, \dots., PK_{AA_D})^s$ (8)

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*.

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

M can be computed from

$$\prod_{d=1 \text{ to } D} \frac{\prod_{\rho(x)\in S}\left(e(c_x, L_{UI,d}) e(c'_x, K_{\rho(x),UI,d})\right)^{w_x}}{e(c', K_{UI,d})} = \prod_{d=1 \text{ to } D} \frac{1}{e(g,g)^{\alpha_d s}} \quad (9)$$

where constants $\{w_x\}$ satisfy

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

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 ^ for all λ_x $\square$ ^.

$$\frac{C}{(e(C',K_{att,UI,d})/A)} = M \quad (10)$$

Key Update: When a user comes to hold or drop an attribute, the corresponding key must be updated for preventing the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively.

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.

- User provides document for new attribute value and give his $SK_{CA.}$
- *CA* verifies the document and assigns the generation work of new *SK* for users to *AA*.
- 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*. If user wants to add new attribute then *AA* generate C_{new} and C'_{new} for that attribute value and generate *SK*.
- Finally, *AA* and *CA* outputs new *SK* for users.

$$CT' = \{T, C = M(\prod e(g,g)^{\alpha_d})^{s+s'}, c' = h^{s+s'}, c_x = h^{A_x}\left(T_{\rho(x)}\right)^{-r_x}, c'_x = g^{r_x} \quad \forall x \in \{1,2\ldots,l\}, \ \forall d \in \{1,2,\ldots,D\}\} \quad (11)$$

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.

Image Retrieval - Customized Gas in Visual Cryptography

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= $\{i_1, i_2,\ldots,i_n\}$ and an access structure (T_{Qual},T_{Forb})

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

Once the secret image is obtained, 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.

Embedding Process: This process involves an embedding of the binary image with the covering shares. For that, the covering shares can be divided into the block which contain the sub pixels each. The input for the embedding process covers the 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)

The cover images are selected to embed the generated shares with the cover images. Now, the shares are turned into meaningful shares. The created shares are preferred to embed the covering images with the shares. And then it is broadcasted to the receiver side. The output of this process be the embedded shares which are more secure and tough to find and hack by the hackers.

Recover Images Figures and Tables: The embedded cover images are extracted and secret shares are done. By loading the shares in the accurate sort will get an original secret image is done. At the receiver side they the shares are stack with the logical or operation and an original secret image is extracted. The prettiness of such a scheme is that a set of qualified participants is able to improve the secret image.

INPUT: Embedded images

OUTPUT: Secret image

METHOD: Extraction Process

The embedded images are stored in the Embedded Images folder. It is used while the extraction operation is performed. At receiver side, the covering images are extracted from the embedded images after accepting the correct password. The extracted shares extracted from the embedded images and stored in the extracted images folder.

Simulation and Results: In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Fig.2 shows the total communication cost that the sender or the storage node needs to send on a association change in each multi-authority CP-ABE scheme. It includes the ciphertext and rekeying messages for non-revoked users. It is measured in bits. In this simulation, the total number of users in the network, attributes and ket are 10,000, 30 and 10 respectively.

The average number of attributes associated with a user's key is 10. The communication cost in HV is less than RC in the beginning of the simulation time. The proposed scheme requires the least communication cost in the network system since the rekeying message in is comparatively less than the other multi-authority schemes.

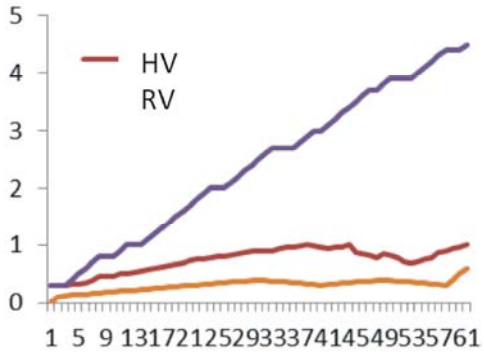

Fig. 2: Communication cost in RM-CPABE System

Table-2 summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the key authority or the storage node needs to send to update non-revoked user's keys for an attribute. Private key size represents the storage cost required for each user to store attribute keys or KEKs. Public key size represents the size of the system public parameters. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its ciphertext size is linear to the number of revoked users in the system since the user revocation message is included in the ciphertext. The proposed scheme requires a user to store more KEKs than HV. However, it has an effect on reducing the rekeying message size. The proposed scheme is as efficient as the basic HV in terms of the ciphertext size while realizing more secure immediate rekeying in Multiauthority systems.

In this section, the existing HVCS is compared with the proposed C-GAS algorithm. The values related to the images are tabulated in the Table 1, which describes a image memory size and dimensions of an images. The five secret images are analyzed in this section. In HVCS, the two shares are split up and stacked to retrieve an original secret image. But by using the C-GAS algorithm, the secret image can be split up into four shares and the secret image can be retrieved with high resolution. The graph shows the variance in between the HVCS and C-GAS algorithm. Higher the memory size leads to high resolution. By comparing the values of Halftone Visual cryptography Schemes (HVCS) with Customized General Access Structures (C-GAS), it is realized that the values of original image resolution is comparatively higher after using the C-GAS algorithm cryptography schemes as shown in Table 1. The graphical representation gives the higher curve in C-GAS shows the higher resolution can be shown in the figure 3. This can also increases the security and the number of shares produced.

Table 1: Comparison between existing and proposed system

	Memory Size		
Secret Image Sharing	HVCS	M-GAS	Dimensions
One	0.866 KB	4.11 KB	344*147
Two	0.934 KB	6.87 KB	478*147
Three	3.77 KB	8.91 KB	568*177
Four	4.08 KB	14.7 KB	720*140
Five	33.2 KB	45.3 KB	1000*369

Table 2: Efficiency Analysis for RM-CPABE

System	Re-keying message	Private keysize	Public keysize
HV	$l(2k+1)c_0$	$(2k+m)c_0$	mc_1+mc_0
RC	0	$(3k+2m)c_0$	$m(t+4)c_0+mc_1$
Proposed	$(n-l)\log c_p \frac{n}{n-1}$	$(2k+1)c_0+\log nc_k$	mc_1+c_0

where C_0 : bit size of an element in G_0, C_1 : bit size of an element in G_1, C_k: bit size of KEK, l-no.of users in attribute group, n-no. of all users in system, m: the number of authorities in system,c_p: bit size of element in Z^*_p.

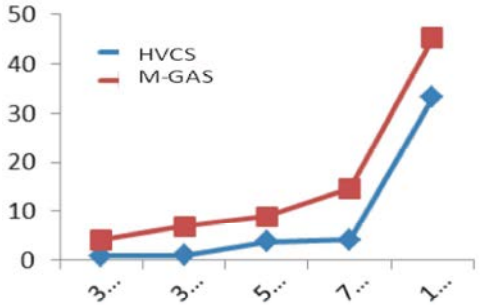

Fig. 3: Representation of HVCS with M-GAS

Conclusion and Future Work: Secure retrieval of text and image is very important as for as DTN is concerned. 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 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 of computation. In future enhancement, location of node may also be identified using geographical routing protocol, which reduce communication cost.

REFERENCES

1. Junbeom Hur and Kyungtae Kang, 2014. Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks, IEEE/ACM Transactions On Networking, 22(1).
2. Roy, S. and M. Chuah, 2009. Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs, Lehigh CSE Tech. Rep., 2009.
3. Goyal, V., O. Pandey, A. Sahai and B. Waters, 2006. Attribute-based encryption for fine-grained access control of encrypted data, in Proceedings of the 13th ACM Conference on Computer and Communications Security, pp: 89{98, 2006}.
4. Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, 2009. AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption, July 27, 2009.
5. Bethencourt, J., A. Sahai and B. Waters, 2007. Ciphertext-policy attribute based encryption, in Proc. IEEE Symp. Security Privacy, pp: 321-334.
6. Saranya, R., L. Malathi and S. Sneha, 2015. A Survey On ABE Schemes For Disruption Tolerant Networks, in Journal of Engineering And Technology Research, 3(6): 1-7.
7. Moni Naor and Adi Shamir, 1995. Visual cryptography. In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, (950): 1-12.
8. Bharanivendhan, N. and T. Amitha, 2014. Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm, International Journal of Computer Applications (0975-8887) 92(8).
9. Ateniese, G., C. Blundo, A. DeSantis and D.R. Stinson, 1996. Visual cryptography for general access structures, Proc. ICAL 96, Springer, Berlin, pp: 416-428.
10. Fall, K., 2003. A Delay-Tolerant Network Architecture for Challenged Internets, in Proceedings of ACM SIGCOMM, 2003.
11. Vaishali S. Raj and Dr. R. Manicka Chezian, 2013. DELAY –Disruption Tolerant Network (DTN), its Network Characteristics and Core Applications, International Journal of Computer Science and Mobile Computing, 2(9): 256-262.
12. Boneh, D. and M. Franklin, 2003. Identity-based encryption from the weil pairing, in SIAM Journal of Computing, 2003.
13. Chase, M. and S.S.M. Chow, 2009. Improving privacy and security in multi authority attribute-based encryption, in Proc. ACM Conf. Comput.Commun. Security, pp: 121-130.
14. Changji Wang and Jianfa Luo, 2013. An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length, Received 21 January 2013; Accepted 16 March 2013.
15. Bozovic, V., D. Socek, R. Steinwandt and V.I. Villanyi, 2012. Multiauthority attribute-based encryption with honest-but-curious central authority, International Journal of Computer Mathematics, 89: 3.
16. Junbeom Hur and Dong Kun Noh, 2011. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems, IEEE Transactions On Parallel And Distributed Systems, 22(7): 1214-1221.
17. Naor, M. and B. Pinkas, 1997. Visual authentication and identification, Springer-Verlag LNCS, 1294: 322-336.
18. Tsai, D.S., T. Chenc and G. Horng, 2008. On generating meaningful shares in visual secret sharing scheme, Imag. Sci. J., 56: 49-55.
19. Ms Ranjani, R. and Mrs L. Malathi, 2014. SIP Flooding Attack Detection Using Hybrid Detection Algorithm" in "International Journal of Modern Trends in Engineering Research, 01(05).