ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Data Retrieval for Decentralized DTN Using Multi - Authority

Nikita Bankhele, Priya Deshmukh, Chandrakant Gawande, Mangesh Manke

Student, Dept. of Computer Engineering, Savitribai Phule Pune University, D. Y. Patil Institute of Engineering & Technology, Ambi, Pune, India.

Student, Dept. of Computer Engineering, Savitribai Phule Pune University, D. Y. Patil Institute of Engineering & Technology, Ambi, Pune, India.

Student, Dept. of Computer Engineering, Savitribai Phule Pune University, D. Y. Patil Institute of Engineering & Technology, Ambi, Pune, India.

Head, Dept. of Computer Engineering, Savitribai Phule Pune University, D. Y. Patil Institute of Engineering & Technology, Ambi, Pune, India

.

ABSTRACT: The CP-ABE for confidential data retrieval in decentralized Disruption Tolerant Networks (DTNs) where multiple key authorities manage their attributes independently. Fast attribute revocation enhances backward/forward secrecy of confidential data by decreasing the windows of vulnerability. The key escrow problem is resolved by an escrow-free key issuing protocol that achievements the characteristic of the DTNs architecture proposed a decentralized approach; their technique does not authenticate users. Determine how to apply the proposed mechanism to securely and efficiently manage the confidential data scattered in the DTNs. Finally the Disruption-tolerant network (DTN) technologies are becoming effective solutions that allow wireless devices carried by soldiers to communicate with each other and access the private data or command reliably by exploiting external storage nodes.

KEYWORDS: Access Control, Attribute-Based Encryption (ABE), Disruption-Tolerant Network (DTN), Multi-Authority ,Secure Data Retrieval.

I. INTRODUCTION

Disruption Tolerant Network (DTN) is a method to computer network architecture that search for to address the technical issues in dissimilar networks that may be absence continuous network connectivity. Disruption may arise because of the edge of the wireless radio range of mobile nodes. Security apprehension for DTNs differs depending on the environment and application, though validation and secrecy are crucial. These security guarantees are difficult to form in a network without tenacious connectivity. The solution for this difficulty is that use of ad hoc network and distributed security investigation, such as use of disseminated security certificate authorities. Original solution from DTN include

• Use of encryption.
• The use of interfere evident table with gossiping protocol.

Encryption is the process of encoding communications or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interruption, but contradicts the message content to the interceptor. In an encryption system, the message or data, referred to as plaintext, is encrypted using an encryption algorithm, producing a cipher-text that can only be read if decrypted. For technical aims, an encryption system usually uses a pseudo-random encryption key produced by an algorithm.It is in standard possible to decrypt the message without possessing the key, but, for a well-designed encryption system, large computational resources and talent are required. An authorized recipient can straightforwardly decrypt the data with the key providing by the creator to receivers, but not to unauthorized interceptors. IN the case of military network use CP-ABE. ABE is a relatively current approach that reconsiders the concept of public-key cryptography. In old-fashioned public-key cryptography, a data is encrypted for a

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

specific receiver using the receiver's public-key. Identity-based cryptography and in specific identity based encryption (IBE) changed the old-fashioned understanding of public-key cryptography by allowing the public-key to be a random string, e.g., the email address of the receiver. ABE goes one stage further and defines the uniqueness not atomic but as a set of attributes, e.g., roles, and data can be encrypted with respect to subsets of attributes (KP-ABE) or policies defined over a set of attributes (CP-ABE). The key dispute is that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" where user keys are always issued by some trusted party.
In CP-ABE which use a storage node. The main purpose of storage node is that which can store the encrypted data from the sender and provide these messages to the intentional recipient. Difficult with this scheme is that the storage node is semi trusted, any issue in the storage node may course loss of all data. To avoid these problems introduce a new scheme in which we can use routing for sending encrypted messages from sender to receiver instead of storing data in the storage node. The routing scheme used in the new scheme is the dynamic routing. Dynamic routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid in response to the change.

II. RELATED WORK

Sr.no	System proposed	Advantage	Disadvantage
1	CP-ABE Method.[2]	Secure against collusion attack	Security degradation in term of backward & forward secrecy.
2	Distributed KP ABE Method.[3]	It enables more realistic deployment of attribute based access control.	Performance degradation.
3	Decentralized CP-ABE Method.[4]	Flexible fine-grained access control.	Efficiency and expressiveness of access policy.
4	Maxprop: Routing Method. [5]	Propose a DTN routing protocol, called MaxProp that performs significantly better than previous approaches.	Load is increased.
5	Performance evaluation of content-based information retrieval Method. [6]	Proposed approach achieved smaller query response time and hence achieve higher query success rate.	The query load increases such that there is a buffer overflow of stored queries, Then the query success rate will drop.
6	Plutus: Novel Method .[7]	Proposed approach is more secure and efficient.	With overhead comparable to systems that encrypt all network traffic.
7	ABE Method.[8]	Performance better than existing system.	Less Expressive method.
8	KP ABE Method.[9]	Efficient sharing of encrypted data.	Selectively shared only at a coarse grained level.
9	mCP-ABE Method.[10]	Instantaneous attribute revocation.	No way to revoke an attribute before the expiration date.

Table: Survey Table

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

I. **Attribute-Based Encryption (ABE)** :

Attribute-based Encryption schemes where encryption and decryption are resolved by then Attributes of the data and the recipients. This functionality comes at anexpensive. In A traditional implementation, the size of the cipher-text is relative to the number of attributesAssociated with it and the decryption time iscompared to the number of attributes used during decryption. ABE systems enable the use of multipleattributes at the same time.

Two Type of ABE Following are:

i. key-policy ABE (KP-ABE)

In KP-ABE, the Encryptor gets to label a cipher-text with a set of attributes. The key authority chooses a strategy for each user that decides which cipher-texts he can decrypt and issues the key to each User by set in the policy into the user's key. CP-ABE is more suitable to DTNs than KP-ABE. Since it enables encryptors such as a commanding officer To prefer an access strategy on attributes and to encrypt secretive Data under the access structure via encrypting with the Equivalent public keys or attributes.

ii. **Cipher-text Policy ABE(CP-ABE)**

The concern of the cipher-texts and keys are reversed in CP-ABE. In CP-ABE, the cipher-text is encrypted with an access policy Selected by an Encryptor, but a key is simply formed with respect To an attributes set. CP-ABE scheme provides a supple Fine-grained access control such that the encrypted .The content scan only be accessed by authorized users. Two unique characteristics CP ABE scheme provides are: (i) the Incorporation of dynamic attributes whose value may Modify over time, and (ii) the revocation feature.

II. ***Lazy Attribute Revocation****:* Bethencourt et al. [13] and Boldyreva et al. [16] first recommended key revocation methods In CP-ABE and KP-ABE, correspondingly. Following a revocation, we believe that it is acceptable for the revoked reader to read unmodified files. A revoked reader, however, must not be able to read updated files, nor may a revoked .The writer is able to change the files. Settling for lazy revocation Trades re-encryption charge for a degree of security Their solutions are too Add one to each attribute an expiration date or time and distribute A new set of keys to valid users after the expiration. The Episodic attribute revocable ABE schemes [8], [13], [16], [17] have two main efforts. The first difficulty is the security degradation in conditions of the Backward and forward secrecy [18]. It is a significant situation That user, such as soldiers may change their attributes frequently, E.g., position or location move when considering these As attributes [4], [9].

i. **Backward secrecy**: A user who recently holds the attribute Might be able to access the previous data encrypted earlier he Obtains the attribute to the data is re-encrypted with the newly updated attribute keys by periodic rekeying(backward secrecy).

ii. **Forward secrecy:** A revoked user would still be able to access the encrypted Data even if he does not pick the attribute any more until .The next expiration time (forward secrecy).

III. ***Key Escrow*:**Most of the existing ABE systems are created in the manner where a single trusted authority has thepower to generate the whole personal keys of users with its Master secret data [11], [13], [14]. Thus, thekey escrow problem is inborn, such that the key authority can decrypt every cipher-text addressed to users in the system by generating their secret keys at any time.

II. EXISTING SYSTEM

In the case of military networks the nodes are mobile for the reason that of this cause the network is suffer from discontinuous connectivity and frequent partitions. To avoid this difficulty introduce a new form of network known as Disruption Tolerant Network (DTN).The most exciting issue for this picture is that the enforcement of authorization policies and the policies keep informed for secure data retrieval. The CP-ABE [8] is the most favorable solution. In the situation of decentralized DTNs CP-ABE [9] [10] uses a multiple key authorities to fare their attributes in dividualistically. In CP-ABE it provides an accessible way of encrypting data such That the Encryptor defines the attribute set that the descriptor needs to retain in order to decrypt the cipher text. Different users are permissible to decrypt a different piece of data per the security Policy.

LIMITATION OF EXISTING FRAMEWORK:

• The issue of applying the ABE to DTNs presents a little security and security challenges. Since a few clients may change theirs Related properties earlier or far ahead, or some private keys may be bargained, key Renouncement (or upgrade) for each one attribute is fundamental with a specific end goal to make frameworks secure.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

• However, this issue is expressively more bothersome, Particularly in ABE frameworks, since each one characteristic is possibly imparted by different clients.
• Another test is the key escrow issue. In CP-ABE, the key authority creates private keys of clients by applying the supremacy's expert Secret keys to clients' related set of properties.
• The last test is the synchronization of traits issued from distinguishing Powers. At the point when various powers oversee and issue Ascribes keys to clients freely with their expert mysteries, it is tricky to depict fine-grained access arrangements over Traits issued from distinctive powers.

III. NETWORK ARCHITECTURE

In this section we describe the network architecture of existing System

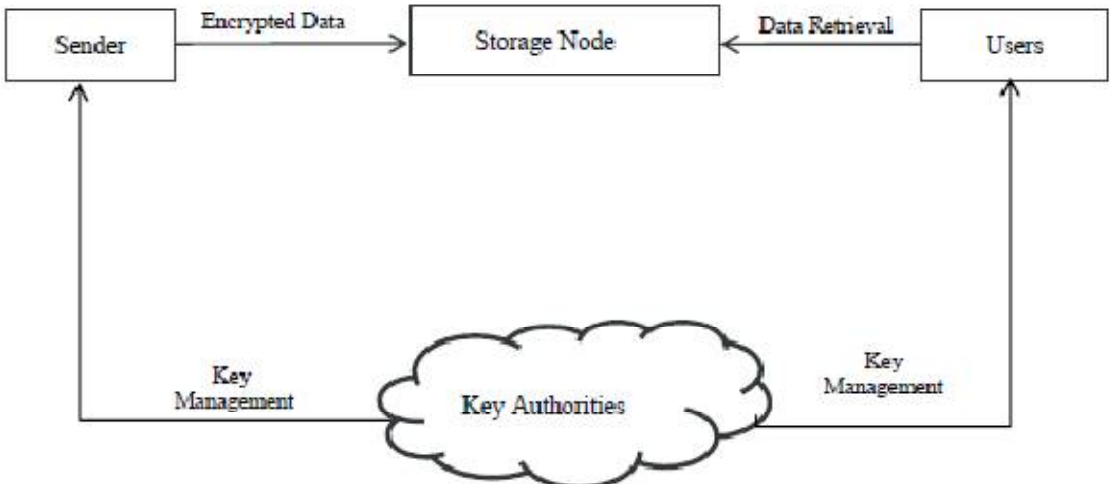

Fig 1.Architecture of secure data retrieval in a disruption tolerant military network.

The network architecture consists of four entities they are
Key Authorities: The object used for the generation of both Public and private key for CP-ABE. It resides on a central Authority and a number of local authorities. They're presenting a protected Communication channel between central authority and local authorities. The main purpose of local authorities Is that it manages various attributes and provides corresponding attribute keys to users
Storage node: Storage node stores data from the sources and provides equivalent access structure to the users. Storage nodes may be mobile or static.
Sender: The source having private data and encrypt. The message with particular access structure. After encrypting the message source can store the data in the storage Node. The last entity is the user. The user is a mobile node Access data from the storage node.
User: The user having a set of features and they can fulfil the access policy designated by the source. The user can decrypt the message if and only if they fulfil the access structure Used by the sender for encrypting the message.

IV. PROPOSED SYSTEM

In the proposed system attribute-based safe data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following successes. First, instantaneous attribute revocation increases backward/forward secrecy of secretive data by decreasing the windows of vulnerability. Second, encrypts can describe a fine-grained access strategy using any monotone access creation under attributes allotted from any chosen set of authorities. Third, the key escrow problem is fixed by an escrow-free key allotting protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol creates and issues user furtive keys by performing a secure (2PC) two-party computation protocol between the key authorities with their own mysteries. The 2PC protocol deters the key authorities

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

from obtaining slightly master secret data of each other, such that none of them could create the whole set of user keys alone. Thus, users are not necessary to completely trust the authorities in order to protect their data to be shared. The data secrecy and privacy can be cryptographically compulsory against any curious key authorities or data storage nodes in the proposed scheme.

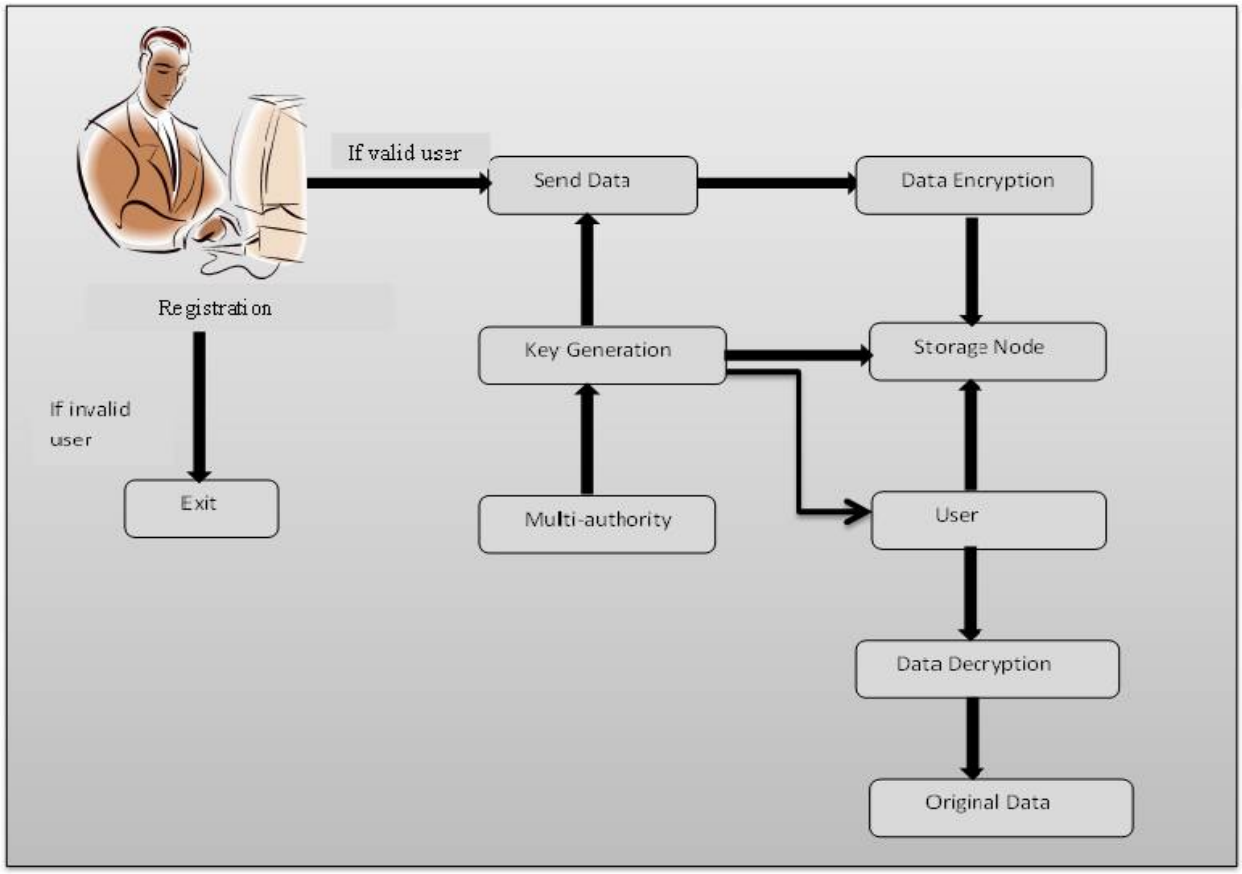

Fig 2.Proposed System Model

Advantages:

i) Data confidentiality: Illegal users who do not have enough authorizations satisfying In addition, illegal access from the storage node or key authorities should also be forbidden.

ii) Collusion-resistance: If several users collude, they may be able to decrypt a cipher-text by merging their attributes even if each of the users cannot decrypt the cipher-text alone.

iii)Backward and forward Secrecy: In the situation of ABE, backward secrecy means that any user who comes to hold an attribute should be prohibited from accessing the plaintext of the previous data exchanged before he holds the attribute On the other side, forward secrecy means that any user who feels an attribute should be prohibited from accessing the plaintext of the succeeding data exchanged after he feels the attribute, unless the other valid attributes that he is holding satisfy the access policy. The access policy should be prevented from accessing the plain data in the Storage node.

V. SIMULATION RESULTS

In *Analysis* phase module we are going to develop the user satisfied trust worthiness. This is analyzed with the following information like i) how long user has touch with network , ii)What type of file sharing and when the user file sharing takes place with the specified time and date . iii) How many users are using in the network.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

System	Cipher Text Size	Rekeying Message	Private Key Size	Public Key Size
BSW	(t+)A0+A+At	l(k+)A0	(k+)A0	A0+A
DDTN	(t+m)A0+mA+At	l(k+)A0	(k+m)A0	mA0+mA
Proposed	(t+)A0+A+At	(n-l) log n/n-l A0	(k+)A0 +log n	A0+Ma

Table 2:Efficiency Analysis

t-Number Of Attributes Appeared in T
A0-Bit Size Of An Element A-Bit Size O An Element T
Ct-Bit Size Of An Access Structure in T n-Number Of All Users In The System
k-Number Of Attributes Associated With Private Key Of User
m-Number Of Authorities In A System l-Number Of Users In Attribute Group

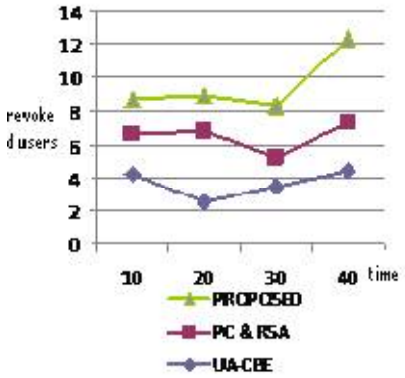

Table I summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the key authority or the storage node needs to send to update non revoked users' keys for an attribute. Private key size represents the storage cost required for each user to store attribute keys or KEKs. Public key size represents the size of the system public parameters. In this comparison, the access tree is constructed with attributes of different authorities except in BSW of which total size is equal to that of the single access tree in BSW. As shown in Table I, the proposed scheme needs rekeying message size of at most to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its cipher text size is linear to the number of revoked users in the system since the user revocation message is included in the cipher text. The proposed scheme requires a user to store more KEYs than BSW. However, it has an effect on reducing the rekeying message size. The proposed scheme is as efficient as the basic BSW in terms of the cipher text size while realizing more secure immediate rekeying in multi authority systems.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

VI. CONCLUSION

Proposed an efficient and secure data retrieval method using CP-ABE 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 hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

VII. FUTURE SCOPE

The proposed scheme features having following achievements:-
i. Immediate attributes revocation boosts up the forward or backward secrecy of secret information by minimizing the windows of vulnerability.
ii. Using any monotone access structure, encryptors can define a fine-grained access policy under attributes issued from any chosen set of authorities.
iii. An escrow-free key issuing protocol can solve the problem of key escrow by exploiting the characteristic of the decentralized DTN architecture.
iv. Hence, users need not to be required to trust the authorities fully in order to protect their data which is being shared.
v. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the remedial scheme.

VIII. ACKNOWLEDGEMENT

The authors are thankful to researchers, publishers. For making the availability of their resources &publications. Teacher's guidance is equally responsible for this paper. We are also thankful to college authorities for providing us basic facilities and equipment which requires. Finally, we would like to extend heartfelt gratitude to friends, family members for their support and encouragement.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop:Routing for vehicle-based disruption tolerant networks," in *Proc.IEEE INFOCOM*, 2006, pp. 1–11.
[2] M. Chuah and P. Yang, "Node density-based adaptive routing schemefor 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. ACMMobiHoc*, 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 DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.
[6] M. Kallahalla, E. Riedel, R. Swami Nathan, Q. Wang, and K. Fu,"Plutus: Scalable secure file sharing on untrusted storage," in *Proc.Conf. File Storage Technol.*, 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] 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.
[11] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*, 2007, LNCS 4329, pp. 515–534.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

BIOGRAPHY

Nikita Bankhele, Student pursing B.E in Computer Engg. from Department of Computer Engg., D. Y. Patil Institute of Engg. & Tech., Ambi, Pune, from Savitribai Phule Pune University, Pune, India.

Priya Deshmukh, Student pursing B.E in Compute Engg., D. Y. Patil Institute of Engg. & Tech., Ambi, Pune, from Savitribai Phule Pune University, Pune, India.

Chandrakant Gawande, Student pursing B.E in Computer Engg., D. Y. Patil Institute of Engg. & Tech., Ambi, Pune, from Savitribai Phule Pune University, Pune, India.

Asst. **Prof**. **Mangesh Manke** received M. Tech. degree from Shivaji University, Kolhapur having 8 years of Teaching Experience as an Assistant Professor. Currently working as Head, Department of Computer Engg., D. Y. Patil Institute of Engg. & Tech., Ambi, Pune, from Savitribai Phule Pune University, Pune, India.