An Efficient and Secure Data Retrieval for Scalable Military Networks

[1]Ch.Keerthi, [2]Dr. R. Jegadeesan [3]V.Priya, [4]T.Akhila,[5]B.Pavan Sai,[6]V.Neelima

[1,3,4,5] Students of Information Technology,[2,5]Associate Professor

[1],[2,3,4,5,6]Jyothishmathi Institute of Technology and Science

Abstract : *Mobile nodes in military environments such as a battle field or a hostile region are possible to attack from intermittent network property and frequent partitions. Disruption-tolerant network technologies are turning into self-made solutions that permit wireless devices carried by troopers to communicate with one another and access the direction or command dependably by exploiting memory device nodes. A number of the foremost difficult problems in this state of affairs are the social control of authorization policies and the policies update for secure knowledge retrieval. Cipher text policy attribute-based encoding may be a promising cryptological answer to the access management problems. However, the matter of applying cipher text-policy attribute-based encoding in suburbanised disruption tolerant networks introduces many security and privacy challenges with relevancy the attribute revocation, key escrow, and coordination of attributes issued from multiple authorities. Secure knowledge retrieval theme is proposed to victimization cipher text-policy attribute-based encoding for suburbanised disruption-tolerant network wherever multiple key authorities manage their attributes severally and also demonstrate a way to apply the planned mechanism to firmly and with efficiency manage the confidential knowledge is confined within the disruption-tolerant military network.*

IndexTerms **-** Access control, attribute based encryption (ABE), disruption tolerant network(DTN), multi-authority, secure data retrieval.

1. INTRODUCTION

In military networks, connection of mobile nodes can be disconnected by jamming, environmental factors and mobility and specially when they are operated in hostile field. Disruption Tolerant Network technologies able nodes to communicate with each other even in extreme networking environments [1]. When their is no connection between source and destination pairs, the messages sent from source nodes need to wait in the intermediate nodes for some time until the connection is established.

Storage nodes in DTNs [2] are introduced to store the data so that only authorized mobile nodes can access the information. To secure the confidential data it need high protection including access control methods that supports cryptographic schemes [3]. Data access policies are defined over user attributes which can manage key authorities. DTN architecture is also referred where multiple authorities issue and manage their own attribute keys independently as decentralized DTN [4].

Attribute-based encryption(ABE) [5] fulfills the requirements for secure data retrieval in DTNs. It enables access control over encrypted data using access policies and described attributes among private key and cipher text. Cipher text-policy ABE(CP-ABE) provides a scalable way for encryption where encryptor defines attribute set so that decryptor can easily decrypt the cipher text [6]. So, that different users can decrypt data with security policy.

The problem of applying the ABE to DTNs introduce security and privacy challenges so that users may change their attributes at some point or some private keys will be compressed, to need systems secure, key revocation is needed. This issue is more difficult in ABE systems, since multiple users share the same attribute. This shows that revocation of that particular attribute would effect on each user in a group.

Key escrow is another challenge. In CP-ABE, key authority generates the private key of user by considering the authority master key to the user which is associated with set of attributes. So, the key authority can decrypt any cipher text which is assigned to user by using the general attribute keys. The compression of key authority the potential threat for privacy especially when the data is highly sensitive. This is a key problem even in multiple authority systems until each key authority have its own attribute keys with own master secrets. So, such key generation mechanism based on the single master secret removes key escrow in single or multiple authority CP-ABE.

The coordination of attributes issued from multiple authorities is the last challenge. Authorities can manage to issue attribute keys to the user independently by using their own master secrets. But the multiple authorities is impossible to issue an attribute and it is very hard to define fine grained access policy. The multiple authorities can use AND, OR logic schemes. But the OR logic scheme cannot be implemented. From this the different authorities can generate their own attribute keys using their own independent master secret key. Every authority have their own individuality. So, the "n-outof-m" scheme cannot be expressed in any previous schemes, because it is very practical and commonly required access policy logic.

2. RELATED WORK

In key-policy Attribute Based Encryption (KP-ABE), the encryptor only gets to describe a cipher text with set of attributes. Each user will be chosen a policy by the key authority that shows which cipher text the user can decrypt and issues key for each user by embedding the policy into the user's key. The roles of cipher texts and keys are reversed in cipher text-policy Attribute Based Encryption (CP-ABE) that means the cipher text is encrypted by the policy that is chosen by encryptor, but the key is created related

to the attribute set. CP-ABE is more appropriate to Disruption Tolerant Networks than KP-ABE because it allows encryptor to choose a policy on attributes and to encrypt secret information [2].

1)Attribute Revocation:

In order to overcome the problem of attribute revocation, the author proposed the Cipher-text policy based attribute based encryption scheme. This scheme provide selective structure secure based on the assumption of parallel Bilinear Diffie-Hellman Exponent. This carryoutthe performance analysis and experimental verification inorder to achieve attribute revocation without any participation of attribute authority [7].

A mediated Cipher text-Policy Attribute-Based Encryption (mCP-ABE) is also proposed which extends CP-ABE with instantaneous attribute revocation and also demonstrate the application of mCP-ABE scheme to securely manage Personal Health Records (PHRs) [5].

The Cipher text Policy Attribute primarily based secret writing (CP-ABE) system tend to target a very important issue of attribute revocation that is cumbersome for CP-ABE schemes. Particularly, to re-solve this difficult issue by considering additional sensible situations within which semi-trustable on-line proxy servers are offered. This tend to bring home the bacon this by unambiguously desegregation the authority to delegate most of hard tasks to proxy servers. Formal analysis shows that our planned theme is demonstrably secure against chosen ciphertext attacks and also tend to show that this technique also can be applicable to the Key-Policy Attribute primarily based secret writing (KP-ABE) counterpart [8].

2)Key Escrow:

The centralized approach is proposed where single key distribution center distributes the secret keys and also the attributes to all the users. This scheme resilient to replay attacks. This uses secure Hash algorithm for authentication purpose [9].

Group communication will take pleasure in scientific discipline multicast to realize ascendable exchange of messages. However, there's a challenge of effectively dominant access to the transmitted knowledge. The scientific discipline multicast by itself doesn't offer any mechanisms for preventing non-group members to possess access to the cluster communication though coding will be wont to shield messages changed among cluster members, distributing the cryptological keys becomes a difficulty. Researchers have projected many totally different approaches to cluster key management. Reasearch approaches will be divided into 3 main classes: centralized cluster key management protocols, localised architectures and distributed key management protocols [10]

3)Decentralized ABE:

Routing is a critical issue in the intermittently connected networks. Maxprop, is a protocol for effective routing of Disruption Tolerant Network (DTN) messages. This priorize the packets based on the routing to peers. Maxprop performs better than other protocols in scheduling the meeting between peers. Maxprop on simulated topologies are also evaluated to show the performance of various DTN environment [1].

Attribute based mostly cryptography (ABE) determines coding ability supported a user's attributes in a very multi-authority ABE theme, multiple attribute-authorities monitor completely different sets of attributes and issue corresponding coding keys to users, and encryptors will need that a user get keys from authority before decryption. Chase gave a multi-authority ABE theme victimisation the ideas of a trustworthy central authority (CA) and world identifiers (GID). However, the CA therein construction has the ability to decipher each cipher text, that looks somehow contradictory to the initial goal of distributing management over several probably untrusted authorities. Moreover, therein construction, the utilization of the same GID allowed the authorities to mix their data to make a full commoner with all of a user's attributes. Multi-authority encryption tend to propose an answer that removes the trustworthy central authority, and gives protection to the users' privacy by preventing the authorities from pooling their data on specific users, so creating ABE additional usable in observe.

3. SYSTEM ARCHITECTURE

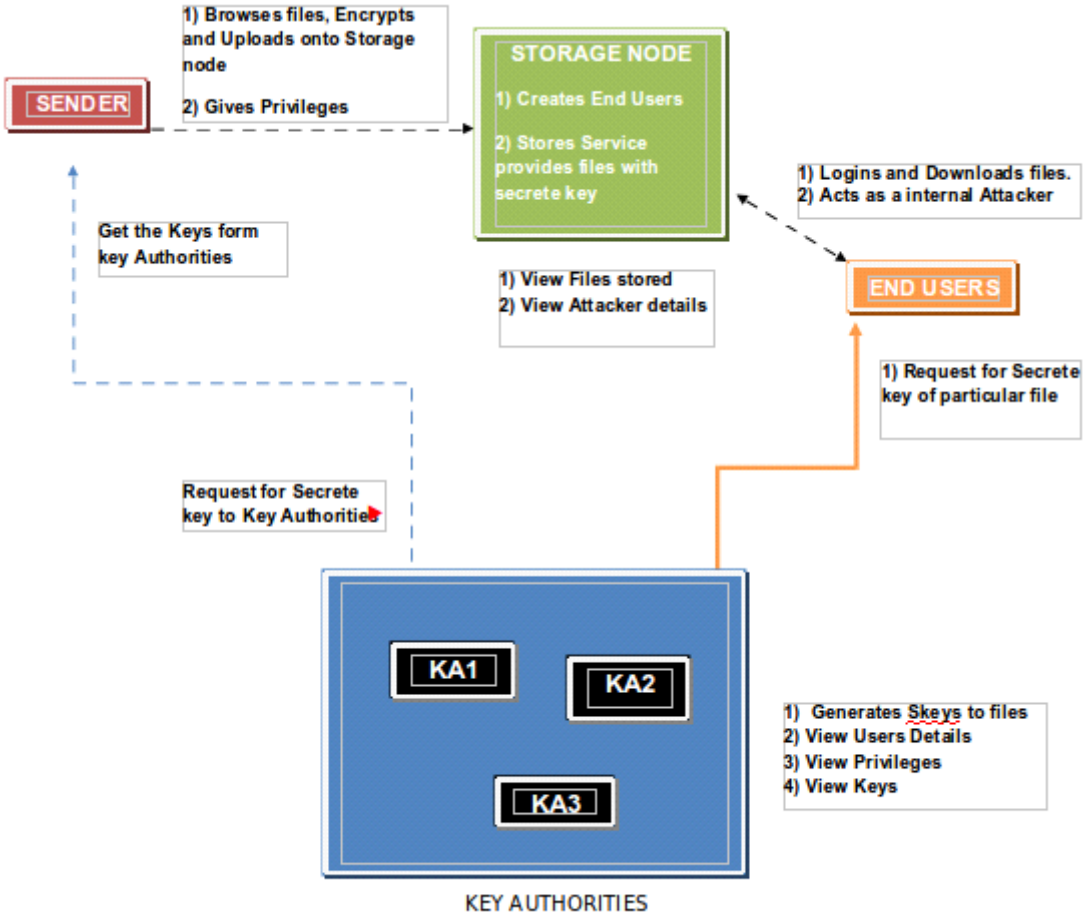

fig1:Architecture of an efficient and secure data retrieval for scalable military networks

- **Sender**

In this module, the sender is responsible for registering the users by providing detailed Name, Password, Confirm Password, Battalion(b1, b2, b3), Region(R1, R2, R3). Sender browses the data file, encrypts it and gets the key from key authority server(KA1, KA2, KA3). Uploads their data files to the storage node and sender is authenticated to provide privileges for end user.

- **Storage node**

The Disruption Tolerant Network Router (DTN) technologies are becoming successful solutions in military applications that allow wireless devices to transmit information between one another and protects the confidential information from attacking by external storage nodes [4]. In this module we introduced storage nodes in DTNs where data is stored or replicated such that the information can be access by authorized mobile nodes quickly and efficiently. In DTN encrypted data file and details will be stored Storage Node.

- **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, keys. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys.

- **End User**

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.

4. SCHEME CONSTRUCTION

The Cipher – SubBytes:
AES's single S-Box
Does a non-linear substitution which is invertible
For Each Byte of Input, {AB}
1. Let {XY} := the multiplicative inverse of {AB} in Galois field GF(2^8)
2. Let {AB}' := An affine transform of {XY}

The Cipher – ShiftRows:
Cyclical Shift of the rows of the state

The Cipher – MixColumns:
Each column is treated as a four-term polynomial.
Polynomial is applied to each column, returning a new polynomial.
a(x) = {01}x^3 + {02}x^2+ {03}x + {04}

The Cipher – AddRoundKey:
From Cipher Key K the key expansion is taken and makes 4*NR 32-bit words, where NR = Number of Rounds
AddRoundKey takes 4 words and the next 4 Round Keys, and returns a new state
For each column, return Col ⊕Key l+i, l = Round#, i =column#

The Cipher - Key Expansion:
Let the initial key size be 128, 196 or 256, and the number of rounds NR, will generate 4*(NR+1) 32-bit words
Uses SubWord function that applies SubByte to 4 bytes
Uses RotWord function that permutes a set of 4 words
First 4-8 Round Keys are cipher key
Later keys are generated based on the given functions.

The Cipher – Inversion:
Every sub-function of the Cipher is exchangable
SubBytes: Reverse the Affine Cipher, then find the Inverse of the result
ShiftRows: Shift the rows by reverse amounts
MixColumns: For each column, inverse matrix is applied.
AddRoundKey: AddRoundKey is used again with same key.

Security of AES:
Certain security attacks exist for the implementations of AES. These don't exploit the particular cryptography of the cipher, however instead attack however specific versions are enforced
Ex: victimization temporal order Attacks to guess Secure Socket Layer Keys
Usually, these attacks need the flexibility to run code on the victim machine. terribly robust options in-built to avoid DES-style attacks. Use of finite field inversion within the S-Box construction helps build Linear and Differential attacks tough. MixColumns helps make sure that there are not any "narrow" methods victimization solely some S-Boxes, once more preventing Linear and Differential attacks.

5. Security:

A. Collusion Resistance:

In CP-ABE, the key sharing ought to be installed into the cipher text rather to the non-open keys of clients. much the same as the past ABE plans, the non-open keys of clients are unpredictable with customized irregular qualities hand-picked by the such they can't be joined inside the anticipated plan. in order to unravel a cipher text, the conniving assailant ought to recoup . To recuperate this, the attacker must attempt from the cipher text and from the inverse plotting clients' non-open keys for a quality. Be that as it may, this outcomes in the value dazzle by some arbitrary esteem, that is unambiguously selected to each client, regardless of whether the property amass keys for the properties that the client keeps are as yet legitimate. This cost are regularly visually impaired out if and on condition that the client has the enough key components to fulfill the key sharing plan implanted inside the cipher text. Another intrigue assault situation is that the plot between repudiated clients to get the legitimate characteristic bunch keys for a couple of properties that they are not affirmed to claim. The trait bunch key appropriation convention, that is finished subtree strategy inside the anticipated subject, is secure regarding the key indistinguishable quality. In this way, the conspiring repudiated clients can in no way, shape or form that get any substantial trait group keys for characteristics that they're not affirmed to convey. In this way, the predetermined esteem can not be recouped by intrigue assault since the cost is unpredictable from a chosen client's non-open key. Plot among the local experts may affirm the customized key piece of some client . In any case, each property key piece of the client is blinded inside the local experts' perused in that they're separated by the mystery, that is scarcely

far-celebrated to the client and CA. Along these lines, the conspiring local experts can't determine the full arrangement of mystery keys of clients.

B. information Confidentiality:

In our trust model, the multiple key authorities don't seem to be any more totally certain what is more as a result of the storage node whether or not or not they're honest. Therefore, the plain data to be hold on must be unbroken secret from them what is more as from unauthorized users. knowledge confidentiality on the hold on data against unauthorized users are usually trivially secured. If the set of attributes of a user cannot satisfy the access tree inside the cipher text, he cannot recover the required worth throughout the cryptography methodology, wherever may be a random value unambiguously appointed to him. On the other hand, once a user is revoked from some attribute groups that satisfy the access policy, he cannot rewrite the cipher text either unless the access policy must satisfy remainder of the attributes . so as to rewrite a node for associate attribute , the user has got to mix from the cipher text and from its personal key. However, this cannot cause the price , that's desired to come up. Another attack on the hold on data are usually launched by the storage node and additionally the key authorities. Since they can't be whole sure, confidentiality for the hold on data against them is another essential security criteria for secure information retrieval in DTNs. The native authorities issue a set of attribute keys for his or her managing attributes to associate documented user u , that are blind by secret information that's distributed to the user from CA . They additionally issue the user a individualized secret key by liberal arts the secure 2PC protocol with CA . As we've got a bent to mentioned in Theorem one, this key generation protocol discourages each party to urge every other's master data to determine the complete set of secret key of the user severally. whether or not the storage node manages the attribute cluster keys, it cannot rewrite any of the nodes within the access tree within the cipher text. this can be as a results of it's alone authorized to re-encrypt the cipher text with each attribute cluster key, but isn't allowed to rewrite it. Therefore, data confidentiality against the curious key authorities and storage node is to boot ensured.

C. Backward and Forward Secrecy:

When a user involves hold a group of attributes that satisfy the access policy at intervals the cipher text at ages instance, the corresponding attribute cluster keys are updated and sent to the valid attribute cluster members firmly. additionally, all of the elements encrypted with a secret key s within the cipher text are re-encrypted by the storage node with a randoms , and conjointly the cipher text elements corresponding to the attributes are re-encrypted with the updated attribute cluster keys. whether or not or not the user has hold on the previous cipher text modified before he obtains the attribute keys and conjointly the holding attributes satisfy the access policy, he cannot rewrite the receptive cipher text. this will be as a results of, whether or not or not he can succeed computing from this cipher text, it'll not facilitate to recover the required value for the previous cipher text since it's blind by a random . Therefore, the backward secrecy of the hold on data is secure at intervals the projected theme. On the alternative hand, once a user involves drop a group of attributes that satisfy the access policy at ages instance, the corresponding attribute cluster keys are updated and sent to the valid attribute cluster members firmly. Then, all of the elements encrypted with a secret key at intervals the cipher text are re-encrypted by the storage node with a random , and conjointly the cipher text elements corresponding to the attributes are re-encrypted with the updated attribute cluster keys. Then, the user cannot rewrite any nodes such as the attributes once revocation due to the resulted from freshly updated attribute cluster keys. in addition, whether or not or not the user has recovered before he was revoked from the attribute groups and hold on that, it'll not facilitate to rewrite the next cipher text re-encrypted with a replacement random . Therefore, the forward secrecy of the hold on data is secure at intervals the projected theme.

6. CONCLUSION

DTN technologies are becoming successful solution similar applications that permit wireless devices to speak with one another and access the confidential info reliably by exploiting external storage nodes. CP-ABE is a solution to the access control and secure data retrieval issues. An efficient and secure information retrieval technique exploitation CP-ABE is proposed for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key written agreement drawback is resolved such the confidentiality of the hold on information is secure even beneath the hostile setting wherever key authorities could be compromised or not totally sure. Additionally, the fine-grained key revocation will be finished every attribute cluster. we have a tendency to demonstrate a way to apply the projected mechanism to firmly and efficiently manage the confidential information distributed within the disruption-tolerant military network.

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 andP.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, "Message ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37–48.

[4] 1.Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[5].Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013 "A Recent Approach to Organise Structured Data in Mobile Environment" R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

[6] Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[7] Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013) "Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[8] Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014 "NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD" Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

[9] Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014 "SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups" Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[10] Jegadeesan,R.,SankarRam,T.Karpagam March-2014 "Defending wireless network using Randomized Routing process" International Journal of Emerging Research in management and Technology

[11] Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

[12] Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[13] Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

[14] Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

[15] Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[16]. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., "Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission" International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018

[17]. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G "Health Monitoring System Using Internet of Things" International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.

[18] S.Roy and M.Chuah,"Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[19] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.

[20] 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.

[21] 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.

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

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

[24] 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.

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

[26] 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.

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

[28] Guangbo Wang and Jianhua Wang, Ciphertext-Policy Attribute Based Encryption with Attribute Level User Revocation in Cloud Storage, Mathematical Problems Hindawi in Engineering, Article ID 4070616, 12 pages, 2017.

[29] Guangbo Wang and Jianhua Wang, Ciphertext-Policy Attribute Based Encryption with Attribute Level User Revocation in Cloud Storage, Mathematical Problems Hindawi in Engineering, Article ID 4070616, 12 pages, 2017.

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

[31] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp.121– 130.

[32] D.Naor,M. Naor, and J.Lotspiech,"Revocationandtracingschemes for stateless receivers," in Proc. CRYPTO, 2001, LNCS 2139, pp. 41–62.