International Conference on Innovative Research in Engineering, Management and Sciences
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 9 | ISSN : 2456-3307

A Survey on Applications of Attribute Based Encryption in Various Networks

J. Joshua Daniel Raj[1], Dr. P . Karthik[2]
[1]Senior Assistant Professor, New Horizon College of Engineering, Outer Ring Road, Marathalli, Bengaluru, Karnataka, India
[2]Professor, K.S.School of Engineering and Management, Bangalore, Karnataka, India

ABSTRACT

We collect various information's by using several sources and use different types of networks to share the gathered information's, the cloud networks is used to share the information to the larger audience over an internet, the delay tolerant networks is used to share the information over the adhoc networks, the fog computing network is used to share the information to the devices residing at the edge of network. The security and privacy issues of those networks are the great concerns among the researchers. The Attribute Based Encryption has been the most promising cryptographical approach for the decades to secure the data in transit and storage in the above mentioned networks. In this paper we survey the applications of attribute based encryption and their security requirements and performance measurement evaluation methods in the above mentioned networks.

Keywords : Adhoc Networks, Cryptographical Approach

I. INTRODUCTION

In the age of information, the information are collected by the means various means such as camera, text, and sensors. When the owner of the information retains the information with himself in a local storage like desktop, flash drives and hard disks, the data is secured. On the other hand when it is transmitted to the other user over the networks it is stored either in terminal node or in an intermediate node or in various nodes, the node consists of servers and networking devices, when the data is stored in the cloud in the plain format, it is very much vulnerable to the attack of the hackers and other malicious software programs, thus the privacy of the user data is under threat [1] [2] [3] [4]. Hence in order to secure the data when it is in cloud and transit, the data need to be encrypted by means of cryptographical methods[5]. This paper surveys the applications of attribute based encryption [6] presented by Amit sahai and Brent waters in various networks and the security parameters to measure the performance of the implementations.

A.Attribute based encryption

One of the most widely used encryption scheme to implement the data centric security is to use attribute based encryption [7] [8], this is a public key encryption, in this the user attributes (eg: role, position, designation) are used to construct a cipher text and secret key. Hence only the user key that matches with the described attributes in the cipher text can decrypt the data.

The major two types of ABE schemes are Key-policy ABE (KP-ABE) [6] and Ciphertext-policy ABE (CP-

ABE)[9], in KP-ABE the owner uses the set of attributes to construct a ciphertext and the private keys are mapped with an access structure. The access structure specifies which type of ciphertext the private keys can decrypt. In CP-ABE the owner uses the user attributes to construct a secret key and access structure is used to construct a ciphertext.

Background

In this section we give the background operational details of ABE. the ABE allows monotonic or non-monotonic access structure [10] [11] . This scheme uses four algorithms as explained in the following table.

Table 1 : Attribute Based Encryption Algorithms

Algorithm	KP –ABE		CP-ABE	
	Input	Output	Input	Output
Setup	Security Parameter	Public Key Master Key	Security Parameter	Public Key Master Key
Encryption	Public Key Message Set of Attributes	Ciphertext	Public Key Message Access structure	Ciphertext
Key Generation	Access structure Public Key Master Key	Private Key	Set of Attributes Public Key Master Key	Private Key
Decryption	Public Key Ciphertext	Message	Public Key Ciphertext	Message

Applications of Attribute Based Encryption

In this section we discuss the implementation of Attribute Based Encryption in various networks with its application details.

1. Secure Data Exchange in Cloud Networks

One of the major applications is preserving personal health records in cloud networks. It is very important to maintain privacy of the personal health records in cloud storage [12] [13]. Ming Li et al [14] have proposed and implemented a frame work as shown in figure 1[14] for secure sharing of personal health records using attribute based encryption. It uses multi authority ABE to improve the security and reduce key-escrow problem in the public domain. This frame work assumed that the server is semi-trusted. The requirements of its implementations are data confidentiality: the unauthorized people should be denied access to the personal health document. On-demand revocation: when an attributes of the user are not valid, an access should be denied. Write-access control: authorized user should not be allowed to modify the record contents. Scalability: as there will be an unpredictable number of users in the public domain the system should allow access to everyone at anytime. It divides the public domain into two groups as public and private domains, for public domain multi authority ABE is used and for a private domain and KP-ABE is used to manage the secret keys and rights to access the data. This frame work also implements break -class access in the case of emergency by overriding a regular access policies.

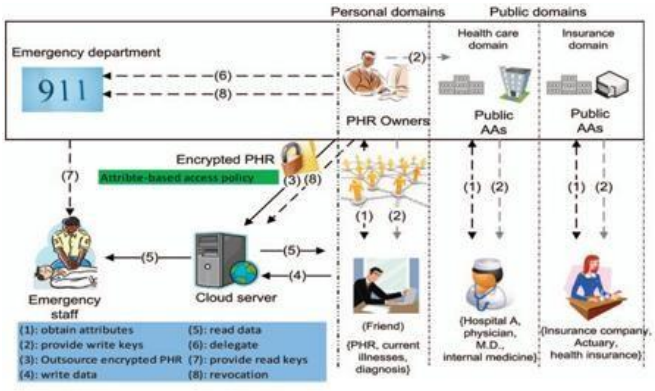

Figure 1: A secure patient- centric framework for cloud networks

Kai fan at al [15] proposed another similar framework for securing personal health records. This scheme uses Key-Aggregate Encryption (KAE) in the private domain and MA-ABE in a public domain.

2. Secure PIN Sharing in Delay Tolerant Networks

The delay tolerant networking is method of computer network that is used to solve the technical problem in heterogeneous networks that does not has continuous network connection between source and destination [16], the DTN uses the store-and-forward approach hence the nodes that stores the data are not fully trusted, and a third part may access the data easily [17]. Amang and Toru [18] designed a framework shown in figure 2[18] to securely exchange a data in the wireless Delay Tolerant Network (DTN), This framework uses ABE to distribute the secret key for symmetric encryption and message authentication to the authorized nodes.

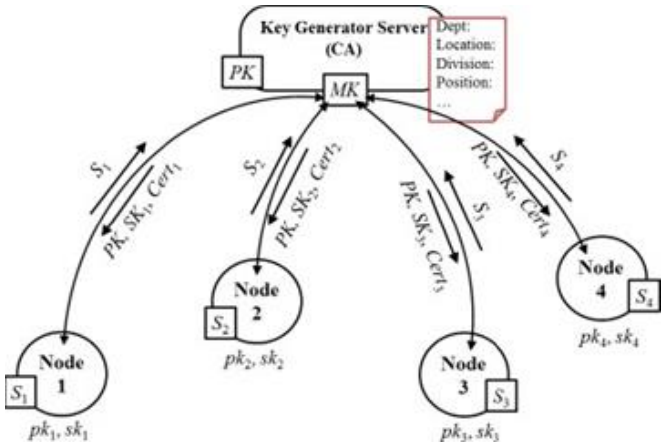

Figure 2 : A secure pin sharing framework for in Delay Tolerant Networks

Hyunsoo, Daeyeong, Changhee and Junbeom [19] proposed device to device (D2D) protocols and they have exploited the CP-ABE to securely communicate the initial key for establishing connection, in order to prevent man-in-the middle attack or replay attack.

3. Secure Key Sharing in Fog Computing

The fog provides extension to the counter in a way it brings the cloud closer to things that are connected to internet, any devices with a computing, network connectivity and storage is a fog node[20] [21]. Arwa et al [22] have proposed and implemented a secure key sharing framework based on CP-ABE in order to achieve confidentiality, authentication, verifiability and access

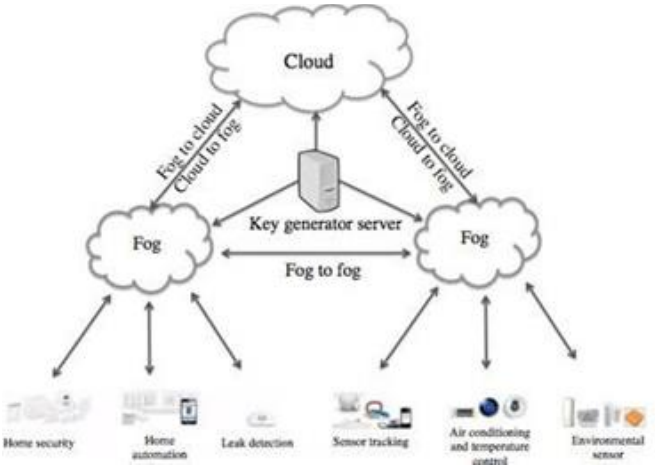

Figure 3: A secure pin sharing framework for Fog Computing

control in fog computing. Their proposed implementation is shown in figure 3. The key generation server generates and distributes the keys among the participating nodes. The cloud provides the access structure and encrypts the data to get cipher text. This method uses digital signature and CP-ABE to reach the security goals. The authors have analyzed their implementations with the certificate based scheme.

Table 2 : Comparison of ABE implementation in various networks

Networks	ABE Primitives	Security Goals	Performance analysis
Cloud Networks	KP- ABE CP-ABE	Data confidentiality On demand revocation Write access control Break glass approach Authentication Authorization	Space complexity Time Complexity
DT Networks	KP-ABE CP-ABE	Confidentiality of routing messages Integrity of routing messages Confidentiality of content data Integrity of content data	Computation cost Storage cost Communication Cost
Fog Network	KP-ABE CP-ABE	Confidentiality Access control Authentication verifiability	Message Size Communication Overhead Comparison

As illustrated in the table 1, the safety requirements for the implementation of ABE remain almost same for all the networks. The primary focus in all of the implementations is confidentiality of messages, access control and authenticity. The performances of the implementations are measured in terms of space complexity, time complexity, computation cost, storage cost, and message size.

II. Conclusion

In this paper, we have conducted a survey on implementation of Attribute Based Encryption in various networks. It is more evident that the Attribute Based Encryption is being a most promising cryptographic based security implementation is highly flexible and it can be implemented to design a framework for any secure network which involves data communication, storage, and computing.

III. REFERENCES

[1]. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan. 2012.

[2]. 3V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," IEEE Trans. Serv. Comput., vol. 9, no. 1, pp. 138–151, Jan. 2016.

[3]. A. Kate, G. M. Zaverucha, and U. Hengartner, "Anonymity and security in delay tolerant networks," in 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007, 2007, pp. 504–513.

[4]. S. Yi, Z. Qin, and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey," in

[5]. Wireless Algorithms, Systems, and Applications, 2015, pp. 685–695.

[6]. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wirel. Netw., vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[7]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, New York, NY, USA, 2006, pp. 89–98.

[8]. T. S. Fun and A. Samsudin, "Attribute Based Encryption—A Data Centric Approach for Securing Internet of Things (IoT)," Adv. Sci. Lett., vol. 23, no. 5, pp. 4219–4223, May 2017.

[9]. Z. Qiao, S. Liang, S. Davis, and H. Jiang, "Survey of attribute based encryption," in Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2014 15th IEEE/ACIS International Conference on, 2014, pp. 1–6.

[10]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in

[11]. 2007 IEEE Symposium on Security and Privacy (SP '07), 2007, pp. 321–334.

[12]. R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based Encryption with Non-monotonic Access Structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY, USA, 2007, pp. 195–203.

[13]. S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "A framework and compact constructions for non-monotonic attribute-based encryption," in International Workshop on Public Key Cryptography, 2014, pp. 275–292.

[14]. M. A. Benamara and H. Li, "Secure of Personal Health Records Shared in Cloud Computing Using Cipher-text Attribute Based Encryption," Int J Secur Netw, vol. 10, no. 3, pp. 183–190, Sep. 2015.

[15]. "GRIN - Securing personal health records in the cloud by using attribute based encryption. A review." [Online]. Available: http://www.grin.com/en/e-book/315416/securing-personal-health-records-in-the-cloud-by-using-attribute-based.

[16]. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[17]. K. Fan, N. Huang, Y. Wang, H. Li, and Y. Yang, "Secure and Efficient Personal Health Record Scheme Using Attribute-Based Encryption," in Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on, 2015, pp. 111–114.

[18]. L. Gao, S. Yu, T. H. Luan, and W. Zhou, Delay Tolerant Networks. Cham: Springer International Publishing, 2015.

[19]. S. Roy and M. Chuah, Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs. .

[20]. A. Sudarsono and T. Nakanishi, "A Secure Data Exchange System in Wireless Delay Tolerant Network Using Attribute-Based Encryption," J. Inf. Process., vol. 25, pp. 234–243, 2017.

[21]. H. Kwon, D. Kim, C. Hahn, and J. Hur, "Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks," Multimed. Tools Appl., pp. 1–15, Jan. 2016.

[22]. I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," Concurr. Comput. Pract. Exp., vol. 28, no. 10, pp. 2991–3005, Jul. 2016.

[23]. S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," in Proceedings of the 2015 Workshop on Mobile Big Data, New York, NY, USA, 2015, pp. 37–42.

[24]. A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An Attribute-Based Encryption Scheme to Secure Fog Communications," IEEE Access, vol. 5, pp. 9131–9138, 2017.