Secure and Efficient Data Retrieval under Location Based Server in Military Networks

Shwetha M,
4th sem, M tech Department of CSE

Mr.Yashonidhi Yajaman,
Assistant.Professor

SJB Insititute of Technology College , Visvesvaraya Technological University,
Department of Computer science and engineering ,
Bangaluru-60

***Abstract:-* Disruption Tolerant Network(DTN) is network which allows wireless devices to communicate with each other even though when disruption has occurred. Storage nodes were used in Disruption Tolerant Network which stores secure and confidential data when there is no end to end communication. In our proposed system we are using concept of Cipher text Attribute based Encryption scheme where Multiple key authority system is used so any key authority is able to generate the key so that we not depending on single key authority system. By this unauthorized end user are unable get information about which particular key authority is generating key .In our project system proposes novel attackers detection and positioning scheme based on Mobile Location Based Server(LBS) and which helps to find the attacker details in Mobile Phone. In our proposed mechanism we manage the secure and confidential data in Disruption Tolerant Network.**

Key words:Distruption Tolerent Network, Military Network,Multiple key authority system,Location based Server.

1.INTRODUCTION

In military network ,connections of wireless devices are used by soldiers were temporarily disconnected by fault-tolerant, propagation delay, , jamming and mobility when they operate in hostile environments. A disruption-tolerant network is a network designed for the temporary communications . Disruption-tolerant network is successful solutions that allow nodes to communicate with each other in the networking hostile environments and for communication network where source and destination node which do not have end-to-end connection between a source and a destination pair, so messages from the source node may need to wait in the intermediate nodes for a some amount of time until the connection would be eventually established.

The basic idea behind DTN network is that endpoints are not connected continuously. In order to transfer data, DTN uses support of store-and-forward approach across routers in disruption-tolerant network than TCP/IP. DTN approach doesn't necessarily mean that all DTN routers on a network would require large storage capacity in order to maintain end- end to end data integrity. Disruption Tolerant Network is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the would normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications. It is an protocol was developed by Delay and Disruption Tolerant

Research Group which operate on network research task.Roy and Chuah were both[1-2] used the storage nodes in DTNs where data is stored such that only authorized mobile nodes can access the necessary information quickly and efficiently. Military applications require increased protection of confidential and high secure data including access control methods that are cryptographically solutions used. In disruption-tolerant military network, a commander has to store a confidential data in storage node, which has been accessed by B1(Batalion1) members who are participating in “Region 2” because of this multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions, which can be frequently changed . There are aspects which effective the design of a DTN are Fault Tolerant ,heavy traffic load , attacks and having minimal latency when routers are unreliable. Fault-tolerant systems are designed so that if a component fails then network route becomes unusable, route can immediately take its place without loss of any service. At software levels, an interface allows the administrator to continuously monitor network traffic at multiple points and locate problems. Fault tolerance is achieved by components and subsystem redundancy in hardware. One of the original motivations for the development of Internet by Advanced Research Projects Agency of the U.S. government was the desire develop for large-scale communications network that could resist massive physical as well as attacks including global nuclear war. In degradation, system continues working to some extent even when a large portion of it has been destroyed or rendered inoperative. In a DTN, such attacks may not be entirely preventable but their effects are minimized and problems are quickly resolved when they occur. Servers has been provided with help of antivirus software and individual points in system can be protected by programs that was detect and remove by the spyware.

DTNs support interoperability of other networks by accommodating long disruptions and delays between and within those networks, and by translating between the communication protocols of those computer networks. In providing these functions, DTNs accommodate the mobility and limited power of evolving wireless communication devices. DTNs overcome the problems associated with intermittent connectivity, long or variable delay, asymmetric data rates, and high error rates by using store-and- forward message switching.

1.1 Attribute Based Encryption

continued communications. NDBAR scheme can achieve the highest delivery ratio

The concept of attribute-based encryption was first proposed by Sahai , Brent Waters and VIPUL Goyal .It is type of public key encryption in which secret key of user and cipher text are dependent upon attributes. In such system decryption of cipher is possible only if set of attributes of user key matches attributes of Cipher text .In ABE user private key and cipher text are associated with set of attributes. Decryption of cipher text `by user is possible only when at least threshold number of attributes overlap between user private key and cipher text. Attribute- based Encryption systems where encryption and decryption are determined by the attributes of the data and the recipients. An ABE system is designed to enable fine-grained access control of the encrypted data. It allows the encryption to attach attributes or policies to a message being encrypted so that only the receiver(s) who is (are) assigned compatible policies or attributes can decrypt it. The attributes can be considered as Boolean variables with arbitrary labels, and the policies are expressed as conjunctions and disjunctions of the attribute variables. The ABE systems can be seen as the generalization of Identity Based Encryption (IBE) systems.

In IBE systems[5], only one attribute is used which is the identity of the receiver, whereas ABE systems enable the use of multiple attributes. ABE schemes are built by cleverly combining the basic techniques of IBE with a linear secret sharing scheme. we can write the access policies in the form of a monotonic Boolean formula over the attribute variables. Identity-Based Encryption [5-7] (IBE) allows for a sender to encrypt a message to an identity without access to a public key certificate. Fuzzy Identity-Based Encryption in which we view identities as a set of descriptive attributes. The ability to do public key encryption without certificates has many practical applications. user can send an encrypted mail to a recipient, for example shwetha@gmail.com, without the requiring either the existence of a Public-Key Infrastructure or that the recipient be on-line at the time of creation.

Message Ferrying[10] is a network paradigm was proposed by Tarig and Ammar where special node called message ferry that facilitates connectivity in mobile ad hoc network where nodes are sparsely deployed. It focus on ferry method which use active nodes in wireless network for message propagation. Message ferry route design algorithm called an Optimized Way-points which generates a ferry route which assures good performance without requiring any online collaboration between the nodes and the ferry. The OPWP ferry route has a set of way-points and waiting times at way-points, that are chosen based upon the node mobility model. Each time ferry nodes traverses in this route, it contacts each of the mobile node within low minimum probability. The problem in designing ferry routes for arbitrarily moving nodes is that we cannot correctly predict the location of the nodes, and hence it may not be possible for nodes correctly and deterministically define position the ferry to contact the nodes. Ferry mobile nodes in Ad-hoc if any Disruption has been occurred in networks.Node-Density Based Adaptive Routing (NDBAR) scheme[11] was proposed by Chuah and yang that allows regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of(compared to other DTN routing approaches) in very sparse ad hoc networks that are prone to frequent disruptions. Node density Based Adaptive Routing Which focus on only active nodes in network and it won’t support store and forward approach.Disruption-tolerant networks (DTNs) attempt to route network messages through intermittently connected nodes. Routing mechanism in such type of environments is difficult because peers have little information about the state of the partitioned network and transfer opportunities between peers are of limited duration. MaxPropa protocol[12] for effective routing of DTN messages. MaxProp is based on prioritizing schedule of packets transmitted to other nodes and the schedule of packets had been dropped. These priorities are mainly based on the path likelihoods to nodes according to historical data and also it has several complementary mechanisms including head-start for the packets, and lists of previous intermediaries attempt. It maximize the efficiency of messages delivered through DTN in intermittently connected network. This is achieved by prioritizing the schedules in sending messages. This approach is good because in DTNs the adjacent nodes have little to no information regarding the neighbouring nodes. It does not provide any emphasis on security aspects of data transmission. The concept of attribute-based encryption (ABE) [13-14] is a promising approach that fulfills the requirements for secure information retrieval in DTNs. ABE features which enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. In existing ABE Schemas[15-16] are constructed on architecture where single trusted authority has the power to generate whole private keys of users with its master key information.

The problem of applying the ABE to DTNs introduces several security issues and privacy issues. Since some users may change their attributes at some point of time and some private keys might be compromised so secrete key should be revoked for each attribute is necessary in order to make systems high secure. In ABE Systems each attribute has been shared by multiple users. Revocation of any attribute or any single user in an attribute group would affect the other users in the group. when user newly joins or leaves an attribute group, the associated of particular attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in problems during rekeying procedure and security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

Bethencourt and Boldyreva[17-18] suggested key revocation mechanisms in CP-ABE and KP-ABE. Their solution are to append to each attribute an expiration date and distribute new set of keys to valid users after expiration. The periodic attribute revocable ABE Schemes has two main problems. The first problem is security degradation in terms of backward and forward secrecy[19].It is a considerable scenario that users such as soldiers may change their attributes frequently for example position or location move when considering these as attributes be able to access previous data encrypted before obtains attribute until the data is reencrypted with newly updated attribute keys by periodic rekeying. The other problem is scalablity problem. The key authority periodically update key by uncast at each time slot so that all nonrevocked users can update their keys.

Chase presented distributed KP-ABE scheme [19-20] where all attributes authorities are participating in key generation protocol in distributed way such that they cannot pool their data and link multiple attributes sets belonging to same users. In Distributed system[21-22] any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of parameters. A party can used as an ABE authority by generating a public key and issuing private keys to different users that react with their attributes. A user can encrypt data in terms of Boolean formula over attributes issued from any chosen set of authorities. The distributed system does not require central authority and leads to performance degradation. In distributed system when there is no centralized authority facility with master secret information, all attribute authorities should communicate with each other in system to generate user's secret key.

C. Contribution

In our project we are providing security for military data i Disruption tolerant network. We are using storage node in upload and receive the file. In existing system we had been depended on single key Authority System. We are using AES algorithm for data encryption which data stored in storage node. The secret key is generated by using key generation unble to receive data .The attackers are trying to receive the data by entering the wrong file name ,wrong attributes and keys. In our project we are using location based server (LBS) to find the information about attackers in mobile phone.

2 SYSTEM DESIGN AND ANALYSIS

A .Description of system Architecture

Architecture describes how secure and confidential data sent from sender (commander) to receiver via storage node. In military network where communication of end users are suffered from network problem because of disruption in network. when there is no end to end communication between sender and receiver where Disruption Tolerant network allows file which contains data are sent by sender it will allow to wait for some amount of time in storage node until connection has established. The data stored at storage node which is encrypted and decrypted by cryptographic algorithm such as AES algorithm. Architecture consist of sender(Commander) , receiver(soldiers), storage node and key Authoritys.

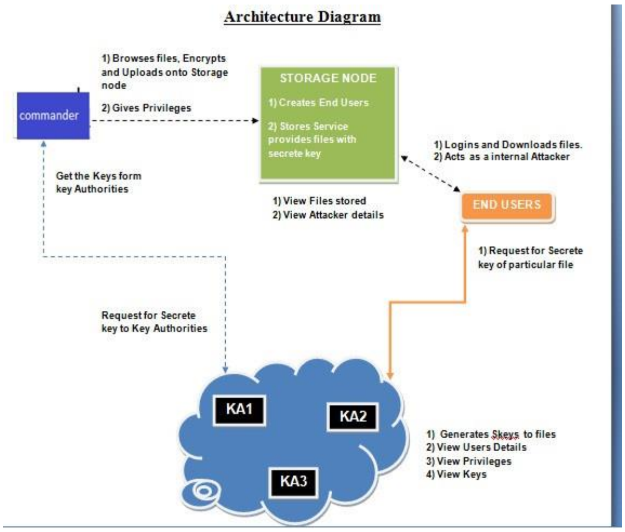
Architecture Diagram
commander
1) Browses files, Encrypts and Uploads onto Storage node
2) Gives Privileges
STORAGE NODE
1) Creates End Users
2) Stores Service provides files with secrete key
1) Logins and Downloads files.
2) Acts as a internal Attacker
END USERS
Get the Keys form key Authorities
1) View Files stored
2) View Attacker details
1) Request for Secrete key of particular file
Request for Secrete key to Key Authorities
KA1
KA2
KA3
1) Generates Skeys to files
2) View Users Details
3) View Privileges
4) View Keys

Fig 1:Architecture Diagram of secure Military data retrieval in Disruption Tolerant Network

A. *System Description and Assumptions*

Fig. 1 shows the architecture of the DTN. As shown in Fig. 1, DTN architecture consists of following system entities:

1.Sender

In this module, the Sender is responsible for registering the Users by providing details Name, Password, Confirm Password, Battalion (b1,b2,b3,b4) , Region(R1,R2,R3,R4). Sender Browses the data File, encrypts it and gets the key from Key Authority Server (KA1, KA2, and KA3). Uploads their data files to the Storage Node and sender is authenticated to provide privileges for End User.

2.Disruption Tolerant Network Router

The Disruption Tolerant Network Router (DTN) technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. In this module we are using storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. In Disruption Tolerant Network Encrypted data file details will be stored Storage Node.

3.Key Authority

The key authority (KA1, KA2, and KA3) is responsible to generate the secret key for the file belongs to the particular Battalion and region. The End User Request to the storage node using the file Name, secret key, Battalion and Region, Then storage node connect to the respective Key authority server. If all specified Details are correct then file will sent to the end user, or else he will be blocked in a storage node. The Key Authority server can view the users, privileges of end user, secret keys. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys.

4.End User

In this module, the End user can access the file details and end user who will request and gets file contents response from the DTN Router. If the credential file name and secret key is correct then the end user will get the file response from the router in Decrypted format.

3. PROPOSED SCHEME

In this section, we provide a multi authority Key Authority scheme for secure military data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. In multiple key authority system any key authority can generate secret the key so that attacker wont get information that which particular key authority is generating key. The scalability and security can be enhanced in the proposed scheme. In our proposed system we are using Location Based Server (LBS) in order to view attacker details in mobile phone.

A. Location Based Server(LBS)

The Data Storage‘s attack is a severe attack that can be easily launched by a pair of external attackers in Wireless Networks. In this attack, an attacker sniffs packets or data at one point in the network by using wrong file name or wrong secret key or by entering wrong attributes for corresponding file. In our system we proposes novel attackers detection and positioning scheme based on mobile (Location Based Server) LBS, which can not only detect the existence of Storage Node attacks, but also accurately localize the attackers for the system to eliminate them out of the storage network. The mobile user can connect with the LBS Server via Bluetooth device to communicate with the mobile. The user will find the Bluetooth server name and then login into mobile to view all current attackers in the Storage Node in Disruption Tolerant networks. Figure 2 describes the how the attacker details in storage node can be viewed in mobile phone with the help of Location Based Server(LBS).

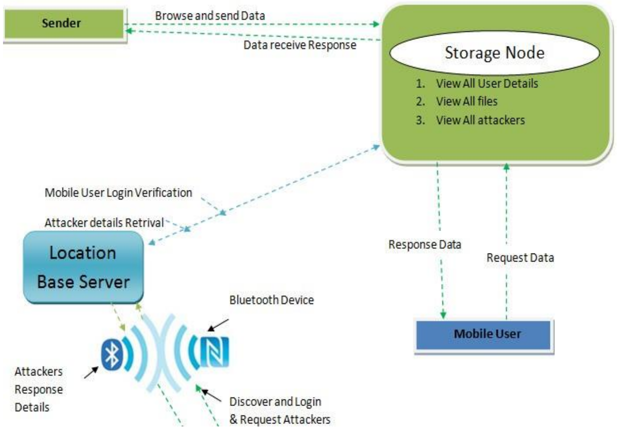

Figure2 Architecture of Mobile Location Based Sever

ipher text policy attribute Based Encryption

A cipher text policy attribute based encryption scheme consists of four fundamental steps:

Setup: The setup step outputs the public parameters PK and a master key MK.

Key Generation (MK,S**):** The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

Encrypt (PK,A, M**):** The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a cipher text CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. Assume that the cipher text implicitly contains A.

Decrypt(PK,CT,SK**):** The decryption algorithm takes as input the public parameters PK, a ciphetext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the cipher text and return a message M.

C. Data Encryption and Description Algorithm

In our paper data has to be stored in secured way using Cryptographic solutions. The data that’s has be stored at storage node should be converted into cipher text so we using AES Algorithm for data encryption and decryption. In our project we are using Advanced Encryption Standard Algorithm for data encryption at storage node when sender upload the file that contains data and also used for data decryption at storage which he receive the file. In following graphs we comparing encryption time and decryption time of AES and RC4 .AES which Encryption and Decryption time is less compared to RC4 so we using AES as cryptographic algorithm.

In our project, 128 bit AES key is generated using secret key given to all node during deployment time .This key is then used for encryption and decryption. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption. In our paper file which contains data that has to. be encrypted so AES algorithm will choose any one keyword in file that contains data. By using that data will encrypted.

D. Key Generation Algorithm

we are using multiple key authority system in cipher text based attribute encryption scheme. we are using secret key for uploading the file and for attribute encryption and receive data from sender. While he receiving data the end user has enter his attributes to decrypt data so all attributes has to be satisfied. Attacker who trying to take data he unable take data because attributes are encrypted .We are using key generation algorithm as RSA algorithm to generate secret key and public key parameter .RSA algorithm uses some random number to generate secret key. The commander has to enter secret key to upload the file and same key has enter receive file which contain data.

4. ANALYSIS

In proposed scheme we using multiple key authority system so we not depend on single key authority system to generate secret key. Here we browsing and uploading file at storage node so that data should be encrypted. In graph we showing upload delay time graph. In graph we calculated how much time is taken to upload the file at storage node. either unless the rest of the attributes of him satisfy the access policy[30-33]. In order to decrypt data by receiver so all attributes should be satisfied. Data is confidential because attributes are encrypted so that attacker are not able to take data because he cont get attribute information. we providing download permission to end user to access data. The attributes are associated with end user are encrypted at storage node so attackers are unable to get data sent by sender. Location Based Sever is connected to mobile phone with the help of Bluetooth so mobile user can view the details of attackers and find the location of the attacker

5. SECURITY

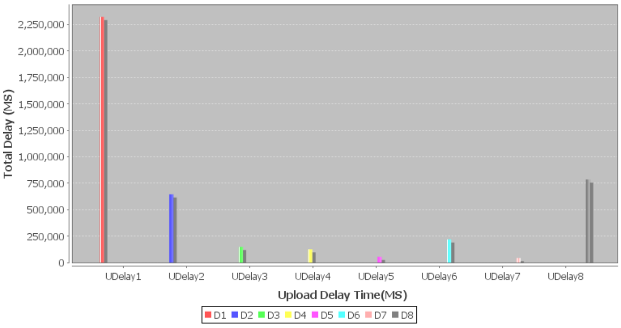

Fig 3:Delay time graph

DTN technologies helps in military applications to access secure and confidential data which allows the commander and soldiers can communicate even though disruption has been occurred in military network environment. we are using CP-ABE scheme where multiple key authorities are used who are responsible for generating key and manage their attribute independently .In multi authority system any key authority can give key so that attackers are unable get information that which key authority is generating the key. In our system receiver has to entered his attribute list to

In this section, we prove the security of our scheme with regard to the security requirements .

A. Collusion Resistance

Collusion-resistance: If multiple users collude, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone [11]–[13]. Consider that existing a user with attributes
{Battalion 1, Region1} and another user with attributes
{"Battalion2", "Region2"}. They may succeed in decrypting a cipher text encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually[22-25]. We do not want these attackers to be decrypt the secret information by combining their attributes.
The colluding revoked user scan by no means obtain any valid attribute group keys for attributes that they are not authorized to hold. Therefore, the desired value cannot be recovered by collusion attack since the blinding value is randomized from a particular user's private key. Collusion among the local authorities could determine the personalized key component of some user . Each attribute key component of the user is blinded in the local authorities' view in that they are divided by the secret , which is only known to the user and . The colluding local authorities cannot derive the whole set of secret keys of users.

ata confidentially

In our trust model, the multiple key authorities are no longer fully trusted as well as the storage node even if they are honest. Therefore, the plain data to be stored in secret way.
Data confidentiality on the stored data against unauthorized users can be trivially guaranteed. If the set of attributes of a user cannot satisfy the access tree in the cipher text, he cannot recover data sent by sender during the decryption process, where is a random value uniquely assigned to him. when a user is revoked from some attribute groups that satisfy the access policy, he cannot decrypt the cipher text
decrypt data so all attributes should be satisfied and all attributes and secret key in storage node are encrypted so attackers are unable to get the data and information about attributes In proposed system .we are using Location Based Server to find attacker details in mobile phone also detect attackers. key escrow problem is resolved the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not full trusted.

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 enforcementin 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.

[19] S. Mittra, "Iolus: A framework for scalable secure multicasting," in *Proc. ACM SIGCOMM*, 1997, pp.277–288. [20] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in *Proc. Symp. Identity Trust Internet*, 2008, pp.26–35.

[21] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE,"in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp.456–465.

[22] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policyattribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.

[23] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proc. ASIACCS*,2009, pp. 343–352.

[24] 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.

[25] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*,2007, LNCS 4329, pp. 515–534.

[26] S. S.M. Chow, "Removing escrow from identity-based encryption," in *Proc. PKC*, 2009, LNCS 5443, pp. 256–276. [27] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials," in *Proc. TCC*, 2008,LNCS 4948, pp. 356–374.

[28] M.Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss,A.Hysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in *Proc. Crypto*, LNCS 5677, pp.108–125.

[29] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proc. CRYPTO*, 2001, LNCS 2139, pp.41–62.

[30] C. K.Wong,M. Gouda, and S. S. Lam, "Secure group communications using key graphs," in *Proc. ACM SIGCOMM*, 1998, pp. 68–79.

[31] Junbeom Hur and Kyungtae Kang," Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", Member, IEEE, ACM