Secured Lossless Data Transmission in Armed Force Networks using CPABME Methodology

Pandit Samuel[1], N.Aditya Sundar[2], Prof . Ch.Suresh[3]
[12]Assistant Professor, [3]Professor,
Department of Information Technology,
[123]Anil Neerukonda Institute of Technology & Sciences – (ANITS)
Sangivalasa – 531162, Bheemunipatnam (Mandal), Vishakapatnam (District)
Andhra Pradesh, India

Abstract- Mobile nodes In military(armed forces) ecosystems, such as in Antagonistic regions, may face some difficulties from interruptions during continuous flow of data in particular time span. One of the effective technologies is disruption tolerant networks that allow cordless devices which are handled by the cadets or soldiers to transmit information with each other in the same or neighboring regions. This confidential information can be accessed securely by the soldiers by exploiting external storage nodes. In this paper, the most difficult task is the compulsion of authorization policies and the policy revocation for retrieving secure data. To control these difficulties during mobility or improper conditions in the military (armed forces) regions, one of the cryptographic algorithms is being developed i.e, Ciphertext-policy attribute-based Mod Encoded encryption (CPABME). The keys are issued by different authorities and this may result in many security and privacy challenges such as coordination of attributes, attribute updation and key escrow problems. Proposed system provides secure lossless data exchange using CPABME for decentralized DTNs where there will be multiple key authorities independently manage their attributes and data.

Keywords- CPABME, DTN, CP-ABE, Encryption, Mod-encoder, military networks, sensor nodes.

I. INTRODUCTION

In the military(armed forces) networks, the connection of cordless devices handled by soldiers sometimes disengage due to disruptions in the network connectivity, such as in antagonistic regions, and the information passed from sender to receiver does not reach properly . This may happen because of bad climatic conditions, improper ecosystem factors and network jamming. One of the effective solution is disruption tolerant network which allow the motes to communicate with each other in these networking environments. when there is a failure in connectivity between originator and receiver, the information may need to stay in the transistional nodes for a short period of time until the connection would be stabilized. The storage nodes are introduced in disruption tolerant networks where data will be stored and the required information can be accessed only by authorized motes quickly.

To increase security for the confidential data and access control methods in military(armed forces) applications, cryptographic solutions are enforced. Depending on the user attributes or roles, differentiated access services are provided and these attributes are managed by key authorities. Here the current location of moving soldiers defines the attributes and these attributes frequently changes when soldiers move from one location to another location. The key authorities generate their own dynamic attributes for the soldiers in their current region. This DTN architecture is named as decentralized DTNs, as the multiple authorities generate and manage their own attributes keys separately.

II. MATERIALS AND METHODS

In this part, we proposed a secure data retrieval in decentralized DTNs to provide a multi- authority CPABME scheme. There are two authorities in this scheme who generates keys for secure communication between the users. One is the central authority and other is the local authority. The local authority performs secure 2pc protocol with the central authority to issue the attribute key components to the users. Hence, in this proposed scheme, we improved the security and scalability issues.

Many CP-ABE schemes have been proposed till now. But in this standard model, the subsequent CPABME schemes are implemented by more manifesting security proofs. However, most of the CP-ABE algorithms failed to achieve the security, integrity and authentication methods. Hence, an efficient system is developed which allowed an encryptor algorithm to specify an access predicate over the attribute by using the monotonic formulae.Hence, in this system, we develop a new algorithm which is partially based on CP-ABE inorder to improve the expressiveness of the access control policy.

Access Tree:

1)Description: A tree is represented with --‘ T ‘ having an access structure. Every nonleaf node of the tree represents a Threshold Gate. If numX is the number of children of a node x and kx is its threshold value, then 0 <= kx <= numX. P(x) represents the parent of the node x in the tree. Each leaf node x of the tree is described by an attribute and a threshold value kx=1. Bx denotes the attribute associated with the leaf node x in the tree T. The children of every node are numbered from 1 to N. The function index (x) returns a number associated with the node x.

The index values are uniquely assingned to the nodes in the access structure for a given key.

2) **Satisfying an Access Tree:** Let us assume for a node x, Tx be the subtree for a rooted tree T. If all the set of attributes z satisfy the access tree Tx, we express it as Tx(z) = 1.

Scheme Construction: Let us take BG as a bilinear group of prime order p, and let g be a generator of BG.
Let e: BG *BG -> BG1 denotes the bilinear map. A security parameter K, will determine the size of the groups. We use a Lagrange's coefficient Δi, ʌ for any i ϵ Zp* and a set, ʌ of elements in Zp* : define Δi,ʌ(x) = $\prod$ jϵʌ, j≠i $(x-j)/(i-j)$. Additionally, an hash function is also added, H: { 0,1} * BG from a universal hash function to associate each attribute in the random group element in BG1.

System setup: According to the security parameter, the member who is a trusted initialize, will choose a bilinear group BG of prime order p with the generator g. Hash functions will also be choosen H: { 0,1} * BG from a given group of universal one-way hash functions. The public parameter param is given by (BG, g, H). For simplicity, the param is removed below.

Central key Authority: The central key Authority chooses a random function λ ϵ R Zp* .It sets h = g^λ. The master public or private key is given by PK(CA) = h , MK(CA) = λ. Here PK represents public/ private key pair and MK represents the Master key.

Local key Authority: Each attribute Ai chooses a random function αi ϵ R Zp*. The master public or private key is given by PK (Ai) = e(g,g)^ αi , MK(Ai) = αi.

Key Generation: In CP-ABE algorithm, the user secret key components consists of a single personalized key and multiple attribute keys. The personalized key is uniquely meant for each of the users individually which prevents the collusion attack with different attributes among the users. The proposed key generation protocol is composed of the personal key generation followed by the attribute key generation protocols. As we have mentioned that with the single key authority key escrow problem can occur during data transfer. Hence the proposed key generation exploits the arithmetic secure 2PC protocol to avoid the key escrow problem such that none of the authorities can recognize the entire key components of the users individually.
Personal Key Generation: In the following protocol both the central authority and each of the local authorities are involved.As we have mentioned that the secure 2PC protocol is used for communication between the users and the central authority. The central authority generates personalized and a unique secret value for the user.To authenticate the user ut, the central authority selects a random exponent γ1, γ2, ….γn ϵ R Zp* for every local authority L1,…..Ln ϵ L ; and sets rt = $\sum_{i=1}^{m} \gamma i$.

Now, the central authority and each of the local authorities Ai involve in a secure 2PC protocol. Where the C.A's private input is (γi , β) and Ai's private input is αi.
The secure 2PC protocol returns a private output x = (αi + γi) β to Ai.This can be done through a general secure 2PC protocol for a simple arithmetic computation.Now the local authority Ai randomly picks T ϵ R Zp*, then it computes
T = g^$\frac{x}{T}$ = g^(αi + γi) β/γ and sends to the central authority.
The central authority then computes B = T^1/ β^2 = g^(αi + γi) /γ β and then sends it to local authority Ai.The local authority Ai outputs a personalized key component
Di = B^T = g^(αi + γi) /β and securely sends it to the user ut.Now, the user ut computes its personal key component D = $\prod_{i=1}^{m} Di = g^{((\alpha 1+\alpha 2+\cdots \alpha m)+\gamma t)/B}$.

Theorem 1 : The above key generation protocol is a secure 2PC protocol for computing
g^(αi + γi) /β by the Local Authorities Ai, assuming that the underlying arithmetic 2PC and zero knowledge proofs are secure.

Attribute Key generation: In this section, each local authorities Ai generates attribute keys after setting up the personalized key components for the user ut with the public parameter which is received from the central authority as follows:
The central authority first generates a random variable r^1 , and sends $g^{rt-r^1} \wedge g^{r^1}$ it to the local authority Ai and the user ut respectively.The local authority then takes the set of attributes Ai subset or equals to Ai(r) as input and outputs a set of attribute keys for the user that identifies with that set Ai. It chooses random rj ϵ Zp* for each attribute λj ϵ Ai. Then, it gives the following secret value to the user ut.

∀ λj ϵ Ai : Dj = g^ rt-r^1 .H(λ j)^rj , D^1j = g^rj.

Now the user computes g^ r^1 . Dj for all its attribute key components and finally get its entire secret key set as

SK (ut) = (D=g^ (α1+α2+....αm)+γt/ β , ∀ λj ϵ S : Dj=g^rt. H(λ j)^rj , D^1j = g^rj).
Where,

S= $U_{i=1}^{m}$ Ai.

In the previous multiauthority ABE schemes, the key issuing problem in terms of communication cost, has occurred more , hence in the proposed scheme during the key generation process using the 2PC protocol it requires (3m+1)Co messages , where m is the number of key authorities the user is associated with, and Co is the bit size of an element in BG Bilinear group. As we know that during the initial key generation phase for each user, the 2PC protocol is used only once. Hence, it can be avoided or we can say, it is negligible when compared to the key issuing problem for encryption or key revocation, which could be much frequently performed in

the DTN's . Each local authority needs to perform two more exponentiation operations in terms of computation cost. Each user required to perform m + 1 operations for the key generation. Again it incurs negligible computation cost compared to the other pairing or exponentiation operations. Hence, we can say that the additional computation cost for the initial key generation process using the 2PC protocol can be acceptable in this system.

Data Encryption : In this phase, the tree access structure T is defined by the sender, when he wants to send any confidential data M, over the universe of attributes L. The sender first encrypts the data under the tree access structure T to enforce the attribute-based access control on the data, and stores that data in to the storage nodes.

The encryption algorithm chooses a polynomial qx, for each node x in the Tree T. These polynomials are chosen in a top down manner, starting from the Root node R. To define the polynomial qx completely, for each node x in the tree T, the algorithm sets the degree dx of the polynomial qx to be one less than the threshold value kx of that node, that is dx=kx-1. For the Root node R, the encryption algorithm chooses a random s ϵ Zp* and sets qR (0) = s. Then, it sets d R other points of the polynomial qR randomly. For aby other node x, it sets qx (0) = qp (x) index (x)) and chooses dx other points randomly to completely define qx.

To create a ciphertext, public keys of each authority is used. Let Y be the set of leaf nodes in the access tree structure T. To encrypt a message M ϵ BG1 under the tree access structure T, it constructs a cipher text CT.

CT= (T , C= $Me(g,g)^{(a1+a2+\dots am)s}$, C = h^s ,

$\forall$ y ϵ Y : Cẏ = $g^{q_y(0)}$, C^1_y = $H(\lambda_y)^{q_y(0)}$) ,

Where C can be computed as C = $M.(PK_{A1} * \dots * PK_{Am})^s$ = $Me(g,g)^{(a1+a2+\dots am)s}$.

Now the data is encrypted and this encrypted data is called as cipher text. After the construction of CipherText, the sender stores it in the storage nodes securely. If the users request for any query, the storage nodes replies in the form of cipher text to the user.

Data Decryption: After requesting for a query, the user receive the cipher text CT, from the storage nodes, and the user can decrypt the cipher text by using its secret key. The algorithm performs in a recursive way. We represent this recursive algorithm Decrypt Node(CT, SK, x) which takes as inputs a cipher text CT, secret key or private key SK, which is associated with the set of attributes and a node x from the tree T. Hence it outputs a group element of BG.

Without loss of generality, Suppose a user ut performs decryption algorithm. If x is a leaf node, then define as follows. If λx ϵ A, then

Decrypt Node(CT, SK, x)

$$= \frac{e(D_x, C_x)}{e(D'_x, C'_x)} = \frac{e(g^{rt}).H(\lambda_x)^{rx}, g^{q_x(0)})}{e(g^{rx}).H(\lambda_x)^{q_x(0)})}$$

$$= \frac{e(g^{rt}, g^{q_x(0)}).e(H(\lambda_x)^{rx}, g^{q_x(0)})}{e(g^{rx}).H(\lambda_x)^{q_x(0)})}$$

$$= e(g,g)^{rt\, q_x(0)} .$$

If λx ϵ A, we represent Decrypt Node(CT, SK, x) = $\perp$

As we have mentioned that the algorithm performs a recursive way. Now we take this recursive case in to an action, as when x is a non-leaf node, the algorithm Decrypt Node(CT, SK, x) performs the following : For all node z, that are children of x, it calls the Decrypt Node(CT, SK, z) and stores the result as F_z. Let us assume S_x be an arbitrary K_x sized set of children node z, such that $F_z \neq \perp$. If none of the set matches or no such s set exists, then we say the node was not satisfied and the function returns $\perp$.

Otherwise, we compute the decryption as:

F = $\prod_{z \epsilon s_x} F_z^{\Delta_{i,\, s'_x}(0)}$, where i=index(z)

$S'_x = \{\text{index (z) : z} \epsilon S_x\}$

$$= \prod_{z \epsilon s_x} (e(g,g)^{rt.q_z(0)})^{\Delta_{i,\, s'_x}(0)}$$

$$= \prod_{z \epsilon s_x} (e(g,g)^{rt.q_p(z)(\text{index}(z))})^{\Delta_{i,\, s'_x}(0)}$$

$$= \prod_{z \epsilon s_x} (e(g,g)^{rt.q_x(i)})^{\Delta_{i,\, s'_x}(0)}$$

$$= e(g,g)^{rt.q_x(0)}$$

I

and returns the output.

The user can decrypt the obtained cipher text by using decryption algorithm. The user starts the algorithm by calling the function on the root node R of the access tree T. We observe that Decrypt Node(CT, SK, x) = $e(g,g)^{r_t \cdot s}$, the algorithm decrypts the cipher text by computing C/ e(C,D)/A) = M.

In this Attribute Based encryption Algorithm ABE, due to regular encryption of data, the data size increases continuously, as the encrypted data contains public keys. If number of nodes increases, it causes traffic or data overload in the network. Hence, to overcome this problem, we proposed a new algorithm called as Mod-Encoder based encryption algorithm.

In this Algorithm, it contains two phases i.e.,

1.Mod encoded based algorithm (MEBE)

2.Cipher Text attribute based Encryption algorithm (CP-ABE)

Mod encoder based algorithm (MEBE): This algorithm uses any standard encryption technique which include lossless

compression in order to provide the needs of low bandwidth and data security. Let S be a set of defined language over the alphabet set. Suppose S be English and be {A,B, ….. Z, a,b,…….z} Let the letters be represented by bi-junction function F that maps a letter to an Integer i where $1 \leq i \leq \text{III}$. Δ is a constant, called modulus constant. Let S be the data string where { s_1, s_2……s_n } ϵ S. computing modulus operation on every F(s_i) by Δ sequentially produce remainder set R as{ r_1, r_2,…. r_n} and quotient set as { q_1, q_2,…. q_n}. The elements in remainder set R contains the values between [0, $\Delta - 1$]. Thus the set elements in R are considered as vector numbers in base R. Each r_1 takes log2 R bits for binary representation. For example, If the size of the message is of n characters, then the number of bits needed to represent the vector is n x log2 R. The quotient set is represented in different way. Let the Base value B = [Δ] + 1 be another parameter. The elements of Q will have the values within the limit of [0, B-1]. Let Q be as number in base B i.e., (q_1, q_2,…. q_n)B. convert this number to highest number. It is obvious that highest base representation would reduce the digits in the numbers. If B is less than 10, we change it to Q_B to

Q_{10} as a base number.

The Mod-Encoder Algorithm can be stated as:

Input : S

N = | S |, i.e., length of S

Z = n x bit size i.e., bits size is the number of bits used to represent each char.

For i=1 to n

4.1) Read s_i, the i^{th} character of S.

4.2) Find R: R[i] = I(s_i)% Δ.

4.3) Find Q: Q[i] = I(s_i)/ Δ.

5) Representation of R: for i = 1 to n

5.1) Represent R[i] in Base Δ.

6) Representation of Q: Interpret Q as a base B number and convert it to Base 10. The vector R is communicated through open channel, whereas Q is encrypted to a cipher Q_c using any standard cryptographic technique and communicated to the receiver to ensure confidentiality of the message M. By doing so, the overhead of encrypting data is reduced, as we encrypt only tuple Q, rather than the whole message M. The receiver on receiving R and Q_c, decrypts Q_c to Q and decodes the message from the bi-tuple <R,Q>

The MOD-ENCODER Decoding Algorithm as follows:

Input : Bi-tuple <R,Q>

Convert Q from Base 10 to Base B: Let QB = (q_1, q_2,…. q_n) be the representation in Base B.

Interpret R as a vector of Base Δ number: for $1 \leq i \leq n$

3.1) i= q x Δ + r_i, where q_i the i^{th} digit of QB r_i the i^{th} element of R.

3.2) $s_i = I - 1(i)$

4) S = $(s_1, s_2 \ldots\ldots s_n)$.

III. EXPERIMENTAL RESULTS

Fig.1: sensor nodes connecting to various server

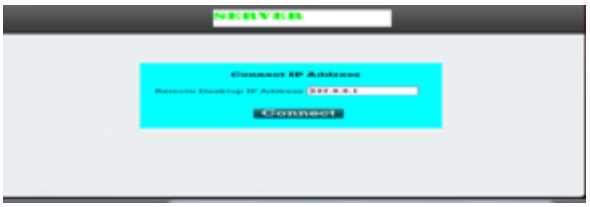

Fig.2: Connect to Server

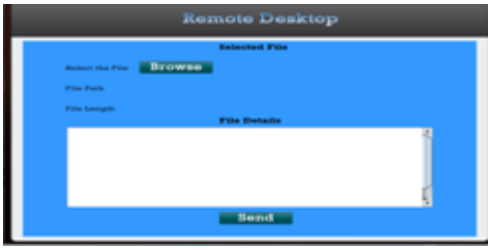

Fig.3: Connecting to various servers through intermediate servers

Fig.4:Selecting a file for sending

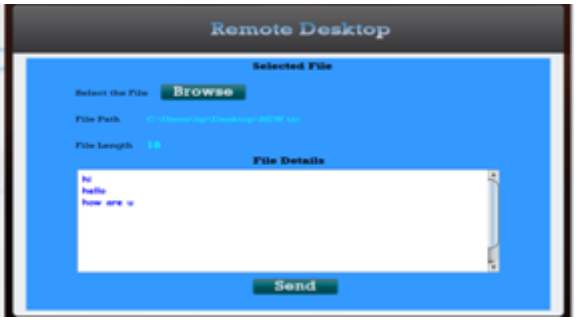

Fig.5: File obtained from browsing

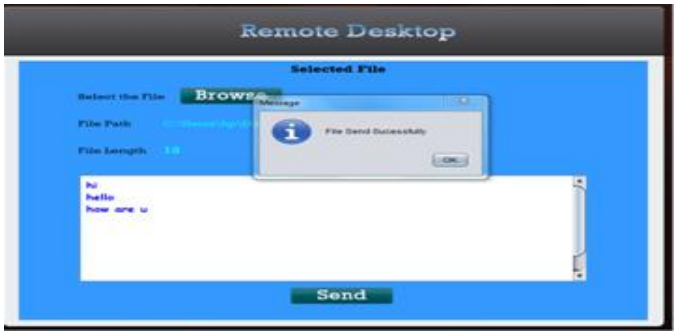

Fig.6:File sent successfully

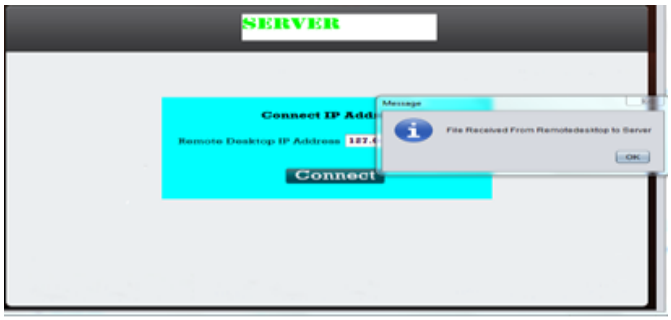

Fig.7:Server

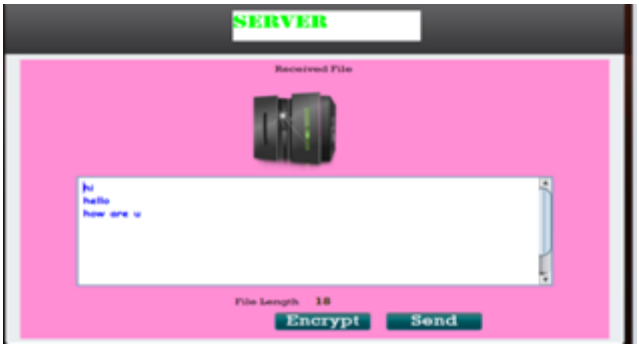

Fig.8: File received from mobile node to server

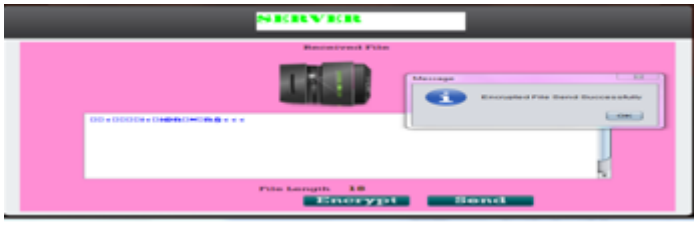

Fig.9:Encryption of the received file in server

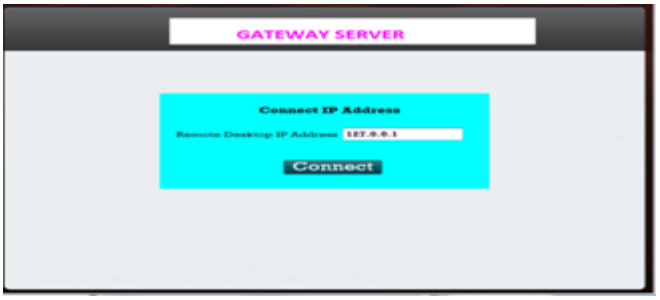

Fig.10: Gateway server

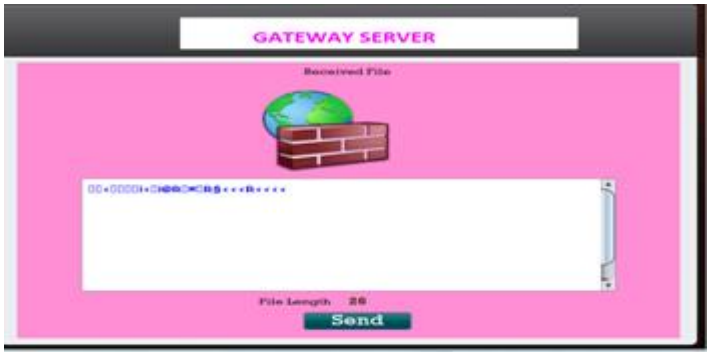

Fig.11:Encrypted file sent from gateway server to web server

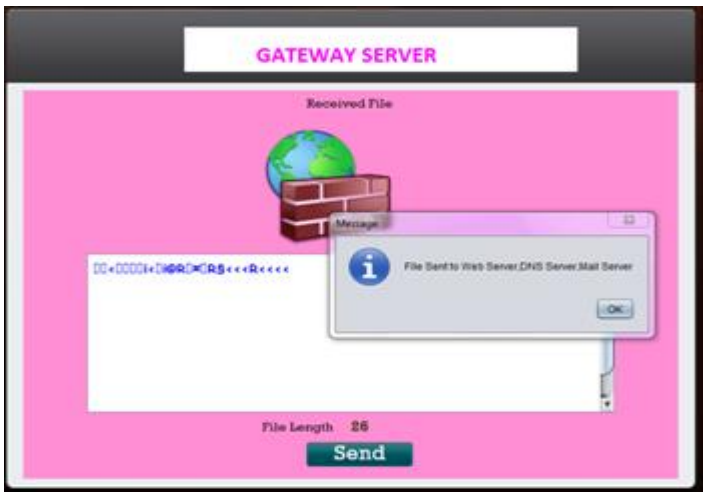

Fig.12: Sending an encrypted file

IV. CONCLUSION

In this paper, we implemented that a Secured lossless data transmission in armed force networks using CPABME methodology, The keys are issued by different authorities and this may result in many security and privacy challenges such as coordination of attributes, attribute updation and key escrow problems. Proposed system provides secure lossless data exchange using CPABME for decentralized DTNs where there will be multiple key authorities independently manage their attributes and data. Mod encoded based algorithm (MEBE),Cipher Text attribute based Encryption algorithm (CP-ABE) algorithms maintain the systemwith high security and efficient purpose

V. REFERENCES

[1]. References is a list of source materials that are used or consulted in the preparation of a work or that are referred during the writing of paper.

[2]. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" IEEE/ACM Transactions on Networking, Vol. 22, No. 1, February 2014.

[3]. Communication within Sensor Networks by Using KeyDistributor , International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 4906-4910.

[4]. A Novel Methodology for Secure Communications and Prevention of Forgery Attacks (0975-8887),International Journal of Computer Applications Volume 96 - Number 22 Year of Publication: 2014.

[5]. A Novel Dual Phase Mechanism for Data Transmission to ProvideCompression and Security ,International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 12, December 2013 ISSN: 2277 128X

[6]. S. Roy andM. Chuah, "Secure data retrieval based on ciphertextpolicy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSETech. Rep., 2009.

[7]. N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective groupbroadcast in vehicular networks using dynamic attribute basedencryption," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[8]. D. Huang and M. Verma, "ASPE: Attribute-based secure policyenforcement in vehicular ad hoc networks," Ad Hoc Netw., vol. 7,no. 8, pp. 1526–1535, 2009.

[9]. A. Lewko and B. Waters, "Decentralizing attribute-basedencryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

[10]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-basedencryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[11]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[12]. 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.

[13]. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp. 261–270.

[14]. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Comput. Commun.Security, 2008, pp. 417–426.

[15]. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in Proc. ACMConf. Comput. Commun.Security, 2006, pp. 99–112.

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