Secure Access Policies for data Retrival

[1]Prof.Vishal Shinde, [2]Pranit Shirke, [3]Sanket Rane, [4]Vighnesh Koparkar
[1]Asst. Professor, [2,3,4]BE Student, [1,2,3,4]Comp. Engg. Dept, SSJCET, Asangaon, India.
[1]mailme.vishalshinde@gmail.com, [2]pranitshrk41@gmail.com, [3]sankrane96@gmail.com,
[4]vighneshkopakar@gmail.com

Abstract : **In the large number of outgrowing commercial environment each and everyone focus to transmit the data securely and to maintain three main goals of network security which are Confidentiality, availability and integrity. Wireless communication is widely used to transfer data between two nodes. But due some reasons like jamming, environmental factors, and mobility, especially when they operate in hostile environments the wireless connection becomes weak or it may loss. To overcome this problem and to get data securely the system called Disruption-tolerant network (DTN) is introduced. Some of the most challenging issues in this scenario is to enforce authorization policies and the dynamic update of policies for secure data retrieval. In this report an efficient approach such as access policies(public, private and protected),attribute revocation, a Repetitive Trust Management(RTM),validation period, Forward & backward secrecy and Attacker Detection is proposed to handle the attacks and to maintain network security goals in DTNs.**

Keywords*: Access policies, 3-DES, disruption-tolerant network (DTN), Repetative Trust management, ABE system, keyescro*

I. INTRODUCTION

There are different types of wireless networks like Mobile ad-hoc networks, Sensor networks, Delay Tolerance Networks, and so on, available in present age, In this report we discuss about Delay Tolerant Network (DTN) applied in various fields for communication.

A traditional TCP/IP network depends on the stable end-to-end connectivity which is often disrupted by heavy rain, bad weather, jamming, physical movement, or destruction of nodes. Such disruption makes it improbable to select a path, restricting the flow of data. DTN is an approach to address this technical issue. It has its own way to send packets which is unique from other networks, routing is done by multi-hop transmission and simultaneous communication amongst nodes. It also uses persistent storage within nodes, along with opportunistic mobility to avoid disruptions in connectivity. Typically, when there is no end-to-end connection between sources and a destination pair, the messages from the sending node has to wait in the hoping nodes for a substantial amount of time till the connection is set. In DTNs where data is stored or replicated such that only authorized users can access the necessary information quickly and efficiently.

In DTN architecture authentication of proper user is done by associating a private key which is based on its attributes, Where multiple authorities issue and manage the keys of users belonging to them independently, However, the problem of applying ABE to DTNs introduces several security and privacy challenges. As some user might change his particular attributes at some point (for example, moving their region), or some private key may be mishandled, revocation of key (or update) for each attribute is necessary in order to make systems secure. But, this problem is more difficult, mainly in ABE systems, since each attribute is

ISSN : 2494-9150 Special Issue-01, MAR 2016.

conceivably shared by various users (Now on, it refers to such a collection of users as an attribute group). This implies that if attribute or user in an attribute group is revoked it would affect the other users in the group. For example, if a user joins or leaves an access of that user to specific group database is removed or controlled for backward or forward secrecy.In decentralised disruption network it contains different storage nodes which are associated with its own attribute set. for e.g. if sender sets access policy as Private/Public/Protected and then he select batalian B1 and Region R1,then data will be store inly in storage node which is associated with attribute set B1 and R1.Thus in this way only authorized user who satisfies the access policy can access data securely. In DTN system Data is Stored in external storage node, so it becomes mandatory to provide security to data stored in storage node. Thus encryption method allows to restrict data from unauthorized access and to maintain confidentiality.

In this paper the encryption method called 3-des method is used. In cryptography, Triple DES (3DES) is usually name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) is a symmetrical-keyblock algorithm, which implements Data Encryption Standard (DES) cipher algorithm is been applied three times to each data block. The size of original DES cipher's key is 56 bits was generally sufficient at time of designing the algorithm, but increasing computational power made brute-force attacks feasible. Triple DES involves a simple method to increase the key size of DES which helps increasing security, without the necessity to develop a new block cipher algorithm. In this report three types of access policies are introduced:

I) Public

II) Private

III) Protected

I) Public **:**

In public policy, it can send file to all batalians present in all regions.

II) Private **:**

In private policy, the user which falls under the category of private in specified batalians and in specified region can access the data.

This policy is used for confidential data which should be access by only specific people.

The people can be categorized according to their Rank, Place, Missions, etc.

This is considered as most secured access policy as compared to other two policies.

III) Protected**:**

In Protected mode it can select all batalians from one selected region.

II. LITERATURE SURVEY

Literature survey is a vital step in software development process. Before developing the tool is useful while getting the time factor, economy and company strength. Once these things are satisfied, then next stage is to decide which OS and programming language can be used for developing the tool. A lot of external support is needed once programmers start building the tool. This support can be obtained from senior programmers, from variors means. After considering the above factors the proposed system is developed.

ABE is developed in two different types called key-policy:-

KEY POLICY ABE (KP-ABE)

In KP-ABE, ciphertext gets labelled with a unique set of attributes. The key authority chooses a access policy for each user that helps decide which cipher texts he is able to decrypt and gives the user a key considering

KP-ABE ALGORITHM

1) Setup:

the policy into the user’s key.

Define the universe of attributes U = {1, 2, n}. Now, for each attribute i ∈ U, choose a number it uniformly at random from Zp. Finally, choose y uniformly at random in Zp. The published public parameters PK are

$T1 = g^{t1}, \ldots, T|U| = g^{t|U|}, Y = e(g, g)^y$.

The master key MK is:

$t1, \ldots, t|U|, y$.

2) Encryption (M, γ,PK):

To encrypt a message M ∈ G2 under a set of attributes γ, choose a random value s ∈ Zp and publish the cipher text as:

$E = (\gamma, E0 = MY^s, \{Ei = T^{s}_{i}\}_{i\in\gamma})$.

3) Key Generation (T, MK):

The algorithm outputs a key that enables the user to decrypt a message encrypted under a set of attributes γ if and only if T (γ) = 1.

4) First choose a polynomial qx for each node x (including the leaves) in the tree T . These polynomials are chosen in the following way in a top-down manner, starting from the root node r.For each node x in the tree, set the degree dx of the polynomial qx to be one less than the threshold value kx of that node, that is, dx = kx − 1.

5) Now, for the root node r, set qr(0) = y and dr other points of the polynomial qr randomly to define it completely. For any other node x, set

qx(0) = qparent(x) (index(x))

and choose dx other points randomly to completely define qx.

6) Once the polynomials have been decided, for each leaf node x, it give the following secret value to the user:

$Dx = g^{qx(0)/ti}$ where i = att(x) .

The set of above secret values is the decryption key D.

7) Decryption (E, D):

It specify decryption procedure as a recursive algorithm. For ease of exposition it present the simplest form of the decryption algorithm and discuss potential performance improvements in the next subsection.

8) first define a recursive algorithm DecryptNode(E, D, x) that takes as input the ciphertext E = (γ, E0 , {Ei}i∈γ), the private key D (assume the access tree T is embedded in the private key), and a node x in the tree. It outputs a group element of G2 or ⊥. Let i = att(x). If the node x is a leaf node then:

DecryptNode(E,D,x)

9) Now consider the recursive case when *x* is a non-leaf node. For all nodes *z* that are children of *x*, it calls DecryptNode(*E*,*D*, *z*) and stores the output as F_z. Let s_x be an arbitrary k_x-sized set of child nodes *z* such that $F_z \neq \perp$. If no such set exists then the node was not satised and the function returns ⊥.

Ciphertext -policy ABE (CP-ABE) :

The ciphertext is created with a certain access policy chosen by an encrypt or, but a key is simply created by also considering the attribute set. CP-ABE is best suited to DTNs than KP-ABE because it enables users who are encrypting data to choose a access policy on attributes and to encrypt confidential data using a structure with involving a certain keys or attributes.

CP-ABE ALGORITHM

Proposed solution consists of 4 phases, Setup Phase, Key Generation Phase, Encryption Phase and Decryption Phase.

1) Set Up:

The setup algorithm chooses a group G of prime order p and a generator g .

Step 1:

A trusted authority generates a tuple

G=[p,G,G1,g ∈ G, e] ← Gen(1k) .

Step 2:

For each attribute ai where 1 ≤i ≤n, the authority generates random value

{ai,t ∈ * Z p } 1 ≤t ≤ni and computes {T i,t = i t ag,}

1 ≤t ≤ni

Step 3:

Compute Y = e(g,g)α where α ∈ * Z p

Step 4:

The public key PK consists of

[Y,p,G,G1 ,e ,{{T i,t } 1 ≤t ≤ni }1 ≤i ≤n]

The master key Mk is

[α, {{ai,t ∈ * Z p } 1 ≤t ≤ni} 1 ≤i ≤n]

2) Key Generation (MK,L):

The Key Generation algorithm takes master key MK and the attribute list of the user as input and do the following

Let L=[L1,L2,…,Ln]={ n t t n t v v v ,1 ,2 , , ,.., 1 2 } be the attribute list for the user who obtain the corresponding secret key.

Step1:

The trusted authority picks up random values λi ∈ * Z p for 1 ≤i ≤n & r ∈ * Z p and computes : D0= g α –r .

Step2:

For 1 ≤i ≤n the authority also computes

D i,1 , D i,2 = [i ti r a g +λ , , i g λ]

where Li = i ti v ,

The secret key is [D0 Di,1 , Di,2].

3) Encrypt(PK,M,W):

An encryptor encrypts a message M∈ G1 under a cipher text policy W=[w1,w2,..,wn] and proceed as follows.

Step1 :

Select s ∈ * Z p and compute C0=g s and C~ = M. Ys = M.e(g,g)αs

Step2:

Set the root node of W to be s, mark all child nodes as un-assigned, and mark the root node assigned.

Recursively, for each un-assigned non leaf node , do the following :

a) If the symbol is ∧ and its child nodes are unassigned , assign a random value si 1≤si ≤p-1 and to the last child node assign the value

Mark this node assigned.

b) If the symbol is ∨, set the values of each node to be s. Mark this node assigned.

c) Each leaf attribute ai ,can take any possible multi values, the value of the share si is distributed to those values and compute

[Ci,t,1 , Ci,t,2]= [i s g , i s T ,ti].

The cipher text CT is

[C~ ,C0 , {{ Ci,t,1 , Ci,t,2 } 1 ≤t ≤ni } 1 ≤i ≤n }].

4) Decryption (CT,SKL):

The recipient tries to decrypt CT, without knowing the access policy W by using his SKL associated with the attribute list L as follows.

III. COMPARISION BETWEEN KP-ABE,CP-ABE AND 3-DES

Srno	Parameter	KP-ABE	CP-ABE	3-DES With Access Modes
1.	Acces control	Low,High with reencryption	Average realization OfComplex Access contol	High with access mode feature
2.	Efficiency	Average	Average	High along with simple Process flow
3.	Computational Overhead	More	Average	More
4.	Collusion resistance	Good	Good	Very Good
5.	Complexity	More	More	Less
6.	Repetative trust	Absent	Absent	Present
7.	E-mail Validation	Absent	Absent	Present
8.	Confidentiality	Less	More	More

IV. PROPOSED SYSTEM

In proposed system, in the DTN network to transmit the data securely between sender and receiver.In this system Central authority plays vital role of managing private keys of users according to its validation periods and thereby keeping the repetitive trust management. Also it handles the attacker list who tries to guess the keys by trial and error method. File keys or public keys of files are managed by different local authoritites thus it solve the key escrow

ISSN : 2494-9150 Special Issue-01, MAR 2016.

problem. Each local authority is associated with its own set of attributes. For e.g. If sender sets the access policy of file as batalian b1 and region r1 then local authority1 will handle the file key of that file.similarily access policies B2-R2,B1-R2, and B2-R1 are associate with local authorities 2,3,and 4 respectively.Also data stored in storage node is stored in encrypted form. 3-Des encryption method is used to encrypt plaintext and to convert it to ciphertext.

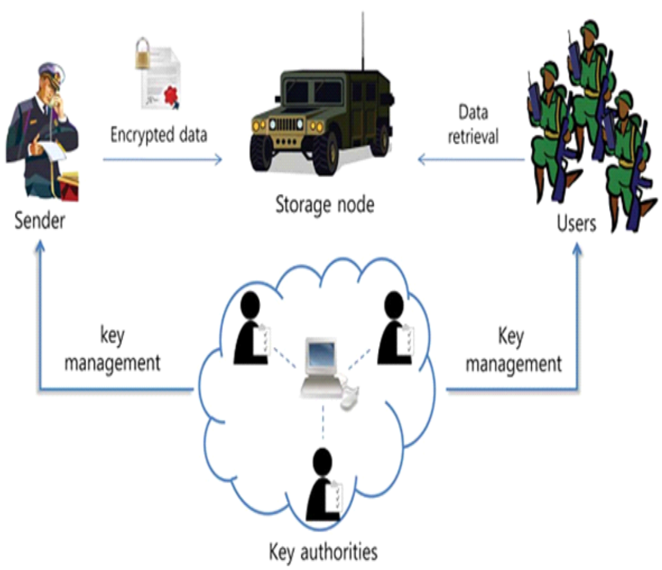

Fig.no.1 SYSTEM ARCHITECTURE

ALGORITHMS

Encryption :

$Encryption\ (plaintext\ ,\ E_{k1}, D_{k2}, E_{k3})$

$if\ (E_{K1} = \ = Key1)$

$Ciphertext\ = E_{k1}(plaintext);\ //\ E_{k1} is\ Encryption\ key1$

$if\ (D_{K2} = \ = Key2)$

$Ciphertext\ = D_{k2}(plaintext);\ //\ D_{k2} is\ Decryption\ key2$

$if\ (E_{K3} = \ = Key3)$

$Ciphertext\ = E_{k3}(plaintext);\ //\ E_{k3} is\ Encryptionkey3$

Return Ciphertext;

Decryption :

$Decryption\ (ciphertext\ ,\ D_{k1}, E_{k2}, D_{k3})$

$if (D_{K3} = \ = Key3)$

$Plaintext\ = D_{k3}(ciphertext);\ //\ D_{k3} is\ Decryption\ key3$

$if\ (E_{K2} = \ = Key2)$

$Plaintext\ = E_{k2}(ciphertext);\ //\ E_{k2} is\ Encryption\ key2$

$if\ (D_{K1} = \ = Key1)$

$Plaintext\ = D_{k1}(ciphertext);\ //\ D_{k1} is\ Decryption\ key1$

Return Plaintext;

3.2.2. *Access modes :*

if (Access mode = = PUBLIC) THEN

Select All Batalians present in All Regionas receiver ;

else if (Access mode = = PROTECTED) THEN

Select All Batalians present in One Region ;

else if (Access mode = = PRIVATE) THEN

Select Only one Batalian present in One Region ;

else

Select Proper Access mode ;

Repetative Trust Management :

if (VALIDATION TIME = = EXPIRATION TIME)

THEN

Generate New Private key ;

Send new private key to user through E − mail Address ;

EXPIRATION TIME = EXPIRATION TIME + 30 min

V. Expected Output

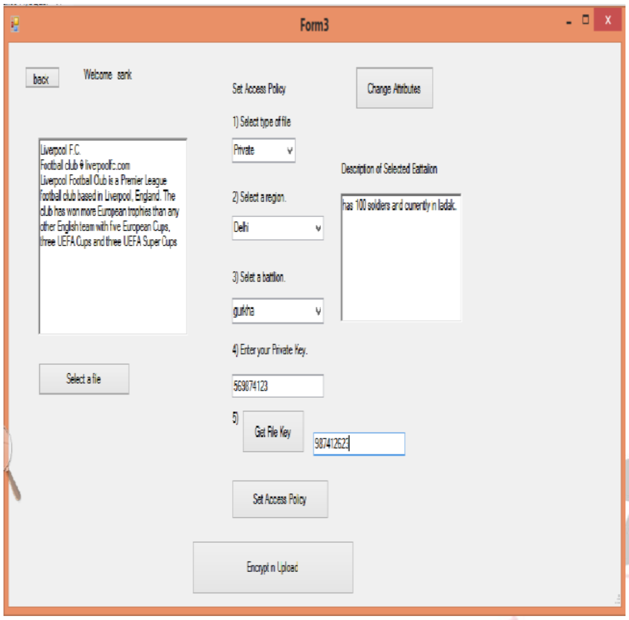

Fig.no.2 Encryption process

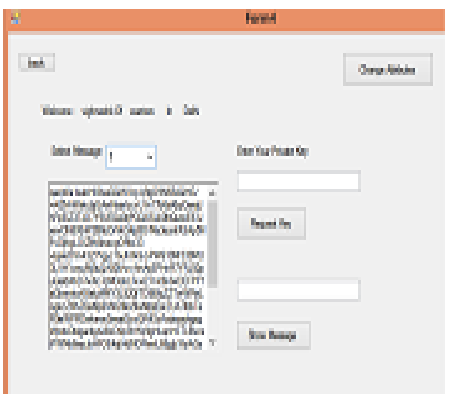

Fig.no.3 Decryption process

VI. CONCLUSIONS

DTN is more secure and successful solution for applications in which connection between two nodes is week or less secure.DTN method uses storage node which is main heart of this system which temporarily stores or replicate data.Thus to provide high security to storage node proposed system is more reliable as compared to existing system with more features like repetitive trust management,emailverification,accessmodes,private key updation etc. Also access modes like Private, protected and public provides strategy to maintain authorization.

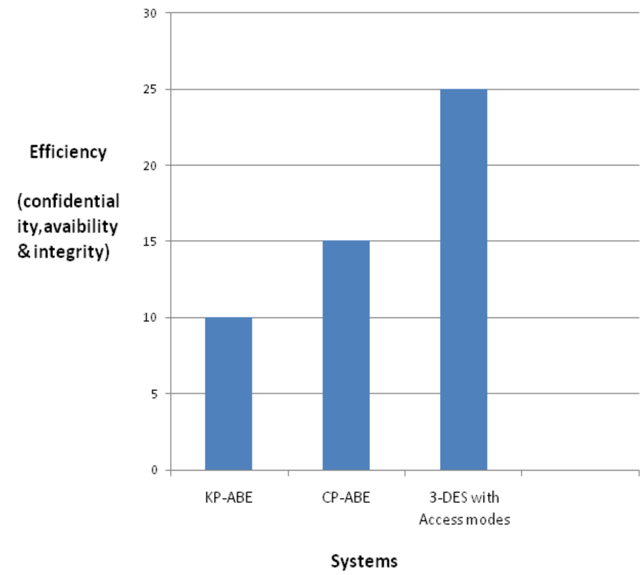

Fig.no.3 comparision graph

REFERENCES

1) J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "*Maxprop: forvehicle-based disruption tolerant networks*," in *Proc.IEEE INFOCOM*,2006,pp. 1–11.

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

3) 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.

4) 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.

5) M. Chuah and P. Yang, "*Performance evaluation of content-based information retrieval schemes for DTN*s," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.

6) M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"*Plutus: scalable secure file sharing on untrusted storage*," in *Proc.Conf. File storagetechnol* 2003, pp. 29–42.

7) 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.

8) 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.

9) D. 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.

10) A. Lewko and B. Waters, "*Decentralizing attribute-based encryption,*"

Cryptology ePrint Archive: Rep. 2010/351, 2010.

11) A.T. Sherman and D.A. McGrew, "*Key establishment in large dynamic groups using one way function trees,* "IEEE Trans. Software engg. , vol.29,no.5, pp. 444-458, May 2003.

12) S.S.M. Chow," *Multi-authority attribute based encryption*" in proc. TCC, 2007,LNCS 5443,pp 256-276.

