INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 3 ISSUE 1 –JANUARY 2015 - ISSN: 2349 - 9303

Secure Data Sharing Algorithm for Data Retrieval In Military Based Networks

A.Lilly sara
Arunai Engineering College,
CSE(with specialization in Networks)
Lillysara2401@gmail.com

E.Elavarasi
Assistant Professor,
Arunai Engineering College,
Department of CSE
Elavarasi17@gmail.com

Abstract— Mobile knots now armed atmospheres such equally battlefield or aggressive area remain expected toward smart after irregular net connectivity and regular panels. Disruption Tolerant Network (DTN) tools stay attractive positive keys that agree knots toward connect with each other in these dangerous interacting atmospheres.The problem of applying the security mechanisms to DTN introduces several security challenges.Since nearly handlers could modification their related characteristics by approximately argument and reliability of data should be changed otherwise around isolated secrets power remain bargained significant reversal aimed at respectively characteristic is essential in command toward create organisms safe in this research a novel approaches are used to overcome the above mentioned problems called secure data sharing algorithm. This algorithm calculate hash importance aimed at coded documents which is used to check the reliability of encrypted confidential data.

Index Terms— Disruption tolerant network ,Secure data sharing algorithm,Cipher text attribute based encryption,Secure hash function,Key policy attribute based encryption.

1 Introduction

When developing secure network the following need to be consider.
1. Access – authorized users are provided the means to communicate to and from a particular network.
2. Confidentiality – Information in the network remains private.
3. Authentication – Ensure the users of the network are who they say they are.
4. Integrity – Ensure the message has not been modified in transit.
5. Non-repudiation – Ensure the user does not refute that he used the network an effective network security plan is developed.

In this system, a novel approach is used to secure data retrieval in military environments called Secure Data Sharing Approach. In SDSA, once users retrieve a data using his private key he/she must perform the hash function computation for verify the reliability of shared confidential data. It computes hash function during both the data encryption and decryption. Then, Compare the generated hash values, if it is similar then the received data should be considered as reliable else the received data considered as not reliable.Details about the wireless network. Initially the network contains network servers, multiple Attribute authority and users. The network server is connected with commander (Sender), Key authorities (central authority and multiple local authorities). Here the Commander directly handles the data. The Key authorities is used for provide secret key to the requested group of soldier and Commander. Initially the commander and user makes register by entering the required details and login to the wireless network. Once a user retrieve a data using his private key he/she must perform the hash function computation for verify the reliability of shared confidential data. This secure data sharing approach computes hash function during both the data encryption and decryption. Compare the generated hash values, if it is similar then the received data should be considered as reliable else the received data considered as not reliable

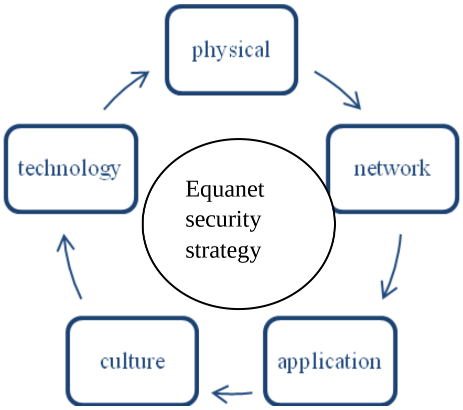


Fig.1:System protection

The SDS Algorithm computes hash function during both the data encryption and decryption. Then, Compare the generated hash values, if it is similar then the received data should be considered as reliable else the received data considered as not reliable. Our proposed research work implements secure data retrieval for military environments using Secure Data Sharing Approach and Cipher text policy-Attribute based Encryption. By allowing ,the secure data retrieval perform by secure data sharing algorithm which comes under SHA(secure hash algorithm)to retrieve the data for users from data owner should be securely. By using SDS algorithm they Provide Confidentiality ,Provide Data Reliability,Provide Secured Communication.

2. RELATED WORK

Melissa Chase, Sherman S.M. CHOW [1] In many applications we find we need to share data according to an encryption policy without prior knowledge of who will be receiving the data. To propose a Multi-Authority Attribute-Based Encryption (ABE) system.

Shucheng Yu, Cong Wang, Kui Ren[2] Cipher text will specify an access policy over attributes. To overcome this difficulty, we introduce many "copies" of each attribute for every position in the access structure tree where it can occur. However, since the actual access structure to be used for a particular cipher text must be embedded into the fixed "universal" tree access structure in the KP-ABE scheme, these causes a blowup in cipher text size.

Allison Lewko, Brent water[3] In many applications we find we need to share data according to an encryption policy without prior knowledge of who will be receiving the data. To propose a Multi-Authority Attribute-Based Encryption (ABE) system.

Luan Ibraimi, Milan Petkovic,Svetla Nikova, Pieter Hartel, Willem Jonker[4]

To supports revocation of user attributes. If an attribute is revoked, the user cannot use it in the decryption phase. The scheme allows the encryptor to encrypt a message according to an access policy over a set of at- tributes, and only users who satisfy the access policy and whose attributes are not revoked can decrypt the ciphertext. A possible extension to this research would be to provide a scheme which would have a security proof under standard complexity assumptions.

Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai[5] Encrypted cipher text will specify an access policy over attributes. To overcome this difficulty, we introduce many "copies" of each attribute for every position in the access structure tree where it can occur. However, since the actual access structure to be used for a particular cipher text must be embedded into the fixed "universal" tree access structure in the KP-ABE scheme, these causes a blowup in cipher text size.

Sherman S.M. Chow[6] Key escrow is inherent.A curious Key Generation Center can only create the user's private key to decrypt a cipher text. However can a still decrypt if it does not know the intended recipient of the cipher text we answer by formalizing anonymous cipher text in distinguishability.

3.PROPOSED ALGORITHM

In our proposed system, a novel approach is used to secure data retrieval in military environments called Secure Data Sharing Approach. In SDSA, once users retrieve a data using his private key he/she must perform the hash function computation for verify the reliability of shared confidential data. It computes hash function during both the data encryption and decryption. Then, Compare the generated hash values, if it is similar then the received data should be considered as reliable else the received data considered as not reliable.

In Proposed system, the CP ABE used for secure data retrieval in military networks. In CP-ABE, the cipher text is encoded by an entrée strategy selected in an encryptor, then a important is only formed by detail towards an characteristics established. CP-ABE allows encryptor such by means of a commander-in-chief towards select an entrée rule scheduled characteristics then towards encode private documents below the entrée assembly through encoding by the consistent community secrets otherwise characteristics.

Signature Data Sharing Approach
Step 1: Randomly picks a prime number p.
Step 2: Compute Hash value (H) for prime number p.
Step 3: Store the hash value in encrypted data.
Step 4: If any unauthorized person/ attacker access the confidential encrypted data the hash value should perform either addition or multiplication operation.
Step 5: Receiver receives it private key, then it compute hash function using its private key
Step 6: The computed hash value as same as generate hash value hence it is original data.
Step 7: Based on step 4, any unauthorized person or attacker accessed the data, and then computed hash value should be mismatched hence the receiver identifies the received data is not an original data.
Step 8: So, receiver neglect the retrieved data.

EXISTING SYSTEM:

In existing system, KP-ABE scheme was used to solve the key escrow problem in a multi-authority system. In this method, entirely (split) characteristic establishments remain joining now the important group procedure now a scattered method such that they dismiss group their informations then connection several characteristic groups going towards the similar handler.

In KP-ABE, the encryptor simply develops towards make a ciphertext through a regular of characteristics. The important specialist selects a rule aimed at separately handler that defines which ciphertexts he dismiss decrypt then problems the important towards respectively handler through surrounding the rule addicted to the handler's important. Then around no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key.There is no separate algorithm for transmitting/receiving the confidential data.Complexity is very high.Reliability of Confidential data is very low.

MODULES

Execution is the phase of the task after the theoretic task is rotated available addicted to a occupied method.

1.Network Deployment module
2.Data encryption module
3.Key distribution module
4.Data retrieval module

4.SYSTEM DESIGN

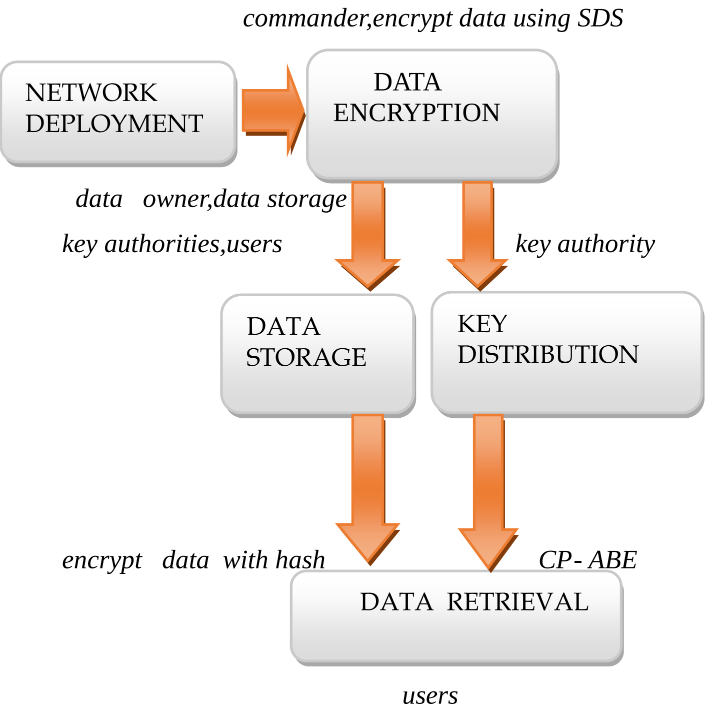


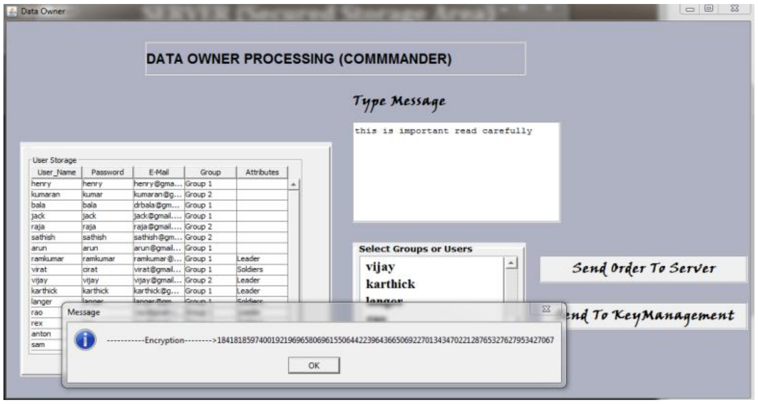
Fig.2. Architetcure Diagram.

4.1.Network deployment module:

This module contains the details about the wireless network. Initially the network contains network servers, multiple Attribute authority and users. The network server is connected with commander (Sender), Key authorities (central authority and multiple local authorities). Here the Commander directly handles the data. The Key authorities is used for provide secret key to the requested group of soldier and Commander. Initially the commander and user makes register by entering the required details and login to the wireless network.

4.2Data encryption module:

This module provides the details about data encryption. Sender is an object who preserves personal communications otherwise documents (e.g., a commander-in-chief) then needs towards supply them addicted to the exterior documents storing knot aimed at simplicity of involvement otherwise aimed at consistent distribution towards handlers in the exciting make contacts surroundings. A source is answerable aimed at important (characteristic established) admission rule then applying it on that one individual documents by encoding the documents below the rule earlier storage the situation towards the storing knot. The commander (sender) encrypts the data.Then hash value for encrypted data using secure data sharing approach which is used to check the reliability of encrypted confidential data.



this is important read carefully

User Storage

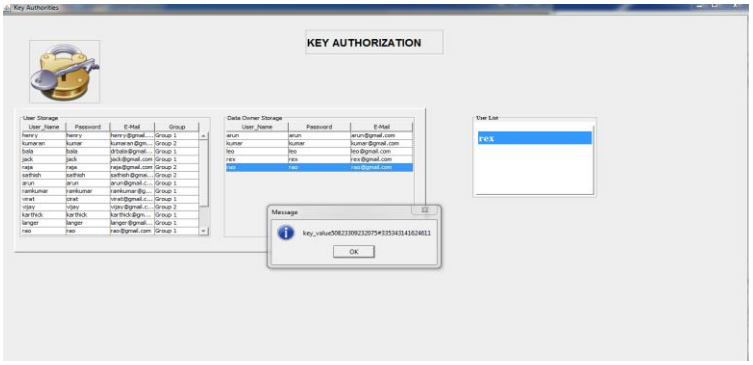
User_Name	Password	E-Mail	Group	Attributes
henry	henry	henry@gma...	Group 1	
kumaran	kumar	kumaran@g...	Group 2	
bala	bala	drbala@gm...	Group 1	
jack	jack	jack@gmail....	Group 1	
raja	raja	raja@gmail....	Group 2	
sathish	sathish	sathish@gm...	Group 2	
arun	arun	arun@gmail...	Group 1	
ramkumar	ramkumar	ramkumar@...	Group 1	Leader
virat	cirat	virat@gmail...	Group 1	Soldiers
vijay	vijay	vijay@gmail...	Group 2	Leader
karthick	karthick	karthick@g...	Group 1	Leader
langer	langer	langer@gm...	Group 1	Soldiers
rao				
rex				
anton				
sam				

vijay
karthick
langer

-----------Encryption-------->184181859740019219696580696155064422396436650692270134347022128765327627953427067

4.3.Key distribution module:

In this module, Cipher text policy- Attribute Based Encryption (CP-ABE) algorithm is used to generate the key for encrypted data that should be generated by sender. The Cipher text Policy –Attribute Based Encryption(CP-ABE) offers a accessible technique of encoding documents such that the encryptor describes the characteristic established that the decryptor wants towards have popular directive to decrypt the cryptograph script. Hence, changed handlers remain acceptable towards decrypt changed parts of documents each the safety rule.



User Storage

User_Name	Password	E-Mail	Group
henry	henry	henry@gmail....	Group 1
kumaran	kumar	kumaran@gm...	Group 2
bala	bala	drbala@gmail...	Group 1
jack	jack	jack@gmail.com	Group 1
raja	raja	raja@gmail.com	Group 2
sathish	sathish	sathish@gmai...	Group 2
arun	arun	arun@gmail.c...	Group 1
ramkumar	ramkumar	ramkumar@g...	Group 1
virat	cirat	virat@gmail.c...	Group 1
vijay	vijay	vijay@gmail.c...	Group 2
karthick	karthick	karthick@gm...	Group 1
langer	langer	langer@gmail...	Group 1
rao	rao	rao@gmail.com	Group 1

Data Owner Storage

User_Name	Password	E-Mail
arun	arun	arun@gmail.com
kumar	kumar	kumar@gmail.com
leo	leo	leo@gmail.com
rex	rex	rex@gmail.com
rao	rao	rao@gmail.com

User List

rex

key_value50823309232075#335343141624611

4.4.Data retrieval module:

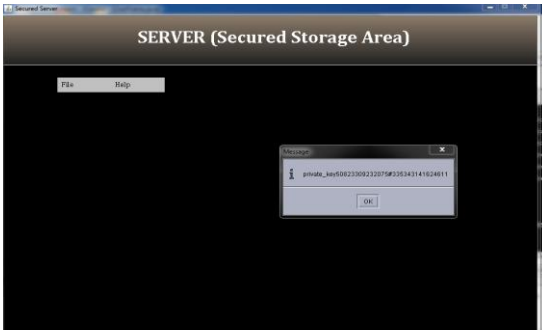
In this module, the user retrieves the shared data. User is a portable knot who needs towards entree the informations deposited on the storing knot (e.g., a warrior). Unknown handler keeps established of characteristics sufficient the entree rule of the encoded documents well-defined through the source, then is not canceled popular one of the characteristics, before he determination remain capable towards decrypt the cryptograph script then get the documents. Once a user retrieve a data using his private key he/she must perform the hash function computation for verify the reliability of shared confidential data. This secure data sharing approach computes hash function during both the data encryption and decryption. Compare the generated hash values, if it is similar then the received data should be considered as reliable else the received data considered as not reliable.

5.DISCUSSION

Our proposed research work implements secure data retrieval for military environments using Secure Data Sharing Approach and Cipher text policy-Attribute based Encryption. The SDS Algorithm computes hash function during both the data encryption and decryption. Then, Compare the generated hash values, if it is similar then the received data should be considered as reliable else the received data considered as not reliable.. Finally our proposed system achieves efficient and secure data retrieval in military networks it also provides data reliability.

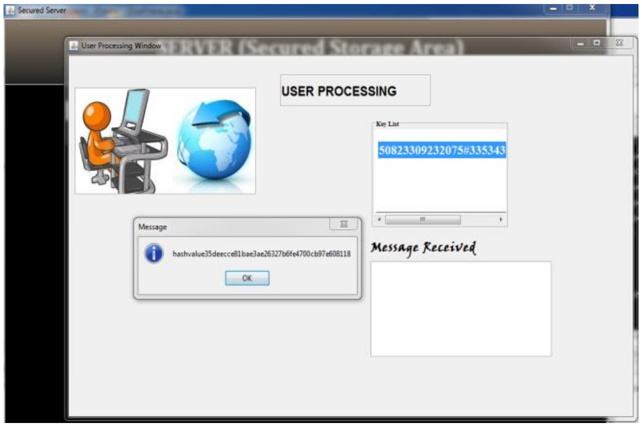
6.RESULTS

By allowing ,the secure data retrieval perform by secure data sharing algorithm which comes under SHA(secure hash algorithm)to retrieve the data for users from data owner should be securely.



private_key50823309232075#335343141624611

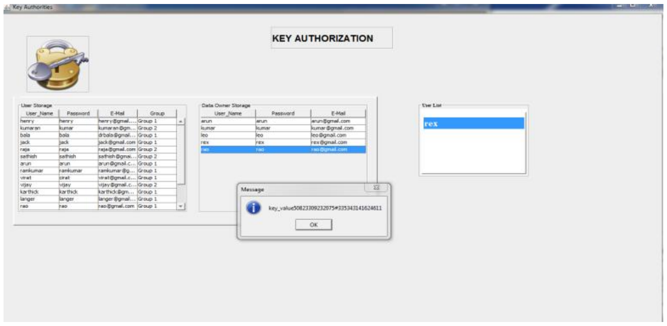
6.1



50823309232075#335343

hashvalue35deecce81bae3ae26327b6fe4700cb97e608118

6.2



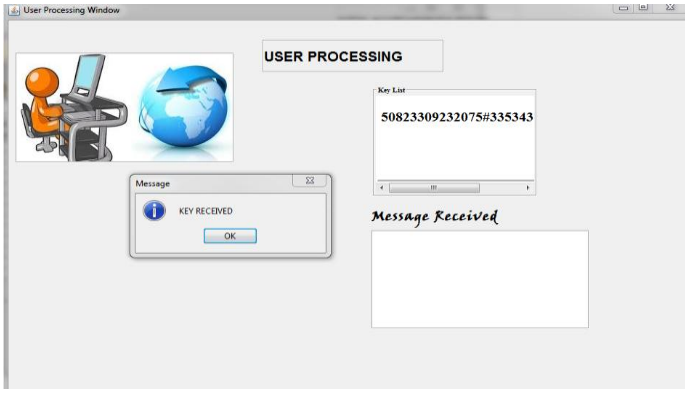
User_Name	Password	E-Mail	Group
henry	henry	henry@gmail....	Group 1
kumaran	kumar	kumaran@gm...	Group 2
bala	bala	drbala@gmail...	Group 1
jack	jack	jack@gmail.com	Group 1
raja	raja	raja@gmail.com	Group 2
sathish	sathish	sathish@gmai...	Group 2
arun	arun	arun@gmail.c...	Group 1
ramkumar	ramkumar	ramkumar@g...	Group 1
virat	cirat	virat@gmail.c...	Group 1
vijay	vijay	vijay@gmail.c...	Group 2
karthick	karthick	karthick@gm...	Group 1
langer	langer	langer@gmail...	Group 1
rao	rao	rao@gmail.com	Group 1

User_Name	Password	E-Mail
arun	arun	arun@gmail.com
kumar	kumar	kumar@gmail.com
leo	leo	leo@gmail.com
rex	rex	rex@gmail.com
rao	rao	rao@gmail.com

rex

key_value50823309232075#335343141624611

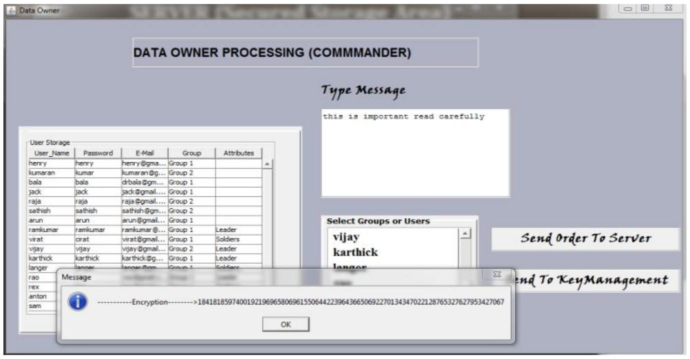
6.3



50823309232075#335343

KEY RECEIVED

6.4



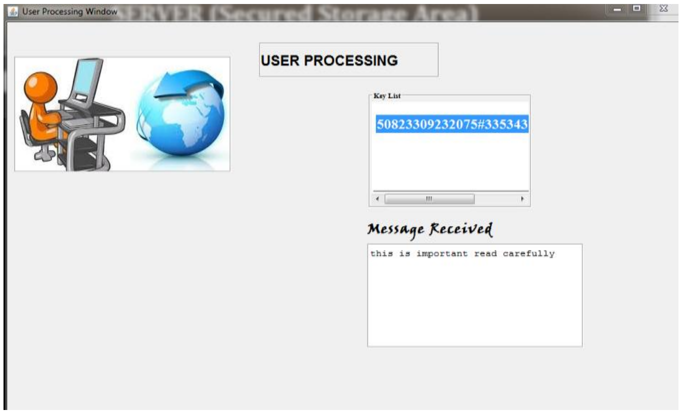
this is important read carefully

User_Name	Password	E-Mail	Group	Attributes
henry	henry	henry@gma...	Group 1	
kumaran	kumar	kumaran@g...	Group 2	
bala	bala	drbala@gm...	Group 1	
jack	jack	jack@gmail....	Group 1	
raja	raja	raja@gmail....	Group 2	
sathish	sathish	sathish@gm...	Group 2	
arun	arun	arun@gmail...	Group 1	
ramkumar	ramkumar	ramkumar@...	Group 1	Leader
virat	cirat	virat@gmail...	Group 1	Soldiers
vijay	vijay	vijay@gmail...	Group 2	Leader
karthick	karthick	karthick@g...	Group 1	Leader
langer	langer	langer@gm...	Group 1	Soldiers
rao				
rex				
anton				
sam				

vijay
karthick
langer

-----------Encryption-------->184181859740019219696580696155064422396436650692270134347022128765327627953427067

6.5



Key List
50823309232075#335343

Message Received
this is important read carefully

6.6

7.CONCLUSION

To conclude of this project is Secured data retrieval in military environment by using Secure Data Sharing Algorithm are:

1.Provide Confidentiality
2. Provide Data Reliability
3. Provide Secured Communication

The SDS Algorithm computes hash function during both the data encryption and decryption.In CP-ABE, the ciphertext is encoded through an entree rule selected through an encryptor then a important is only formed through admiration towards an characteristics set. CP-ABE allows encryptor such for example a commander-in-chief to select an entree rule on attributes then towards encode personal documents below the entree assembly through encoding through the equivalent unrestricted solutions otherwise characteristics. Finally our proposed system achieves efficient and secure data retrieval in military networks it also provides data reliability.

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–