Comparative Model for Secure Data Transmission in Military Networks

Srinath KS[#1], Binesh Kumar Chaurasiya[#2], Rajeev Kumar Das[#3], Swati Verma[#4], Sheela Rani CM[#5]
[#]*Dept. Of CS&E, Sambhram Institute of Techonology,*
Bangalore, INDIA
1solansrinath@gmail.com
2bkc2069@gmail.com
3rajeev.das806@gmail.com
4vermaswati154@gmail.com
5sheela.cm@gmail.com

***Abstract*— In military network, the data transferred should not compromise the confidential information. During transmission in this network, the data is likely to suffer from issues like data breaches, data modification, insecure interface attack, malicious insider attack and data loss attacks performed by some unauthorized user. Cryptography is a promising solution to such issues. Under it, we have few basic techniques such as: IBE (Identity based encryption), ABE (Attribute based encryption) and CP-ABE (Cipher policy- attribute based encryption), which are being used from past few years. In this paper, we have compared IBE, ABE and CP-ABE model for their efficiency in providing high security in decentralized disruption-tolerant military network (DTN). We have implemented these three techniques to check effectiveness of securing the data. The comparison among the three techniques is quite helpful in considering the better and the efficient one. Based on their level of data security needed for a particular domain, the most suitable one can be selected.**

***Keywords*— DTN, IBE ABE, CP-ABE.**

I. INTRODUCTION

Cloud computing has evolved through many phases which include grid and utility, application service provision (ASP) and Software as a service (SaaS). The idea of cloud computing was introduced in the sixties and is attributed to John McCarthy who proposed the idea of computation being delivered as a public utility and to J.C.R. Licklider proposed the idea of intergalactic computer network. Few years back, consumers including various companies with their own servers to maintain company's data and important documents and common people had their own computer system with bytes of useless as well as useful data stored in their computer systems. But, if something goes wrong with the company's server or PCs, or if data is to be accessed from elsewhere; then all the hard work needs to be done. But, emergence of cloud solves all our problems within fraction of seconds [1].

In cloud computing, the word Cloud is used as a metaphor for "the internet" and thus by cloud computing we mean "a type of computing based on the internet". We can define cloud computing as a medium to empower omnipresence, pertaining to convenient required network access to a shared pool of configurable computing resources that can be rapidly obtained for current and future use and released with minimal management effort. Cloud computing is one of the latest categories of web hosting that includes virtual machines and elastic computing.

Cloud has various types such as *private cloud, public cloud, community cloud* and *hybrid cloud*. The *Public cloud*s are shared without any restriction; it can be accessed with internet connection and a credit card. The customer has no visibility and control over where the computing infrastructure is hosted. The *Private clouds* are those which are privately managed and maintained and are restricted to a particular business or just to a part of that business. *Community clouds* are used by collaborative groups. These involve sharing of computing infrastructures in between organizations of same community. *Hybrid clouds* are combination of both public cloud and private cloud. It may be used by a private company or government which needs both private and public clouds.

Private companies like Amazon, Google, Salesforce and Microsoft are using cloud as per their requirements as well as providing various cloud services. These services include online data storage services, web-based email services, data backup solutions, hosted office suites and documents collaboration services, database processing, managed technical support services, virtual cloud services. However, the problem of applying security techniques such as: IBE, ABE and CP-ABE for particular networks causes several security and privacy challenges, Since some users may change their associated attributes at some point , or some private keys might be compromised, key revocation for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in military network scenarios[2][3].

II. PROBLEM SPECIFICATION

As all the other things can never be perfect, there are certain problems with services and technologies of cloud. Various challenges in cloud computing services are VM sprawl challenge, security breaches, scalability problems and cloud automation issues[4][5].

Among all these challenges we will be giving our major concentration on the security issues. It include several problems such as data breaches, data loss, account hijacking, insecure interfaces, denial of service attacks, malicious insiders, abuse of services, insufficient due diligence, shared

vulnerabilities and more. This affects the authentication, authorization, integrity, non-repudiation, and confidentiality of data which reduce the trust on military networks and cloud owners. In this paper, we compare the well known cryptographic mechanisms such as IBE, ABE and CP-ABE for understanding the best technique suitable for particular domain.

III. SYSTEM ARCHITECTURE

In this section, we describe the security model architecture for military networks.

The system architecture has been depicted in the fig. 1. It has a key generator/authority, storage node, sender and receivers.
The **Key generator** is the trusted authority which keeps the keys secret to it. The key generator generates the key pair and stores onto the database. It is assumed that there are secure and trustworthy communication links between a central authority and each local authority during the initial key setup and generation phase[6].

The **Storage** node is a mobile node which keeps on moving along its specified path. These paths are calculated using some algorithms. While the storage nodes move between the sender and the receiver, it is able to transfer the required information to and fro. It can be assumed as partially trusted mobile node.
The **Sender** can be any military personnel (commander) who sends important information to the receiver or local authority through storage nodes [7][8]. It defines the attribute and the access policies in order to ensure security for data being transferred. It encrypts the data using the access policies defined.

The **Receiver** may comprise of one or more groups and each group having one or more members. It retrieves data from storage nodes and decrypts it by satisfying the set of attributes and access policy defined by sender.

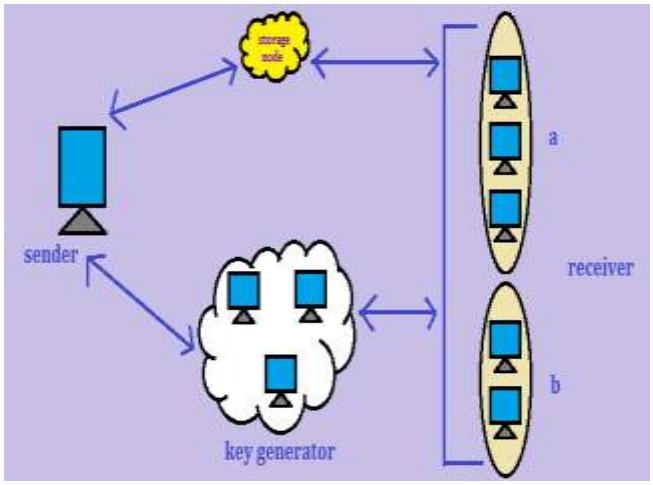

Fig. 1: System Architecture

IV. PROPOSED SCHEME

In this section, we compare IBE, ABE, CP-ABE which provides security to the sensitive information in decentralized DTNs.

A. Identity based encryption (IBE)

Identity based encryption or ID based encryption is a type of public key encryption. In ID based encryption some unique id of the user is used to retrieve the private and the public key. Unique id of the user may be an email id, date of birth or name [9].

In IBE, when the sender is willing to send the data it first intimates the key generator requesting for public key. The sender has to send receiver's id. Key generator will generate the key pair based on the id and stores in its database along. The generator then sends the public key to the sender. He will encrypt the data using public key and sends to receiver. Then, receiver will ask for the private key from key generator, once he gets the key and decrypts the cipher text. The architecture of IBE is shown in the fig. 2.

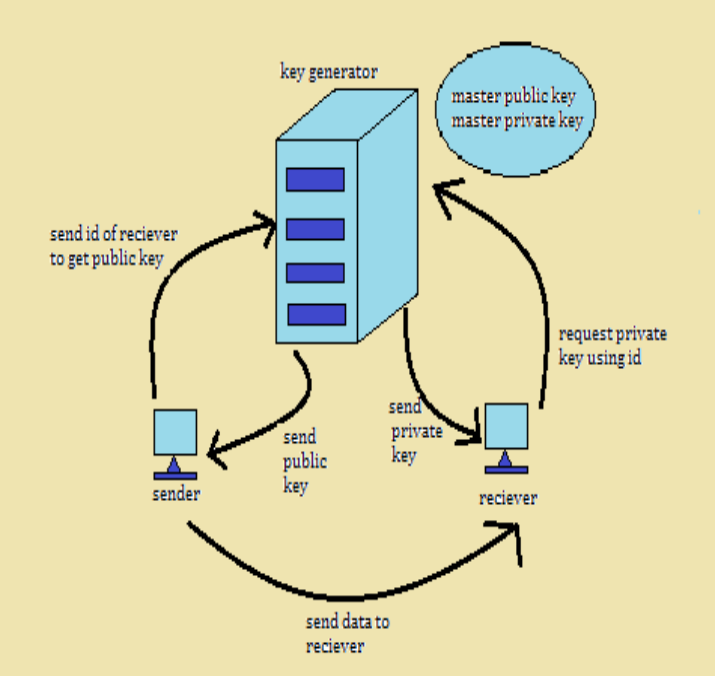

Fig.2: Identity Based Encryption model

IBE system is completed with four algorithms: ***setup, extract, encrypt*** **and** ***decrypt***. These four algorithms will give a quite clear idea of how the system units interact among themselves.
Step 1: The setup is the first algorithm for IBE which runs only once in order to create the entire IBE environment. Setup phase is run by the trusted key generator. It takes the security parameter *k*. Security parameter is just a variable which is used for measuring the length of computational problems and this length is in binary notation. The output of setup algorithm

is a set of system parameters *sp* with cipher text space *c* and message space *m*, and a master key *mk*.
Step 2: In Extract, The key generator runs the extract algorithm whenever a private key is requested by the user. The output of setup algorithm becomes the input to extract algorithm, i.e. master key *mk* and set of system parameters *sp* are the input to this algorithm with an extra parameter unique identifier *id* given by the user. The output of this is the requested private key *pk*.
Step 3: Next comes the encrypt algorithm. The input to this algorithm is the system parameter *sp* and the message $M \in m$, where *M* is to be encrypted with the private key *pk*. The output of extract algorithm is the encrypted cipher text $C \in c$.
Step 4*:* Lastly, the decrypt algorithm takes the system parameter *sp*, unique user id, private key *pk* and encrypted cipher text *C* as its input parameters. The output of this algorithm is the decrypted message.

Advantages of IBE are it was a primary type of public key cryptography. The keys are always considered valid once they are issued. Hence, for finite number of users, after issuing the third party's secret can be destroyed, henceforth the protection of the data over public and private key pair is compromised if there is no procedure for authenticating the user to whom the keys are being provided by the key generator.

B. Attribute Based Encryption (ABE)
ABE is another type of public key encryption, proposed to overcome the issues faced through IBE. When the sender want to send data it will encrypt data based on receiver's attributes and receiver will decrypt the data based on its own matching attributes. The architecture of ABE is quite similar to identity based but instead of just one id we are using more than one attribute to ensure better security. Fig.3 depicts about the ABE model [10].

In ABE the sender will pass receiver's gid (group id) along with some more attributes to key generator. Key generator uses these attributes to generate the key pair and stores them to database and also sends public key to sender. Sender uses this public key to encrypt the data. After encrypting, sender will store this cipher text onto the storage node. Then receiver will provide its id and attribute set to key generator, key generator verifies the receiver and provides the private key. Then receiver retrieves data from storage node and decrypts it using private key received from key generator.

Advantage of ABE is that, it can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. And disadvantage is that, since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure, key escrow problem.

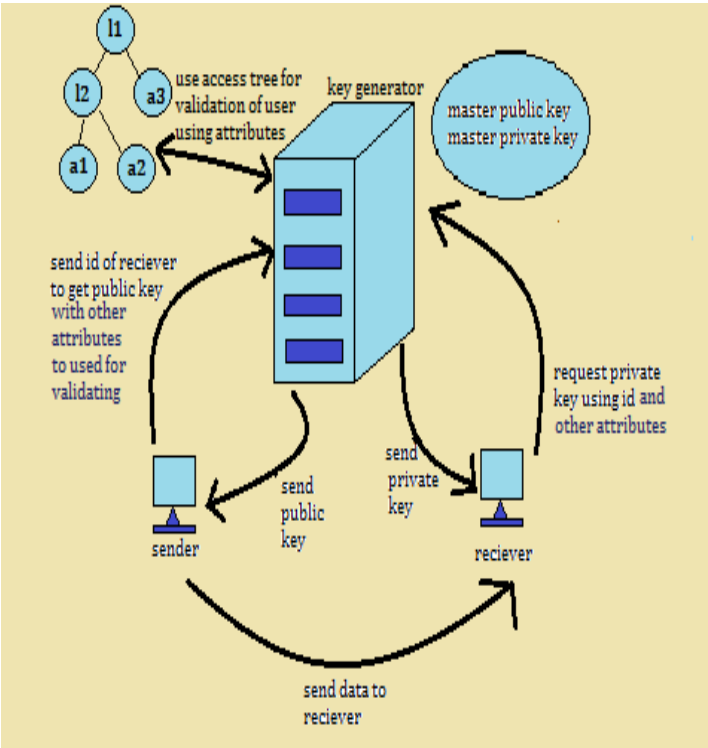

Fig.3 Attribute Based Encryption model

Algorithm For ABE
Unlike IBE, ABE also comprise of four randomized algorithms. They are: *setup*, *encryption*, *key-generation* and *decryption.* Below all these four algorithms are explained.
Step 1: Setup is the first algorithm; setup takes no input as was the case earlier. Only input taken by setup is the security parameter which is in bits. Output of this is the public parameters which will be used by other algorithms as per their respective needs.
Step 2: The next algorithm is the encryption. Encryption takes input the message *m* to be encrypted, the public parameters given by the setup and key. Output of this is an encrypted data i.e. the ciphertext.
Step 3: Key generation is the randomized algorithm whose input is the access structure, master key and the public parameters. It gives the key pair i.e. the private and the public key needed for encryption and decryption.
Step 4: Another randomized algorithm is the decryption; decyption algorithm takes the encrypted data i.e. the ciphertext and the private key which has to be used to decrypt the ciphertext which results out the the decrypted data.

C. Ciphertext Policy Attribute Based Encryption
Ciphertext policy attribute based encryption (CP-ABE) is another cryptographic technique proposed after ABE to overcome the issues of ABE. CP-ABE is almost similar to ABE except that we add a access policy to the ABE technique.

The working model of CP-ABE is shown in the fig.4 it has sender, key generator, storage node and receivers [13][14]. The receiver may have more than one group, here we have considered two groups each having more than one member.

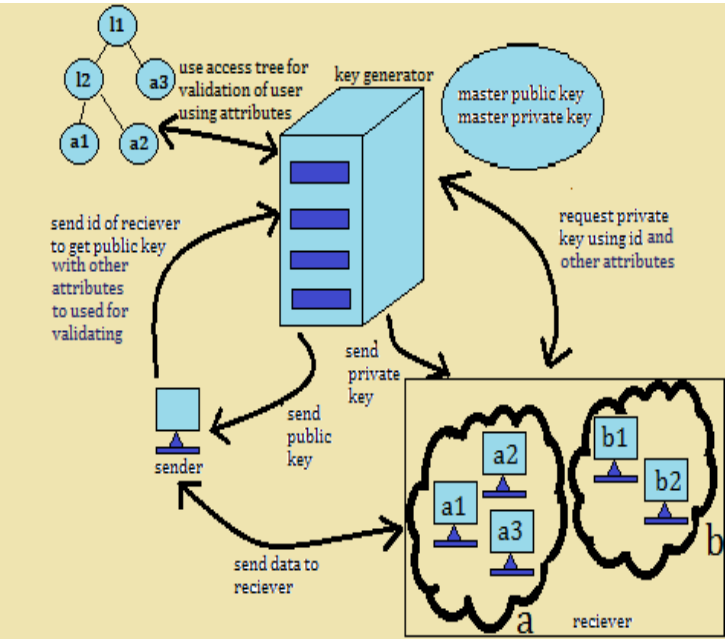

Fig.4: CP-ABE model

In CPABE technique, sender will send the receiver's gid to key generator. Key generator will generate key pair and store to database and sends public key to sender for encryption purpose. Sender will get public key and encrypt data hence ciphertext is generated, then sender will add some access policy to the generated cipher text and will be stored to storage node. Receiver will send its attribute to key generator to get private key, after receiving private key receiver will retrieve ciphertext from storage node and will provide its policy. It will be matched with the policy defined in the ciphertext. If the policies match, the receiver will decrypt the data [12][15].

Algorithm For CP-ABE

A CP-ABE scheme consists of the following four algorithms:

Step 1: Setup: This is a randomized algorithm that takes a security parameter as input, and outputs the public parameters *PK* and a master key *MK*. *PK* is used for encryption and*MK* is used to generate user secret keys and is known only to the central authority.

Step 2: Encryption: This is a randomized algorithm that takes as input a message *M*, an access structure *T*, and the public parameters *PK*. It outputs the ciphertext *CT*.

Step 3: KenGen: This is a randomized algorithm that takes as input the set of a user (say *X*)'s attributes *SX*, the master key *MK* and outputs a secret key *SK* that identifies with *SX*.

Step 4: Decryption: This algorithm takes as input the ciphertext *CT*, a secret key *SK* for an attribute set *SX*. If *SX* satisfies the access structure embedded in *CT*, it will return the original message *M*.

V. ANALYSIS

In this section, , we analyze and compare the efficiency of the results produced by the identity based encryption, attribute based encryption and the cipher-text based encryption Then, the efficiency of these scheme is demonstrated in the network simulation in terms of the communication cost.

A. IDENTITY BASED ENCRYPTION:

In identity based encryption only the receiver id is used. We have considered five receivers and their id's as 'a', 'b', 'c', 'd', and 'e' respectively. The sender sends the encrypted data only to the particular receiver by giving their id's. Time taken to encrypt and decrypt the data is given in the table I. and the fig.5.

TABLE I
Time taken for encryption and decryption

Receiver	Size of Message (bits)	Encryption (ms)	Decryption (ms)	Total Time (ms)
A	20	385	366	751
B	40	410	381	791
C	60	370	340	710
D	80	360	357	717
E	100	406	392	798

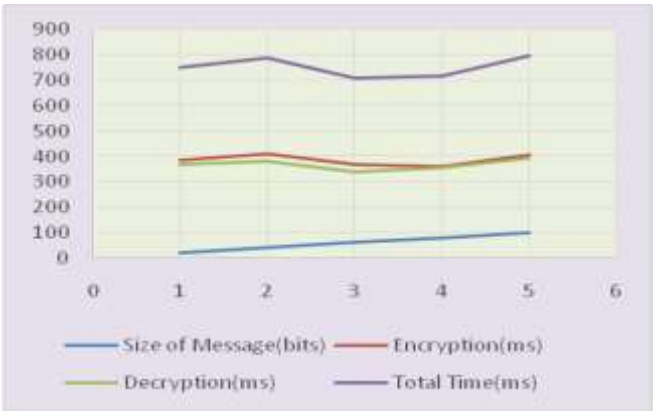

Fig. 5: Graphical representation of time taken for Encryption and decryption in IBE

B. Attribute Based Encryption

The attribute-based encryption may contain many attributes like: name, address, group id etc. Here, we have assumed only two groups: group 'a' and group 'b'. The group 'a' contains three members (name a1, a2 and, a3) and group 'b' has only two members (b1 and b2). Time taken to encrypt and decrypt the data is given in the table II. and the fig.6.

Table II
Time taken for encryption and decryption

Group	Id	Encryption (ms)	Decryption (ms)	Total Time (ms)
A	a1	413	397	810
A	a2	428	403	831
A	a3	446	457	903
B	b1	473	399	872
B	b2	377	387	764

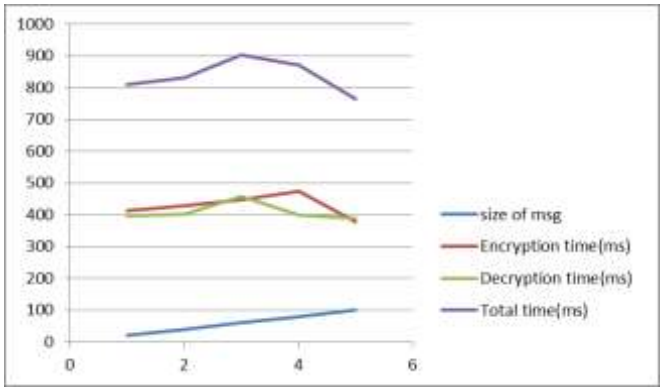

Fig.6 : Graphical representation of time taken to encrypt and decrypt the message

C. CP-ABE

In the CP-ABE, sender will send access policy with ciphertext, so only the user which has valid attributes and the access policy can decrypt the data. For example, we have taken two groups namely 'a' and 'b' [16][17].

After receiving the public key, the sender encrypts the data and makes an access policy and sends both to the cloud. The receiver requests for the private key to the key generator and after receiving the private key it decrypt the data. This process needs some amount of time which is given in the below Table III and the fig.7

Table III
Time taken for encryption and decryption

Group	Size of Message (bits)	Encryption (ms)	Decryption (ms)	Total Time (ms)
A -> a1	20	413	397	810
A -> a2	40	428	403	831
B –> a3	60	446	457	903
B -> b1	80	473	399	872
B -> b2	100	377	387	764

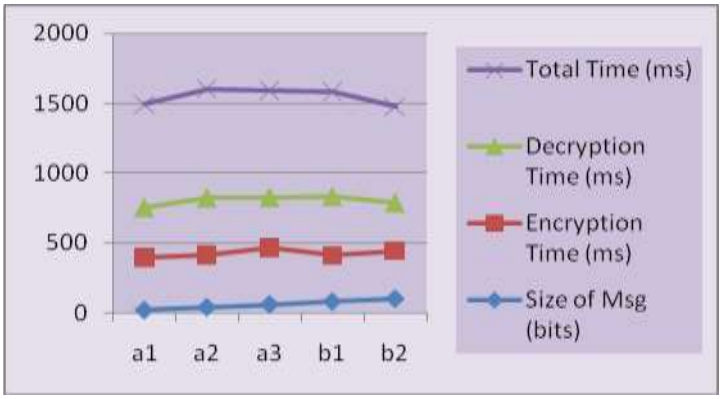

Fig.7: graphical representation for time taken for encryption and decryption

From the above three models we saw that time taken by IBE is the least but since the security level is too low it cannot be considered the best model. Coming to the ABE the time taken is more than IBE but the security level is upgraded as we are using a set of attributes instead of a single id. Finally, comes the CP-ABE; time taken by CP-ABE is same as ABE but it overcomes the issues faced in prior model. Hence, we can say that CP-ABE is better than the other two.

VI. CONCLUSION

Nowadays, DTN technologies are becoming successful in military applications that allow wireless devices to communicate with each other and access the confidential information. IBE, ABE and CP-ABE are the scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we compared afore mentioned efficient data retrieval methods and ensured that CP-ABE is efficient than IBE and ABE in terms of security [18]. We also implemented CP-ABE with multiple key authorities to manage their attributes independently. Further, we can check with fine-grained key revocation for each attribute group.

Authors Information

Srinath K S B.E., M.Tech., MISTE., was born in Bangalore, India. He completed his Bachelor Degree in Engineering with specialization in Information Science and Masters Degree in Technology with specialization in Network and Internet Engineering from Visvesvaraya Technological University, Belgaum, Karanataka. Presently he is working as Assistant professor, Department of Computer Science & Engineering, Sambhram Institute of Technology, Bangalore, India. His areas of interest are Web Service, Web Security, Network security and cryptography.

Binesh Kumar Chaurasiya, pursuing BE, in Computer Science & Engineering from Sambhram Institute of Technology, Bangalore India

Rajeev Kumar Das, pursuing BE, in Computer Science & Engineering from Sambhram Institute of Technology, Bangalore India

Swati Verma, pursuing BE, in Computer Science & Engineering from Sambhram Institute of Technology, Bangalore India.

Sheela Rani C.M. BE, M.Tech., was born in Bangalore, India she Completed her Bachelor Degree in Engineering with specialization in Information Science & Engineering and Master Degree in Technology with specialization in Computer Science. Presently she is working as Assistant Professor, Department of Computer Science & Engineering, Sambhram Institute of Technology, Bangalore, India. Her Area of Interest are Data Mining and Web Mining, Computer Networks.

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

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.

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

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

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

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

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

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

