International Journal of Cloud-Computing and Super-Computing
Vol.2, No.2, (2015), pp. 1-6
http://dx.doi.org/10.21742/ijcs.2015.2.2.01

Attribute-based Encryption for Electronic Health Records in a Cloud Computing Environment

Emmanuel Kusi Achampong[1], and Clement Dzidonu[2]

[1]*Department of Medical Education and IT, University of Cape Coast, Cape Coast*
[2]*Accra Institute of Technology*
Email: eachampong@ucc.edu.gh

Abstract

Attributes have a major role to play in attribute-based encryption (ABE) scheme. For health records and cloud computing systems, attributes have the potential to significantly contribute to ensuring security, privacy and confidentiality of health data. This paper posits that ABE have the potential to enhance the security of health records in a cloud computing environment. The study seeks to find alternatives to improve the current state and use of some ABE schemes for health records and the cloud computing system. Attribute-based encryption schemes have the potential to minimise communication cost of the Internet, and also provide a fine-grained access control system for EHR in a cloud computing environment. In this paper, an analysis of ABE systems is discussed with their types (CP-ABE, KP-ABE, HABE and DABE) and suggestions are given for their improvement for EHR in a cloud computing environment.

Keywords: *Attribute-based Encryption (ABE), Ciphertext Policy-ABE, Hierarchical ABE, Distributed ABE*

1. Introduction

The benefits of ubiquitous computing are pushing various sensitive organisations including healthcare organisations to adopt the use of these modern technologies in the management of their data. Cloud computing is a relatively new technology that is advancing ubiquitous computing. The cloud computing system has also emerged to deliver various applications and storage services to satisfy users' expectations[1]. Cloud computing technology transforms numerous computer networks into a large single virtual computer. This therefore create unlimited storage infrastructure to execute health data with fewer maintenance cost and high scalability. Because of the Open System Architecture (OSA) of cloud computing, security, privacy and confidentiality of data are major issues in the cloud environment. These security challenges must be addressed to make the cloud computing system a convenient environment for the processing and storage of confidential data. Emerging universal computing environments demand flexible cryptographic systems that ensure a higher level of privacy and confidentiality of health data/information.

With a high number of dynamic users in these ubiquitous computing environments, implementing cryptographic methods with access control mechanisms would guarantee optimum security for Electronic Health Records (EHR) within a cloud computing environment.

Article history:
Received (August 2, 2015), Review Result (October 5, 2015), Accepted (November 1, 2015)

ISSN: 2205-8567 IJCS

Cryptographic security systems must also go with key management system that is effective and secure from user collusion. This key management system must include secure generation, storage, delivery and retrieval of encryption and decryption keys. Encryption has a major role to play in ensuring that health data/information is protected from unauthorised access and use. There are many types of encryption technologies, which are employed to ensure the security of confidential data at rest and in motion. For the purposes of this study, arguments would be advanced to confirm why attribute-based encryption method is most suitable for securing EHR in a cloud computing environment. For the cloud computing environment, data owner(s) must make flexible and scalable access control policies to control users' access rights, in order to prevent unauthorised access[2],[3].

Sahai and Waters[4] proposed an attribute-based encryption (ABE) system. The ABE system uses client's identity as attributes, and a group of attributes are used to encrypt and decrypt data. The ABE system resolves challenges encountered with the traditional public key infrastructure where data owners uses authorised user's public key to encrypt data. Nail, Adams and Miri [5] proposed a threshold attribute-based encryption, which could prevent collusion attacks. After Sahai and Waters [4] introduction of ABE, other researchers including Sahai and Waters themselves have also contributed immensely to ABE and advanced it development to the next level. Attribute-based encryption (ABE) is more appropriate to protect the privacy and confidentiality of data in a cloud computing environment[6].

Electronic health records (EHR) as a very sensitive data require high level of security in order to prevent unauthorised access. Owing to requirements for end-to-end security, straight and simple encryption (i.e., public and private key encryption) approaches cannot be used. Traditional public key infrastructure may be used in the data encryption process but may not be the best for protecting EHR in a cloud computing environment. As part of measures to protect EHR, cryptographic technologies can also be applied to ensure maximum security of the EHR.

This literature study seeks to examine attribute-based encryption (ABE) and their types and its possibility to be applied to EHR in a cloud computing environment. The study assesses the types of ABE methods and their readiness to be employed in securing EHR within the cloud computing environment.

2. Key-Policy attribute-based encryption (KP-ABE)

Goyal, Pandey, Sahai and Waters [6] proposed a key-policy attribute-based encryption (KP-ABE) scheme that made access policy part of the user's private key and defined the encrypted data with attributes of users. The KP-ABE scheme has the potential to achieve fine-grained access control. It is more flexible in KP-ABE to control users than the traditional ABE scheme. Thus, KP-ABE is an enhanced form of Sahai and Waters ABE[4]. Ostrovsky, Sahai and Waters [7] also proposed a non-monotonic access structure. Their scheme allows individual attributes to attach a word in front of them. Attribute-based encryption (ABE) may be considered as either monotonic or non-monotonic depending on the type of access structure.

Nevertheless, there are some disadvantages of KP-ABE. For KP-ABE, access policy is added to users private key, as such data owners are unable to select who can decrypt data except selecting set of attributes which are used to describe the data. This is unsuitable for the EHR application because data owners must trust the key issuer. Furthermore, the access structure in KP-ABE is a fixed structure; it cannot express negative attributes to remove users the data owner does not want to share data with.

2.1. Ciphertext-Policy attribute-based encryption (CP-ABE)

Bethencourt, Sahai and Waters [8] proposed a ciphertext-policy attribute based encryption (CP-ABE) scheme. The CP-ABE scheme resolves the problem of KP-ABE where data owners only trust the key issuer. The CP-ABE scheme includes the access policy into the data, which is encrypted with the set of attributes in the user's key. Several variants of ABE schemes have been suggested based on the CP-ABE model [9], [11], [6], [12], [13], [14], [14], [16], [16].

Ciphertext Policy Attribute-based Encryption (CP-ABE) can be generally applied as an access control method in EHR systems[17]. For example, the sensitive medical records, tightly related to patients' privacy, must be accessed only if doctors are consented by patients. Recently, CP-ABE has demonstrated to efficiently deal with EHR, by encrypting the health records with expressive access structures. Examples include "Specialty: Medicine" or "Position: Physician" [8], [18], [19]. Characteristics of CP-ABE makes it a good candidate for securing access to EHR in a cloud computing environment and as compared with KP-ABE, a better candidate.

2.2. Distributed attribute-based encryption (DABE)

Muller, Katzenbeisser and Eckert [21] proposed a distributed attribute-based encryption (DABE) scheme. In their paper, they proposed DABE as an extension of CP-ABE that supports a random number of attribute authorities that are allowed to dynamically include new users and authorities anytime. They offered an efficient design of DABE that made use of two pairing operations in the algorithm for decryption and no pairing operation for other algorithm[21].

A limitation of DABE is that access policies have to be in disjunctive normal form. A more expressive DABE system needs to be designed. DABE has the potential to be a good candidate for managing privacy and confidentiality issues of EHR in a cloud computing environment. But the addition of new users to access the EHR must have some level of control, otherwise the EHR would be open to abuse and misuse by the dynamically added users. It is always important to regulate the number of professional users who access the EHR in a cloud computing environment.

2.3. Hierarchical Attribute-based Encryption (HABE)

Wang, Liu and Wu [21] and Wang, Liu and Guo [23] proposed a hierarchical attribute-based encryption (HABE) system. This system uses a disjunctive standard form policy and produces the keys hierarchically. This system assumes that the same domain authority administers all the attributes in one conjunctive clause.

The HABE scheme uses properties of hierarchical identity-based encryption (HIBE) scheme in the generation of keys. Also, it uses disjunctive normal form (DNF) to show the access control policy. The attribute (domain) authority in the HABE scheme administers attributes in a single conjunctive clause. Four roles are identified in this scheme. These are the cloud service provider (CSP), data owner (patients and healthcare providers), the attribute (domain) authority, and data users (health professionals)[23]. The role of CSP is to work with the healthcare provider to ensure that EHR is secured from unauthorised access. Data owners and the application system must ensure that health records are encrypted after use. The role of domain (attribute) authority is to manage all the semi-autonomous multiple authorities and all professional and patient users in its domain. Users may use the generated secret keys to decrypt the encrypted health records[21].

The key generation in the HABE scheme assumes a hierarchical approach. The attribute authority makes use of the presented attribute by a user to generate a decryption key for users. This is done for the various levels of the hierarchy. HABE is a good candidate for ensuring fine-grained access of EHR in a cloud computing environment and from the arguments so far, it has the potential to ensure that the EHR is accessed by only authorised users.

3. Multi-Authority CP-ABE (MA CP-ABE) and HABE for EHR security

Müller et al. [24] first proposed the concept of MA CP-ABE. For the application of MA CP-ABE, the system was made up of a main authority (health authority) and multiple attribute authorities (departments within a healthcare facility). These attribute authorities distinctly maintain their own attributes. The key components of the system are master, attribute authorities and users including patients. The multiple attribute authorities are semi-autonomous and are able to distribute encryption and decryption keys to users within their departments who request access to the EHR. The master (health authority) only monitors the distribution of private keys by the multiple attribute authorities. Attribute authority verifies users and distributes private attribute key to users that can be used for decrypting the ciphertext. Users produce attributes that are used to provide the private key for the decryption of the ciphertext. Whenever needed user decrypts the ciphertext and retrieves the original message[24].

A combination of HABE and CP-ABE may enhance the security of EHR in a cloud computing environment. Since the key generation in the HABE scheme assumes a hierarchical approach, it has the potential to enhance the implementation of CP-ABE. The CP-ABE scheme combines the access policy with the data, which is encrypted with the set of attributes in the user's key. The combination of multi-authority CP-ABE and HABE may protect the EHR in a cloud computing environment from unauthorised and malicious access.

4. Discussion and conclusion

Multi-authority ABE model is suitable for cloud computing environments and for EHR. Electronic health records (EHR) in a cloud computing environment would require a multi-authority application of CP-ABE and HABE to ensure the security and privacy of health data.

Since EHR is a single platform for the cloud environment, managing attributes within the cloud environment can best be achieved by employing multi-authority systems for the different professionals within the healthcare setting grouped into different departments/units. To avoid collusion between users, dynamic generation of encryption and decryption keys is proposed for managing access to the EHR. The attribute authority, patients or any of the multiple authorities should be able to revoke any user when breach is suspected with certain form of limitations. The paper proposes distribution of encryption and decryption keys based on submitted attributes of patients and professional users of the EHR. The paper proposes an efficient attribute revocation technique in multi-authority CP-ABE and HABE systems. To ensure fine-grained access control, high performance, full delegation and scalability, a combination of HABE and CP-ABE may guarantee utmost security for EHR in a cloud computing environment.

In this paper, a review of the features, advantages and disadvantages of different attribute-based encryption schemes has been done. In this study, a survey of the types of ABE was explored and arguments advanced in defense of CP-ABE and HABE as most suited for EHR in a cloud computing environment. The paper explains that despite the benefits of other types of ABE like the KP-ABE and DABE, CP-ABE and HABE stands out as most appropriate for securing EHR in a cloud computing environment.

References

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing", Communications of the ACM, Vol. 53, pp. 50-58, **(2010)**.

[2] C.C. Chang, I.C. Lin, and C.T. Liao, "An Access Control System with Time-constraint using Support Vector Machines", International Journal of Network Security, Vol. 2, No. 2, pp. 150-159, **(2006)**.

[3] S.F. Tzeng, C.C. Lee, and T.C. Lin, "A Novel Key Management Scheme for Dynamic Access Control in a Hierarchy", International Journal of Network Security, Vol. 12, No. 3, pp. 178-180, **(2011)**.

[4] A. Sahai, and B. Waters, "Fuzzy Identity-based Encryption", Advances in Cryptography V EUROCRYPT, Vol. 3494, pp. 457-473.

[5] D. Nali, C. Adams, and A. Miri, "Using Threshold Attribute-based Encryption for Practical Biometric-based Access Control", International Journal of Network Security, Vol. 1, pp. 173-182, **(2005)**.

[6] N. Meghanathan, "Review of Access Control Models for Cloud Computing", Computer Science and Information Technology, pp. 77-85, **(2013)**.

[7] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded Ciphertext Policy Attribute-based Encryption", in Proceedings of the ICALP, **(2008)**, Reykjavik, Iceland.

[8] 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, **(2007)**, Alexandria, Virginia, USA.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext Policy Attribute-based Encryption", in Proceedings of IEEE Symposium on Security and Privacy, **(2007)**, Berkeley, CA, USA.

[10] L. Cheung, and C. Newport, "Provably Secure Ciphertext Policy ABE", in Proceedings of the ACM Conference on Computer and Communications Security, **(2007)**, Alexandria, Virginia, USA.

[11] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A Ciphertext Policy Attribute-based Encryption Scheme with Constant Ciphertext Length", in Proceedings of the Information Security Practice and Experience, **(2009)**.

[12] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext Policy Attribute-based Encryption and its Application", Information Security Applications, Vol. 5932, pp. 309-323, **(2009)**.

[13] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "Efficient and Provable Secure Ciphertext Policy Attribute-based Encryption Schemes", in Proceedings of the Information Security Practice and Experience, **(2009)**.

[14] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully Secure Functional Encryption: Attribute-based Encryption and Hierarchical Inner Product Encryption", Advances in Cryptology V EUROCRYPT, Vol. 6110, pp. 62-91, **(2010)**.

[15] X. Liang, Z. Cao, H. Hin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute-based Encryption", in Proceedings of the 4th International Symposium on Information, Computer and Communications Security, **(2009)**, Sydney, Australia.

[16] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based Encryption with Patially Hidden Encryptor-specified Access Structures", in Proceedings of the Applied Cryptography and Network Security, **(2008)** New York, USA.

[17] B. Waters, "Ciphertext Policy Attribute-based Encryption: An Expressive, Efficient and Provably Secure Realisation", Public Key Cryptography V PKC, pp. 53-70, **(2011)**, Taormina, Italy.

[18] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-based Systems," in ACM Conference on Computer and Communications Security, **(2006)**, Alexandria, Virginia, USA.

[19] 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, **(2006)**, Alexandria, Virginia, USA.

[20] M. Chase, and S.S.M. Chow, "Improving Privacy and Security in Multi-authority Attribute-based Encryption", in ACM Conference on Computer and Communications Security, **(2009)**, Chicago, Illinois, USA.

[21] S. Muller, S. Katzenbeisser, and C. Eckert, "Distributed Attribute-based Encryption", in Proceedings of ICISC, **(2008)**.

[22] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-based Encryption for Fine-grained Access Control i Cloud Storage Services", in Proceedings of the 17th ACM Conference on Computer and Communications Security, **(2010)**, Chicago, Illinois, USA.

[23] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical Attribute-based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers", Computer and Security, Vol. 30, pp. 320-331, **(2011)**.

[24] S. Müller, S. Katzenbeisser, and C. Eckert, "On Multi-authority ciphertext-policy attribute-based encryption", Bulletin of the Korean Mathematical Society, Vol. 46, No. 4, pp. 803-819, **(2009)**.

Authors

Mr. Emmanuel Kusi Achampong

Emmanuel Kusi Achampong is a Lecturer at the Department of Medical and Information Technology, School of Medical Sciences, College of Health and Allied Sciences, University of Cape Coast. Mr. Achampong teaches medical informatics. His research interests include electronic health records, cloud computing security and e-learning technologies.

Prof. Clement Dzidonu

Professor Clement Dzidonu is a professor of computer science at the Accra Institute of Technology (AIT), Ghana.