IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Secured Data Retrieval for Decentralized Disruption-Tolerant Disaster Networks

Dhanashree Karadi[1], Umesh V. Somanatti[2]

P.G. Department of Computer Science and Engineering, Dr. M.S. Sheshgiri College of Engineering and Technology, Belgaum, Karnataka, India [1, 2]

Abstract: The wireless devices carried by the user in scenario such as disaster situation, which may include earthquake, floods, would be temporary disconnected for some time, it would be due to discontinues network connection and partitioning. Disruption-tolerant network (DTN) is one of the successful techniques which allow the devices to communicate with other devices in such situation. This is accomplished by using the storage node as the intermediary node. If the sender wants to send the message or the data to receiver in such scenario where the network connectivity is not continuous, the message is been stored in the storage node of some time. If the receiver wants to access the message it can retrieve from storage node. Attribute-Based-Encryption(ABE) provides a capable approach in which it fulfils the requirement for retrieving of the data in DTN's in a secured way. ABE provides technique in which different access-control for the encrypted message over different access policy can be defined. There are several problems to apply Attribute-Based-Encryption(ABE) for the DTN, in terms of safety and confidentiality of data. The Cipher-text Policy-ABE(CPABE), defines the technique in encryption of the data in such that, sender will define some of the attribute, the receiver must hold to decrypt the data or message, such that different receiver's are permitted to decrypt the different piece of the data as defined in security policies.

Keywords: Attribute-Based-Encryption(ABE), Ciphertext Policy-Attribute-Based-Encryption (CP-ABE), Disruption-tolerant network (DTNs)

I. INTRODUCTION

In disaster network scenarios, the connection of the wireless devices taken by different users would be disconnected for short period of time, this may be due to environment factors faced during disaster or mobility. Disruption-Tolerant-Networks (DTN) are attractive solution which permit the different devices to perform communication in such extreme environmental situation. Whenever there are no direct connections from source to the destination, the messages sent from source must be stored in some intermediary node for, some time, until some of link to the receiver or the destination is established.

In order to retrieve the messages in disaster network scenarios, the storage node in Disruption-Tolerant-Network (DTN) were introduced. Using the intermediary node such as storage node the messages or data are copied or stored in such a way that only the authorized devices would have access to the data. In disaster network scenarios, there is need for security between the officials to access the confidential information. In different scenarios, it is necessary to provide the access-policies that are been defined over different users or officials attributes. For instance, The Chief Commandant may store some message or data that should be accessed by a Rescue Employee belonging to particular region. The DTN architectures in which different authorities can give access permission and can manage different attribute are called as decentralized Disruption-Tolerant-network (DTN).

Consider a case where it is essential for an officer to encrypt a data in such a way that it could be accessed only by those officers who all are involved in a particular region. In this type of systems, the receivers can decrypt the document, if the attributes that they hold, match this policy. Here it is required to realize the security against all the receivers and therefore this has become one of the key challenges in building these systems. For instance, the unauthorized receivers must not be permitted to access the encrypted message. A solution has been presented for the above mentioned problem by Sahai and Waters[10] and this solution is named as Attribute-Based-Encryption (ABE). In this system, it is possible to specify different access permission to the data to the attributes by a party encrypting data. If and only if the attributes are associated with their private, it is possible to perform decryption of a cipher-text by receiver.

Attribute-Based-Encryption(ABE) provides a capable approach in which it fulfils the requirement for retrieving of the data in DTN's in a secured way. ABE provides technique in which different access-control for the encrypted message over different access policy can be defined. Junbeom Hur and Kyungtae Kang, (2014) "Attribute-Based-Encryption(ABE) is classified in, two types, that are, Key-Policy-ABE(KP-ABE) and the Cipher-text Policy-ABE (CPABE). In Key-Policy-ABE(KP-ABE), sender has the ability to label a list of different attributes, whereas the key authority has the ability to provide the access policy[1]. In Cipher-text Policy-ABE(CPABE), the encryptor or the sender provides the access policies for the receiver and key authority job is just to generate the key.

DOI 10.17148/IJARCCE.2016.56172

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

The Cipher-text Policy-ABE (CPABE), defines the technique for encrypting the message such a way that, sender defines the attribute that the receiver must hold to decrypt data or message, such that different receiver's are permitted to decrypt the different piece of the data as defined in security policies"[1].
There are several problems to apply Attribute-Based-Encryption(ABE) for the DTN when security and privacy of the data is considered. That is, Chief Commandant would provide access policy to access message or data for rescue employee, in existing system, all of the rescue employee has the privileges to access the data belonging to a particular attribute, but here the Chief Commandant cannot provide fine grained access policy in which only some of the rescue employee can access the data among the whole employees, this may degrade the security.

The second challenge which is called Key-Escrow problem, here key authority is responsible for generating the keys. Here the key authority has a access to decrypt the data of a particular users by generating the attribute key. In such a situation if key authority is been attacked by some adversary, when this is implemented in the situation like disaster scenario, then this would be the possible threat to the privacy or the confidentiality whenever the data been stored is sensitive.

II. DESIGN METHODOLOGY

In this paper, securely retrieving of message or data is been introduced using CPABE. The first problem is overcome by defining the access policies for the individual user in the group. That is the Chief-Commandant may send a message that should only be access by only some members of the rescue employee, in which the Chief Commandant can view all the receiver's list, and can select a particular receiver to which the message is to be transferred. Whereas in the existing system, the access policy is been defined for the entire group that is, the access policy can be defined for all rescue employees in a attribute group, but cannot be defined for the single receiver. The second problem is overcome in this implementation, that is by defining the key authority that is only responsible for generation of the keys, but it cannot provide access or decrypt the data. Here the sender himself gives the access policy for data, before storing data in storage node, that specifies which should individual receiver can access the data.

A. System Architecture

The below figure describes the architecture of secured retrieval of data in disaster scenario, Junbeom Hur and Kyungtae Kang, (2014) "the architecture consists of different modules which are as follows.

- Key Distribution Authority
- Storage Node
- Sender(Service Provider)
- Receiver(User)
- Cipher-Policy-Attribute-Based-Encryption(CPABE) Method.

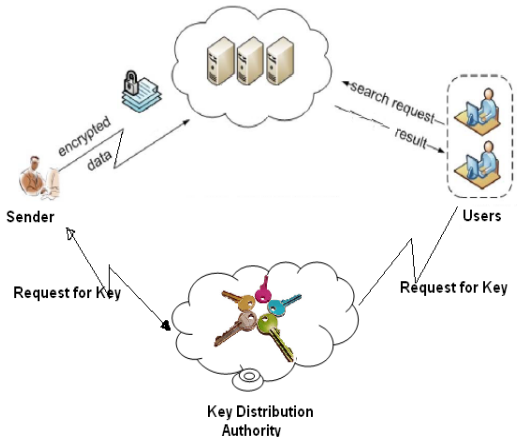


Figure 1: Architecture of Attribute-Based secured data retrieval for disaster management.

The working of each module are as follows:

➢ Key Distribution Authority:
Key authorities are responsible for generating of the public or private parameters for the CP-ABE. Key authority consist of different authorities. Each of the authority performs the managing of different attribute and issues the attribute key to the users. They are responsible for proving the access-rights to the every user based on the specific user attribute.
➢ Storage node:
Whenever the sender wants to send message or the data, sender stores the message in the storage node, which provide the access to the receiver.
➢ Sender (Service Provider):
Sender is the one who has the confidential data or message (e.g., Chief Commandant), and the sender stores the message in the storage node in order to make it easy for sharing the data or to provide reliable delivery for the different user in situation such as disaster occurred. Here sender provides the access policy on the message or data before storing the message or data to storage. It is very much essential to define the access policy and then enforcing this access policy onto message or data that is sent by sender. This is carried out by the sender prior to the storage of message or data in to storage node by encrypting the data under this policy.
➢ Receiver (user):
Receiver is a mobile node. This node is meant to access message or data which is stored at storage node (such as a Rescue Employee). It is possible for the user to obtain the data by decrypting the cipher text if and only if the user already have the set of attributes that are in accordance with the access policy of the encrypted data defined by the user.
➢ CP-ABE Method:
In this scheme, the sender has the rights to provide the policy, which defines who are able to decrypt the message or data. Attribute are used to define the policies. The access policies are sent with cipher-text. In such a scheme, the data which is encrypted is confidential, if even though server is not trusted node." [1] The tasks of different module can be viewed the figure shown above.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

B. Block Diagram

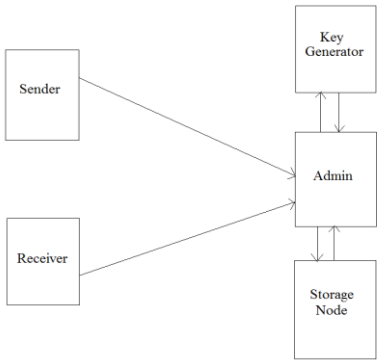


Figure 2: block diagram depicts the working of the system.

The block diagram depicts the working of the system. Here the Admin is responsible for registration of sender and receivers. Once the sender and receiver are registered, sender can exchange the message or data with the receiver. The key generator is responsible for generation of the keys in order to encrypt the data at sender and decrypt it at receiver. The data sent from the sender is been stored in the storage node, at the receiver side it is been extracted from the storage node.

C. Sequence Diagram

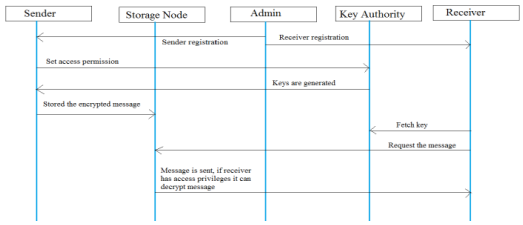


Figure 3: Sequence Diagram.

The sequence diagram shows the sequence of steps how they are occurred in the operation. In the diagram above the steps are as follows:

- Admin register's the sender by entering the sender name, username, password, and sender work for particular region. Next the Admin registers different receivers that belong to particular region by entering the receivers name, username, password, area code, and the receiver work as whether Regional Head, Rescue Employee or Squad.
- In the next step, if the sender is the registered user, then sender can set the access permission for the particular receivers.
- Once the access permission are been set, the keys are been generated by the key authority in order to encrypt message.
- Now the sender can enter the message and send it to particular receivers, this is done through storage the message in the storage node.
- At the receiver, if the user is the registered receiver, and have the access permission set by the sender, then receiver can access the data by decrypting it. This is done by extracting the message from the storage node.

D. Use case Diagram

Use-case dig defines the behavioural dig which is defined and is created by using the analysis of the Use-case. Diagram building blocks are:

- A use case - A use case describes a sequence of actions.
- Actors - An actor is responsible to perform communication with system.

Figure 4:Case Diagram

E. Use case diagram for Admin

The diagram below shows the use case diagram for the admin. Here admin is an Actor. Admin performs different tasks such as Registers sender and receivers, performs the region entry, squad entry, and the area information in which the state and particular city is been linked.

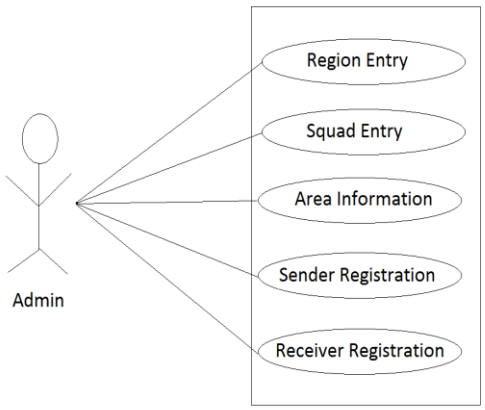


Figure 5: Use case diagram for Admin.

F. Use case diagram for Sender

The diagram below shows the use case diagram for the sender. Here sender is an Actor. Sender performs different tasks such request key, encrypt data, give access permission and store data in storage node.

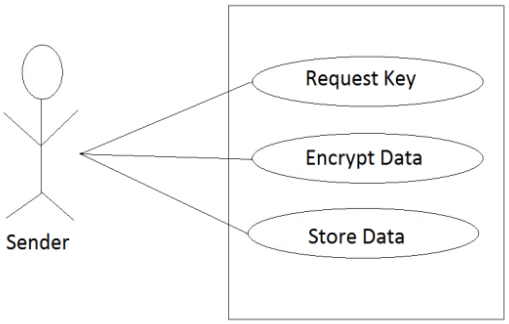


Figure 6: Use case diagram of sender

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

G. Use case diagram for Receiver

The diagram below shows the use case diagram for the receiver. Here receiver is an Actor. Receiver performs different tasks such as fetch a key, decrypt the data and retrieve the data from the storage node.

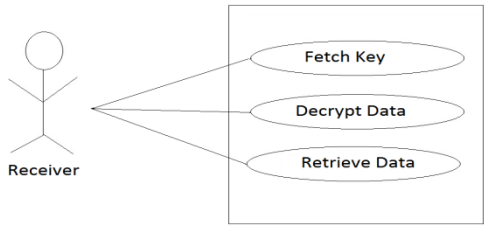


Figure 7: Use case diagram of receiver.

III.IMPLEMENTATION

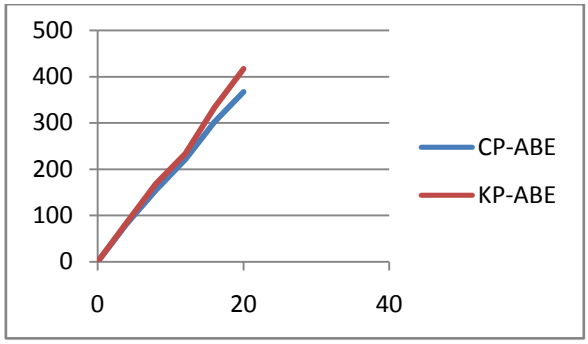
Implementation defines how actually the working is done, when put in use in reality. In Attribute Based Secured Data Retrieval for Disaster Management, the implementation consist of different steps. Here firstly, the Admin enters the region such as Karnataka or Maharashtra, next Admin enters the Squad information such as city, that is Bangalore, Belgaum, Hubli, next Admin link the region to the squad that is, Bangalore belongs to Karnataka, Belgaum belongs to Karnataka, next task of Admin is to performs the registration of the Sender by providing the sender name, username password, sender region. Next the Receivers that belong to particular region are registered, it registers by proving the receiver name, username, password, and whether the receiver works as Regional Head(RH) or Rescue Employee(RE) or Squad. After the registration the sender can view all the receivers to whom it can send the message, next the sender performs the access policy by setting permission to which receiver the message is accessible. Next sender enters the message, the Cipher-Policy-ABE(CPABE) is used to encrypt the message, this is done by using the keys which are generated by key-authority, then sender sends message to different receiver. At, the receiver, if the receiver has the access permission, receiver can view the date of the message been received, name of the sender, and can decrypt the message and can read the message or data.

IV. RESULT ANALYSIS

1.Comparison of Cipher-Text-Policy-ABE(CPABE) with Key-Policy-ABE(KPABE) in terms of encryption time

Encryption Time Comparison		
Execution Time (m Sec)		
Number of Attributes	CP-ABE	KP-ABE
0	0	0
4	82	85
8	155	169
12	221	234
16	302	333
20	367	417

Table I: Encryption Time Comparison.



Graph 1: comparison of CP-ABE and KP-ABE

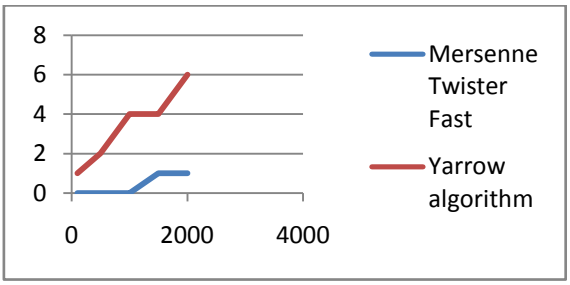
The Cipher-Text-ABE(CPABE) is compared with the Key Policy-ABE(KPABE) , as shown in the comparison table and the graph, the Cipher-Text-ABE(CPABE) execution time is less when compared with the Key Policy-ABE(KPABE) when different number of Attributes are considered.

2.Comparison of Mersenne Twister Fast with Yarrow algorithm

The Mersenne-Twister-Fast is one of the pseudorandom number generator (PRNG). This algorithm is most widely used general-purpose PRNG [23]. The aim to design this algorithm was to overcome the flaws that are found in the earlier PRNGS. This was first PRNG which provided high quality generation of pseudorandom. This algorithm is having long period $2^{19937} - 1$. The long period defines security as the number is not repeated for long time when compared with other algorithm which defines $2^{\wedge 32}$ would be problematic [26]. Below table shows the comparison of Mersenne Twister Fast with the Yarrow algorithm.

Number of Execution	MersenneTwister Fast	Yarrow algorithm
100	0	1
500	0	2
1000	0	4
1500	1	4
2000	1	6

Table II: Comparison of Mersenne Twister Fast with Yarrow algorithm:



Graph 2: Comparison of Mersenne Twister Fast and Yarrow algorithm.

By observing the table and the graph it can be observed that Mersenne Twister Fast algorithm repeats a random number, not as frequently as the Yarrow algorithm. According to the result, when the M-Twister Fast

algorithm executes it repeats just 1 random number during the 1500 executions, whereas Yarrow algorithm repeats 4 random numbers, which would be threat for the confidential message. It is easy to predict the random number as compared with Mersenne Twister Fast algorithm.

V. CONCLUSION

Disruption-Tolerant-Network are attractive solution in disaster network scenario applications, in which they make use of storage nodes to store the data for the purpose of communication with the other devices in the network. Cipher-Policy-Attribute-Based-Encryption(CPABE) provide solution, such that, sender can provide the access permission on the message or the data that has been store in the storage node, due to which only the receivers in the group having the access permission to read the message or data has access, others users can't access the data. Here, efficient and the secured retrieval of data, method using CP-ABE for disaster management network is been introduced. The problem in the existing system of providing access policies for the individual user is overcome, by providing fine grained access policy within the group of users. The problem is overcome by defining the access policies for the individual user in the group Whereas in the existing system, the access policy is been defined for the entire group. The other problem of existing system is overcome by defining the key authority that is only responsible for generation of the keys, but it cannot provide access or decrypt the data. Here the sender himself gives the access policy on data, before storing data in storage node, that specifies which should individual receiver can access the data.

REFERENCES

[1] Junbeom Hur and Kyungtac Kang, Member, IEEE, ACM, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", in Proc. IEEE TRANSACTIONS ON NETWORKING, 2014.
[2] Mooi-Choo Chuah"Performance Evaluation of Node Density-Based Adaptive Routing Scheme for Disruption Tolerant Networks"
[3] Mooi-Choo Chuah "Performance Evaluation of Node Density-Based Adaptive Routing Scheme for Disruption Tolerant Networks"
[4] 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.
[5] 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.
[6] Kevin Fall, Jayanthkumar Kannan, Fernando Silveira, "A Disruption-Tolerant Architecture for Secure and Efficient isaster Response Communications".
[7] Sarvesh Kumar "A Survey on Delay Tolerant Network in Disaster Management". International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 3 Issue 7, July - 2014.
[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] Allison Lewko, Brent Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
[10] Amit Sahai and Brent Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473.
[11] 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.
[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp.321–334.
[13] 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.
[14] Shucheng Yu, Cong Wang, Kui Ren, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp. 261–270.
[15] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in Proc. ACMConf. Comput. Commun. Security, 2006, pp. 99–112.
[16] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003.
[17] Ling Cheung,Calvin Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.
[18] 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.
[19] M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.
[20] M. Chase, "Multi-authority attribute based encryption," in Proc. TCC, 2007, LNCS 4329, pp. 515–534.
[21] 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.
[22] Chung Kei Wong, Mohamed Gouda, and Simon S. Lam, "Secure group communications using key graphs," in Proc. ACM SIGCOMM, 1998, pp. 68–79.
[23] E.g. Marsland S. (2011) Machine Learning (CRC Press), §4.1.1. Also see the section "Adoption in software systems".
[24] Website:[https://docs.python.org/release/2.6.8/library/random.html 9.6 random -Generate pseudo-random numbers]. Python v2.6.8 documentation. 2012-05-29.
[25] Web site: "Random" class documentation. Ruby 1.9.3 documentation. 2012-05-29.
[26] Note: 2^{19937} is approximately 4.3×10^{6001}; this is many orders of magnitude larger than the estimated number of particles in the observable universe, which is 10^{87}.
[27] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Proc. CRYPTO, 2001, LNCS 2139, pp. 41–62.
[28] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444–458, May 2003.