Privacy-preserving access control for sharing health data in cloud environment

Insaf Boumezbeur
LIRE Laboratory
University Constantine 2
insaf.boumezbeur@univ-constantine2.dz

Karim Zarour
LIRE Laboratory
University Constantine 2
karim.zarour@univ-constantine2.dz

Abstract

Cloud computing has been developed as a critical computing paradigm to offer inescapable and on-demand availability of different resources within the shape of hardware, software, infrastructure and storage. Cloud computing offers several advantages that make it more adopted by different domains, especially the healthcare field. It plays an important role in the sharing of health data. However, putting sensitive health data to the cloud still implies severe privacy risks, particularly the issues of access control that are still far from being solved. Besides, patients certainly do not need their personal and sensitive data to be shared with another one who is not completely trusted or not authorized. This paper surveys some important founding and recent works that have proposed solutions to the problem of access control and privacy ensuring in the cloud healthcare systems. These access control preserving-approaches have been compared together according to their strengths and weaknesses. In addition, the paper proposes a hybrid solution for access control based on the RBAC and ABAC models.

1 Introduction

Cloud computing paradigm is widely used by healthcare domain for different purposes such as storing, sharing and management of health data. Due to the cloud computing benefits, many healthcare organizations are considering adopting this technology to resolve different issues in healthcare field. It became a fundamentally portion of the operation of health. It can enable focusing on healthcare organizations efforts, healthcare services and improving patient care. It gives a higher way to realize sharing sensitive information to hospital and third-party research or healthcare institutions. It also can improve the transfer, availability and retrieval of health records, sharing large data volumes as well as exchanging Electronic Medical Record (EMR) between hospitals and healthcare organizations. Moreover, it makes possible to remote patient monitoring by medical providers [Bou18].

On the other hand, there are boundaries for sharing health data through cloud. The patient health information is exceptionally sensitive since it incorporates personal information, medical history, treatment, related infections, symptoms or indeed the family health history. The moving of these sensitive health data or health records to the cloud managed by third-parties is susceptible to unauthorized access, consequently, implies severe privacy risks. For example, a doctor in hospital, who is trusted and authorized, completely has the access to the health information including personal information. However, patients certainly do not need their personal and sensitive data to be shared with another one who is not completely trusted or not authorized.

Sharing health data in cloud environment raises important concerns about the security and privacy of these data, so that needs particular attention. It must be ensured that sensitive health data are accessible only to authorized parties. To protect data from unauthorized access, the control must be given to the appropriate users who will decrypt and use this data adequately. The health information constitutes a serious breach of the privacy of the patient that is why it must be dealt with carefully. Whereas the privacy issues are the foremost critical variables for the adoption of cloud computing in healthcare domain, frequently, privacy-preserving is one of the most concerns in e-health cloud systems especially in sharing health data. According to the literature, several works discuss corresponding data privacy preserving issues in sharing health data and present novel mechanisms to solve access control.

The remainder of this paper is organized as follows: Section 2 gives a background about the medical records and access control models. In section 3, we survey literature related to access control in sharing health data in cloud. Section 4 shows the results of the presented solutions' comparison. Sections 5 describes some recommendations. Section 6 closes this paper with conclusion.

2 BACKGROUND

2.1 MEDICAL RECORDS DEFINITION

Medical records fall into three main categories: Electronic Medical Record (EMR), Electronic Health Record (EHR) and Personal Health Record (PHR) [Zha10]. These categories describe completely different concepts according to HIMSS analytics (Healthcare Information and Management Systems Society). EMR is a computer tool used by the doctor to monitor the progress of the patient in hospital or in consultation as well as the various procedures performed during his stay. EHR is the latest evolution in healthcare. It is defined as a shared digital record. PHR is the health record that is initiated and maintained by an individual.

2.2 RELATIONSHIP AMONG PHR, EMR AND EHR

A patient's medical records may refer to PHR, EMR and EHR. A part of PHR can be obtained from the EMR systems of different Health Service Provider Organizations (HSPOs). Once the EMR data are shared with other HSPOs, they become EHRs. Due to confidentiality, many patients do not want to place their PHRs in EMRs or EHR systems. Figure 1 presents the intrinsic relationship between PHR, EMR and EHR from a patient perspective. PHR, EMR and EHR overlap partially. The degree of overlap differs from one patient to another due to the requirements of personalized confidentiality [Zha10].

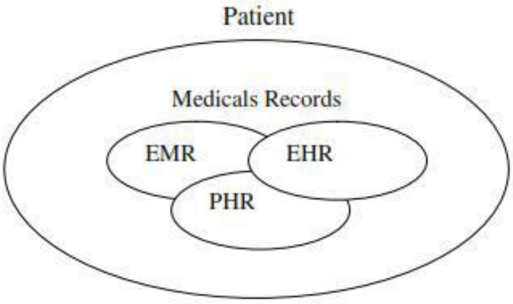

Figure 1: Relationship among PHR, EMR and EHR [Zha10].

2.3 ACCESS CONTROL MODELS

2.3.1 Role Based Access Control (RBAC)

The access permission is accepted or rejected based on the user role. In this context, the users must not only be members in more than one group but also having different roles and responsibilities in each group. So, depending on roles and privileges they are allowed to read the information [Cha16].

2.3.2 Attribute Based Access Control (ABAC)

ABAC describes an access control model where access rights are admitted to users by the use of policies. Attributes are properties that describe specific features of the subject, object, environment conditions, and requested actions that are predefined and preassigned by an owner or administrator or authority [Aft15].

2.4 ATTRIBUT BASED ENCRYPTION VARIANTS

2.4.1 Key Policy Attribute Based Encryption (KP-ABE)

It is the modified form of classical model of ABE. Users are assigned with an access structure (AS) over the data attributes. **In order** to reflect the access structure, the secret key of the user is defined. Cipher texts are labeled with sets of attributes and private keys are associated with monotonic access structure that control which cipher texts a user is able to decrypt [Lak15].

2.4.2 Cipher text Policy Attribute Based Encryption (CP-ABE)

The converse of KP-BE, a message in the CP-ABE is encrypted under an access policy that defines the access structure, whereas the users' private keys are associated with a set of attributes. Then, only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. [Abb14]

2.4.3 Multi-Authority Attribute Based Encryption (MA-ABE)

Multi-authority attribute-based encryption scheme uses multiple parties to distribute attributes for users. A Multi Authority ABE system is composed of K attribute authorities and one central authority. Each attribute authority is also assigned a value dk [Lak15].

3 SOLUTIONS TO PRESERVE ACCESS CONTROL

Access control mechanism is an important part of security to protect sensitive data from unauthorized access of malicious users. A secure access control mechanism is necessary to ensure data privacy. Access control mechanisms can be classified into three categories: Identity Based Access Control (IBAC), Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC). IBAC is not realizable in cloud environment because the number of users in the cloud environment is too large.

On the other hand, Attribute-Based Encryption (ABE) is a good technique for realizing scalable, flexible, and fine-grained access control solutions. The main types of ABE are Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute-Based Encryption (KP-ABE).

3.1 ROLE AND ATTRIBUTE-BASED ACCESS CONROL

Several papers have used ABAC model to preserve access control in cloud-based e-health [Sah11] [Seo18] [Pus16] [ROG 13] [Med17]. In [Sah11] the authors proposed a technique for aspect-based Electronic Health Record access policy administration on ABAC. This technique creates a desirable EHR access policy on the fly by using subject’s attributes and a set of primitive policies as input. The authors in [Lu13] proposed a secure and privacy preserving opportunistic computing framework (SPOC) for mobile healthcare (m-healthcare) emergency. The proposed framework implements an efficient access-control methodology using ABAC to achieve privacy in their m-Health system.

[Pus16] proposed a secure attribute based EHR sharing scheme using selective disclosure of attributes to preserve a secure and flexible EHR sharing scheme. The proposed ABAC model capable of provisioning fine grained EHR access. In [Seo18], the authors proposed an ABAC model based on XML, which divided into access control and the application of encryption and digital signatures. The proposed model protects the security of patients' privacy and achieves convenient access control.

Other works such as [Nag14] [Liu15] [PRO 16] used the RBAC as access control mechanism. The authors in [Nag14] proposed a secure mobile health application based on a hybrid cloud, by coordinating cryptographic techniques and RBAC, to protect healthcare data of patients and improves medical services by means of providing security and privacy. In [liu15], the authors have combined RBAC with Hierarchical Identity-Based Encryption (HIBE) schema to come up with an encryption technique to secure patient’s data before they are outsourced to the storage data. [Gop16] proposed an Electronic Patient Health Record (EPHR) reference security model to handle efficiently the patients EPHR data. The proposed model consists of a multi-level data flow hierarchy, and an efficient access control framework based on the conventional RBAC and Mandatory Access Control (MAC) policies.

3.2 ATTRIBUTE-BASED ENCRYPTION (ABE)

Many access control schemes using attributed-based encryption, which adopts the KP-ABE and CP-ABE to enforce fine-grained access control. In [Als12], the authors presented a design that provides secure access to EHRs using CP-ABE. This design offers effective solutions to some of the issues related to standard encryption mechanisms. [Wan13] designed and implemented a patient-centric, cloud-based PHR system based on open source Indivo project using CP-ABE mechanism. The proposed system focused on the fine-grained control to read and decrypt. The authors in [Zha18] proposed a Privacy Aware Smart Health access control system (PASH) which is privacy aware s-health access control system. The PASH introduces a large universe CP-ABE scheme with partially hidden access policies to deal with both data security and user privacy issues. A new method to realize a secure fine-grained access control to PHRs is proposed in [Yan16], which is based on ABE primitives and division of the PHR data into privacy levels. The proposed method used KP-ABE to provide fine-grained access control storage system for outsourced sensitive data. It can also provide efficient user revocation by using a timestamp in the private key.

Others ABE variation is Multi Authority Attribute Based Encryption (MA-ABE) which is used in [Li13] to propose a novel framework of secure sharing of personal health records in cloud computing to reach fine-grained and scalable data access control for PHRs. [Shr16] combined efficient encryption algorithms such as Advanced Encryption Standard (AES) and MA-ABE schemes to present a secure healthcare system against attacks from unauthorized users.

The used of RBAC and ABAC alone in medical system have some restrictions. In order to secure sharing personal health records in cloud computing [Med17] proposed a new scalable lightweight data access control scheme using KP-ABE encryption and ABAC model. The proposed scheme ensures fine-grained access control and data confidentiality of PHRs. In [Fab15] the authors presented data sharing strategy in multi-cloud environment, which provides a high level of security and privacy for patient data in semi-trusted cloud computing environments. The approach enforces RBAC through CP-ABE.

According to [Hsi12], the authors proposed a design for a secure interoperable cloud-based Personal Health Record service that uses a self-protecting security framework that integrates access control, confidentiality, integrity control, and authorization in an integrated and fine-grained way. A new architecture for storing and sharing of personal health records in federated cloud environment proposed in [Sin13] using MA-ABE and ABAC model. In this system patient should have full control over their privacy by encrypting the PHR’s and providing fine-grained access.

4 DISCUSSION AND REMARKS

This paper presents some works over the past nine years (2011-2018). The approaches that using ABAC as an access control model achieved the flexibility. This is due to the dynamic nature of an open and distributed ABAC system contrary to RBAC, which has a static nature. The ABAC model supports dynamic environments so it is more scalable in

Cloud environment. However, RBAC is famous because of its robustness and ease of management for permissions and roles. Meanwhile ABAC does not provide ease of management for the administrator due to heterogeneity of the user attributes.

An important point, the works that applied CP-ABE and KP-ABE schemes are used to achieve flexible, security, privacy, data confidentiality and fine-grained access control of outsourced data in cloud computing. All solution using CP-ABE, KP-ABE and MA-ABE achieved the collusion resistant and data confidentiality.

The comparison between these two schemas gives that in CP-ABE, there is an access tree for the ciphertext, whereas in KP-ABE, there is an access tree for the private key [Yük17]. The CP-ABE keeps the access policy decisions in the hand of the data owners, which means that it is more appropriate for the data sharing system. Moreover, the CP-ABE improves the disadvantage of KP-ABE. The CP-ABE improves the disadvantage of KP-ABE. Indeed, the data owner who encrypt data has no explicit control over who has access to the data he encrypts. The encryptor cannot decide who is the decryptor of data [Atr17]. In CP-ABE, the encryptor can specify a suitable access policy over which the data is encrypted [Moh14]. However, the CP-ABE scheme is highly efficient whereas. In KP-ABE, the anonymous users obtaining the private key can easily tamper the data [Shy17].

Further, the CP-ABE has much more flexibility and is more suitable for general applications, which means that is one of feasible schemes compared with KP-ABE, which is not naturally suitable to certain applications. In addition, the CP-ABE can support the access control in the real environment and the level of user access depends on upon the number of attributes possessed by the data users through which it achieves the property of fine-grained access control [Shy17].

On the other hand, in CP-ABE scheme, delegation of private keys is much simpler compared to KP-ABE delegation [Zhe11]. Generally, CP-ABE is conceptually closer to RBAC, while KP-ABE is closer to ABAC [Zhe 11]. Finally, Table 1 gives a comparison of the studied solutions in terms of access control with identifying strengths and weaknesses.

Table 1: COMPARISON OF ACCESS CONTROL PRESERVING SOLUTIONS.

work	Year	Access model	Strengths	Weaknesses
Sah11	2011	ABAC	EHR access policy flexible, scalable, cost-effective manner.	Not able to protect access to other types of resources
Als12	2012	CP-ABE	Ensures flexibility, scalability. Fine-grained access control. Collusion resistant. Data confidentiality	Interoperability. Verification user attributes. User accountability. User revocation.
Hsi12	2012	RBAC/CP-ABE	Access control, confidentiality, integrity control, and authorization. Collusion resistant.	User accountability.
Lu13	2013	RBAC	Height reliability of PHI. Efficient user-centric privacy access control	Inflexible access control.
Sin13	2013	ABAC/MA-ABE	Flexibility. Fine-grained access control. Collusion resistant. Data confidentiality	-
Wan13	2013	CP-ABE	Fine-grained access control. Collusion resistant.	User accountability. User revocation.
Li13	2013	MA-ABE	Efficient revocation. Dynamic modification of access policies. Fine-grained access control Collusion resistant.	Methods only for KP-ABE systems.
Nag14	2014	RBAC	Availability, confidentiality, integrity.	Inflexible access control.
Fab15	2015	RBAC/CP-ABE	Fine-grained access control. Collusion resistant. Data confidentiality	Does not guarantee the malicious attacks, data integrity.
Liu15	2015	RBAC	Data confidentiality. Revocation.	Inflexible access control.
Pus16	2016	ABAC	Flexible EHR sharing scheme. User revocation, flexible access.	**-**
Gop16	2016	RBAC/MAC	Robustness, Practicality.	Inflexible access control.
Yan16	2016	KP-ABE	Fine-grained access control. Confidentiality.	Scalability. User accountability.

			Collusion resistant.	User revocation.
Shr16	2016	MA-ABE/AES	Fine grained access control. Scalability, confidentiality, collusion resistant.	-
Med17	2017	ABAC/ KP-ABE	Fine grained access control. Confidentiality, flexibility. Collusion resistant.	-
Seo18	2018	ABAC	Guarantees patient privacy. Assure confidentiality. Authorization integrity. Flexible access control.	Does not improve the security of the ABAC protocol process.
Zha18	2018	CP-ABE	Fine grained access control. Collusion resistant. Data confidentiality	User accountability. User revocation.

5 Recommendations in Access Control Layer

Each medical actor must have his own credential key automatically generated and delivered by the hospital or health authorities to access EMR or EHR. On the other hand, they supply a username and password to different actors from the hospital or other health organization to access databases. The EMR and EHR must be associated with access control for designated actors or groups of actors having the right to read the contents of the record and to add information in a systematic way or using some conditions. Here we mean by a group of actors the team that will take care of a patient. Any other actor that does not have these rights must not have access. A Better protection is possible when we consider the roles of health actors. For each role, we associate permissions represented by access rights. Our recommendation is to combine two important models of access control illustrates in Figure 2. They are RBAC and ABAC. With RBAC, the users have access permissions according to these roles. It provides easier management of access rights. Indeed, health care systems (especially EMR and EHR) contain multiple users playing various roles, e.g. there are users who have the doctor role, others play the nurse role and other users play the patient role...

RBAC is insufficient to control access to an open environment like the cloud. The dynamism and flexibility of the ABAC model are a major cause of our choice. The combination of both models allows combining the advantages of each other. Each user must activate its role and create its session according to its attributes. To open the session, it must identify and authenticate. If authentication is enabled, the session is opened and the user can access objects and perform operations on these objects according to the access level. Else, the session does not open and access is prohibited. The authorizations are not associated only with the roles, but also to the attributes of the subjects (e.g. identifier of doctor) objects (EMR or EHR) and environment (e.g. time). The following Table 2 shows the advantage of the hybrid model. The rest of our recommendations are:

- Virtual Private network (VPN) between all health information systems, patient home and the data center using wireless network links between them. This is achieved by sourcing the services from an Internet Service Provider (ISP).
- Local data to satisfy local needs and not necessarily to interact with other local databases. Indeed, the health actors and patients are very attached to their personal notes for their own use. However, it is essential to share this information with other stakeholders.
- Hospital or health authorities have a number of powers recommendation, decision, regulation and sanction. They also ensure some form of control over different medical staff.
- The medical actors will be able to access the databases via internet. The patient will access his medical records using credentials from these devices. EHR/EMR consists of an important amount of information. It is stored and capable to be consulted even from distance. The sharing of medical information is vital in medicine concerning at the same time: diagnosis, prognosis, analysis and care continuance. It is a progress factor for better medical care, faster and adapted, and so, systematically transmits information to other participants. To improve information traffic and functioning of our approach, the medical record is primordial. It helps to: (i) Minimize medical errors, (ii) Accelerate knowledge diffusion and (iii) Help decision-making.
- View: It is a logical representation of subsets of information. This concept limits access to the EHR / EMR. It allows presenting the same data according to different views. For example, the emergency doctor has the right to a global view of EHR/EMR, but an ophthalmic specialist doctor has the right to a view concerning the data related to his field. These views are represented according to the access level of each user.
- Time: This concept allows the management of access rights according to the temporal condition. It allows checking if the user has the right to perform or not certain tasks or operations in the current time. For example, in cases of work leave, the treating physician has the right to access only his patients' information.
- In regards to the cryptographic techniques, the variants of ABE are usually used to enforce access control policies in healthcare systems. CP-ABE and KP-ABE enables the encryption of sensitive information according to an attribute-based policy in such a way, only the authorized entities with certain roles who will decrypt and access this information, and that in order to protect the data from accessed by unauthorized parties. According to the discussion in section 4, the CP-ABE technique is more suitable for healthcare field than KP-ABE.

Furthermore, a virtual collaborative working space reserved for all user actors allows them to work while being geographically distant and by keeping a permanent assistance around the patient. Each patient, doctor or nurse uses his or her mobile handset for accessing the medical record stored in hospital or health organization database. Each of the actors will have a different level of access to the EHR/EMR. This is part of the security measures to prevent any leakage of important record. Therefore, the actor needs to be authenticated before being able to view the available record.

Table 2: THE ADVANTAGES OF HYBRID SOLUTION

Characteristics	**RBAC**	**ABAC**	**Hybrid solution**
Flexibility	No	Yes	Yes
Dynamic	No	Yes	Yes
Less of a privilege	No	Yes	Yes
Change privilege	Difficult	Easy	Easy
Simplicity	Yes	No	Yes
Policy	Simple	Complex	Simple

Flexibility: RBAC is not flexible in an open environment unlike the ABAC model. Thus, the hybrid model is flexible.

Dynamic: RBAC is static and ABAC is Dynamic. The latter is based on users attributes. Hybrid model is static and dynamic.

Less privilege: there is little privilege in RBAC because users who have the same role have the same privileges. This is the case in hybrid model.

Change privileges: Changing a user's privilege is very difficult in the RBAC system. Indeed, to change a user's privilege, it is mandatory to change the user's role. This requires a change in policy. On the other hand, in the ABAC system to change a user's privilege there is no need to change the security policy and the user's identity. In hybrid model, it is very easy to change the user's privileges. Indeed, if there is a change in the authentication or authorization process, it is done at a specific point.

Simplicity: RBAC is very simple and easy to use. Authorizations are statically assigned to roles according to predefined policies. ABAC is more complex due to the heterogeneity of users attributes.

Policy: In RBAC, policy specification is easy. However, in ABAC, it is very difficult because the heterogeneity of its attributes.

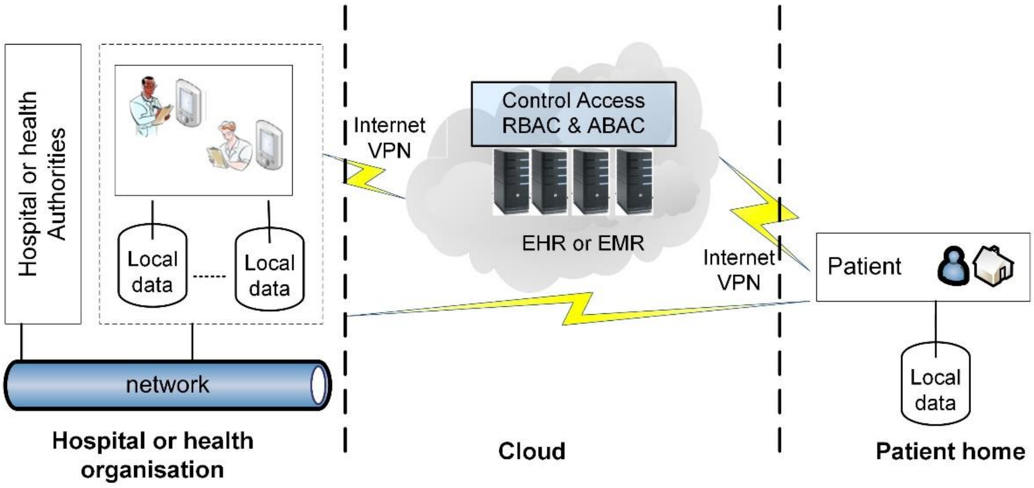

Figure 2: The proposed recommendations

6 CONCLUSION

The access control in sharing health data in cloud environment is an important issue that needs particular attention. In this paper, we have presented a review of solutions based on several studies that mainly focus on the important issue of access control in sharing health data in a cloud. We have presented a comparison of the access control preserving-approaches. Moreover, we have proposed a hybrid solution for access control based on the RBAC and ABAC models. We recommended two important concepts: views and time. Our proposal solution provides secure, flexible and adaptable access. It improves the relationship between patients and health organizations and increases the trust between them. Various research results have proposed approaches to enforce the access control of shared health data in cloud. Despite all these efforts, there are also many issues still need more attention, to protect patient data from being accessed only by authorized users. As a first observation, RBAC and ABAC have shown some limitations when they are used alone in medical system. On the hand ABAC model is the most suitable model for a cloud environment. Usually, the variants of Attribute-based encryption are envisioned as a highly promising solution to realize fine-grained access control. Most of the existing works on ABAC-based access control mechanisms use a cryptographic primitive Attribute Based Encryption. Finally, in CP-ABE the ability that data owner selects an access structure based on attributes and encrypt data under this structure makes it more suitable to control data access in cloud than KP-ABE.

References

[Abb14] A. Abbas, S. U. Khan. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics, 18(4): 1431-1441, 2014.

[Aft15] M. U. Aftab, M. A. Habib, N. Mehmood, M. Aslam, M. Irfan. Attributed role based access control model. In 2015 Conference on Information Assurance and Cyber Security (CIACS) (pp. 83-89), IEEE, December 2015.

[Als12] S. Alshehri, S. P. Radziszowski, R. K. Raj. Secure access for healthcare data in the cloud using ciphertext policy attribute-based encryption. In 2012 IEEE 28th International Conference on Data Engineering Workshops (pp. 143-146). IEEE, April 2012.

[Atr17] S. Atram, N. R. Borkar. A Review Paper on Attribute-Based Encryption Scheme in Cloud Computing, 2017.

[Bou18] I. Boumezbeur, K. Zarour. Privacy Preserving Requirements for Sharing Health Data in Cloud. In International Conference Europe Middle East & North Africa Information Systems and Technologies to Support Learning (pp. 412-423). Springer, Cham, October 2018.

[Cha16] R. Charanya, M. Aramudhan, Ra. K. Saravananguru. A Review on Access Control Issues in Ehealth Application in Cloud Computing. Indian Journal of Science and Technology, 9(42): 1- 5, 2016.

[Fab15] B. Fabian, T. Ermakova, P. Junghanns. Collaborative and secure sharing of healthcare data in multi-clouds. Information Systems, 48: 132-150, 2015.

[Gop16] P. Gope, R. Amin. A novel reference security model with the situation based access policy for accessing ephr data. Journal of medical systems, *40*(11): 242, 2016.

[Hsi12] G. Hsieh, R. J. Chen. Design for a secure interoperable cloud-based Personal Health Record service. In 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings (pp. 472-479). IEEE, December 2012.

[Lak15] R. N. Lakshmi, R. Laavanya, M.Meenakshi, C. S. G. Dhas. Analysis of attribute based encryption schemes. International Journal of Computer Science and Engineering Communications, 3(3): 1076-1081, 2015.

[Li13] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE transactions on parallel and distributed systems, *24*(1): 131-143, 2013.

[Liu15] W. Liu, X. Liu, J. Liu, Q. Wu, J. Zhang, Y. Li. Auditing and revocation enabled role-based access control over outsourced private EHRs. In High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conference on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on (pp. 336-341). IEEE. August 2015.

[Lu13] R. Lu, X. Lin, X. Shen. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE transactions on parallel and distributed systems, 24(3): 614-624, 2013.

[Med17] N. Meddah, A. Jebrane, A. Toumanari. Scalable Lightweight ABAC Scheme for Secure Sharing PHR in Cloud Computing. In International Conference on Advanced Information Technology, Services and Systems (pp. 333-346). Springer, Cham, April 2017.

[Moh14] A. Mohandas. Privacy preserving content disclosure for enabling sharing of electronic health records in cloud computing. In Proceedings of the 7th ACM India Computing Conference (p. 7). ACM, October 2014.

[Nag14] K. A. Nagaty. Mobile health care on a secured hybrid cloud. J Sel Areas Health Inform, *4*(2): 1-9,2014.

[Pus16] H. S. G. Pussewalage, V. A. Oleshchuk. An attribute based access control scheme for secure sharing of electronic health records. In e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on (pp. 1-6). IEEE, September 2016.

[Sah11] N. Sahavechaphan, U. Suriya, N. Harnsamut, J. Phengsuwan, K. Aroonrua. An efficient technique for aspect-based EHR access policy administration on ABAC. In *ICT* and Knowledge Engineering (ICT & Knowledge Engineering), 2011 9th International Conference on (pp 27-33). IEEE, January 2012.

[Seo18] K. Seol, Y. G. Kim, E. Lee, Y. D. Seo, D. K. Baik. Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System. IEEE Access, *6*: 9114-9128, 2018.

[Shr16] N. M. Shrestha, A. Alsadoon, P. W. C. Prasad, L. Hourany, A. Elchouemi. Enhanced e-health framework for security and privacy in healthcare system. In Digital Information Processing and Communications (ICDIPC), 2016 Sixth International Conference on (pp. 75-79). IEEE, April 2016.

[Shy17] P. G. Shynu, K. J. Singh. An enhanced ABE based secure access control scheme for E-health clouds. International Journal of Intelligent Engineering and Systems, *10*(5): 29-37, 2017.

[Sin13] R. Singh, V. Gupta, K. Mohan. Dynamic federation in identity management for securing and sharing personal health records in a patient centric model in cloud. International Journal of Engineering and Technology, *5*(3): 2201-2209, 2013.

[Wan13] C. Wang, X. Liu, W. Li. Design and implementation of a secure cloud-based personal health record system using. Int. J. of Intelligent Information and Database Systems, *7*(5): 389-399, 2013.

[Yan16] H. Yan, J. Li, X. Li, G. Zhao, S. Y. Lee. Shen, J. Secure access control of e-health system with attribute-based encryption. Intelligent Automation & Soft Computing, *22*(3): 345-352, 2016.

[Yük17] B. Yüksel, A. Küpçü, Ö. Özkasap. Research issues for privacy and security of electronic health services. Future Generation Computer Systems, 68: 1-13, 2017.

[Zha10] R. Zhang, L. Liu. Security models and requirements for healthcare application clouds. In 2010 IEEE 3rd International Conference on cloud Computing (pp. 268-275). IEEE, July, 2010.

[Zha18] Y. Zhang, D. Zheng, R. H. Deng. Security and privacy in smart health: efficient policy-hiding attribute-based access control. IEEE Internet of Things Journal, *5*(3): 2130-2145, 2018.

[Zhe11] Y. Zhen. Privacy-preserving personal health record system using attribute-based encryption (Doctoral dissertation, Worcester Polytechnic Institute), 2011.