EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Privacy-Preserving Data Sharing using Multi-layer Access Control Model in Electronic Health Environment

Shekha Chenthara[1,*], Khandakar Ahmed[1], Frank Whittaker[1]

[1]Victoria University, Melbourne, Australia

Abstract

Electronic Health Data (EHD) is an emerging health information exchange model that facilitates healthcare providers and patients to efficiently store and share their private healthcare information from any place and at any time as per demand. Generally, Cloud services provide the infrastructure by reducing the cost of storing, processing and updating information with improved efficiency and quality. However, the privacy of Electronic Health Records (EHR) is a significant hurdle while outsourcing private health data in the cloud because there is a higher peril of leaking health information to unauthorized parties. Several existing techniques are able to analyse the security and privacy issues associated with e-healthcare services. These methods are designed for single database, or databases, with an authentication centre and thus cannot adequately protect the data from insider attacks. Therefore, this research study mainly focusses on how to ensure the patient privacy while sharing the sensitive data between same or different organisations as well as healthcare providers in a cloud environment. This paper proposes a multi-layer access control mechanism named MLAC Model to construct a secure and privacy-preserving EHR system that enables patients to share their data with stakeholders. In this paper, we use a Dual layer access control model named Pseudo-Role Attribute based access control (PR-ABAC) mechanism that integrates attributes with roles for the secure sharing of EHR between multiple collaborators. The proposed framework also uses the concept of Provenance to ensure the Integrity of patient data. This work is expected to provide a foundation for developing security solutions against cyber-attacks, and thus contribute to the robustness of healthcare information sharing environments.

Received on 08 February 2019; accepted on 20 May 2019; published on 04 July 2019

Keywords: Electronic Health Records, security, privacy, MLAC, cyber-attacks, Provenance

Copyright © 2019 Shekha Chenthara *et al.*, licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi:10.4108/eai.13-7-2018.159356

1. Introduction

EHD (also known as electronic health records or computerised patient records) is a systematic collection of electronic health information about individual patients or populations [1]. Such records include a whole range of data including demographics, medical histories, medication and allergies, immunisation status, laboratory test results, radiology images, billing information and all sensitive patient information. EHD systems have significant advantages over traditional systems based on paper records. Unlike paper-based records, EHR incur less manpower, time and physical storage [2]. The advantages of EHRs include easier access to clinical data, ability to maintain effective clinical workflows, fewer medical errors, improved patient safety, reduce medical costs, stronger support for clinical decision-making, etc. Across Australia, millions of healthcare documents are sent across

[*]Corresponding author. Email: Shekha.chenthara@live.vu.edu.au

the country. Over 90% of Australian medical service providers have adopted EHD systems, as the value of EHDs can provide vital information for medical resource allocation, medical research, and improved healthcare. According to a national survey : 94% of providers reported that their EHR makes records readily available at point of care, 88% reported that their EHR produces clinical benefits for the practice, 75% of providers reported that their EHR allows them to deliver better patient care [2]. However, the transition from paper-based to EHR systems poses some unique challenges for privacy and confidentiality, security, data integrity and availability.

As Cloud computing is emerging as a new computing paradigm in healthcare sector [3], it not only facilitates the exchange of electronic medical records (EMR) among healthcare providers or organisations, but also acts as a medical record storage center. As the health data is increasing day-by-day in the big data epoch, cloud plays an important role for data storage by providing virtually unlimited storage that can be accessed over the Internet [4]. That facilitates healthcare providers and patients to create, manage and access healthcare information from any place and at any time per demand. Cloud services provide the infrastructure by reducing the cost of storing, processing and updating information with improved efficiency and quality. As computerised medical records are integrated into one place, data can be accessed from different places by different users and this increases the risk of invasion of privacy. Since most of the data are sensitive, strictly confidential and stored on a third-party server where the owner does not have direct access, entails serious threats in terms of data privacy [5] and security [6]. Patient with chronic conditions and associated sensitive information need to be securely shared and accessed by healthcare providers. This project will focus on identifying the most appropriate method to share private information between multiple healthcare providers in the patients' care team and the patient and their family or carers in the cloud environment.

Hence, EHRs in healthcare is facing problems with privacy breaches and unauthenticated record access in the recent years, the prime most one is related to privacy [7] and security of medical data [6]. The issues range from malware attacks that compromise the integrity of systems and confidentiality of patients to distributed denial-of-service (DDoS) which can disrupt facilities ability to provide patient care. In healthcare systems, for instance, cyber-attacks like Ransomware can have ramifications beyond financial loss and breach of privacy [8]. Earlier this year, hackers broke into the databases of Community Health Systems (CHS), one of the largest hospital groups in the United States, and accessed personal health information, name, address and personal data including social security numbers from around 4.5 million patients. Hackers from Internet vigilante group Anonymous also targeted several hospitals, launching a DDoS attack on the hospital website as an act of hacktivism [9]. So, there is an indispensable need to protect the privacy, security, confidentiality, integrity, and availability of protected health information (PHI) in EHR [10]. In this context, Cyber security is utmost required to prevent, detect, and act on unauthorized access to health system and its impact towards social, economic, political and cultural conflicts. Therefore, the primary research question is to strengthen the security infrastructure by providing protection mechanism in e-health care [11] aiming towards patients' confidence and thereby providing privacy [12] to EHD. The research work mainly focusses on how to ensure the patient privacy while sharing the data between same or different organisations as well as healthcare providers in a cloud environment. It emphasises on how we can access and transfer the data efficiently in a cloud arena. The main research questions include:

RQ1: What are the challenges and how to overcome those while sharing the data between different healthcare providers?
RQ2: How to implement privacy preserved healthcare data storage?
RQ3: How to maintain Integrity of the Electronic Health Data?

1.1. Individual Objectives

This research aims to build a multi-party framework that effectively and securely stores, access and share patient data between the different organisation and healthcare providers while preserving patient confidentiality. The overall aim of the research is to develop a secure and efficient task-based multi-party framework thereby strengthen the security infrastructure in health care aiming towards patients' confidence in e-health care and thus providing security and privacy to EHD. It also points to strengthening the data security to prevent a possible breach of data by providing efficient Access Control Mechanisms for data sharing on EHD database federations. To achieve the overarching aim of the project the following individual objectives are identified: The individual objectives

1. Initially, the research will focus on how appropriate access control mechanisms can be applied to EHD for ensuring the data privacy so that the system will be immune to both inside and outside attacks. This will also reduce the cost of managing access control to

encrypted EHD and thus provide a practical solution to data mining on encrypted EHD database federations; our research will improve population health knowledge to the benefit of Australians' wellbeing.

2. Data is encrypted and stored in a third-party system like Cloud. Since the data is stored in an encrypted form, normal searching schemes cannot be applied. We should have some 'searchable database' implementation to query the data. Otherwise, either the entire data should be downloaded to the local system, decrypt and search OR decrypt in the cloud system itself and search and retrieve only the required files. The former approach results in high bandwidth consumption and the latter results in a security violation.

3. Up to what extent, the access control should be implemented. In some cases, table level access control is sufficient whereas, in others, access control should be implemented to rows, columns and to each cell. E.g., an orthopaedic doctor needs to access only rows related to orthopaedic data. An insurance person should have access to the insurance related details and not to medical records.

4. Focus to improve privacy protection against insider attacks and to provide security in data storage. Our research will be protecting patient data against both outsider and insider attacks, which uses the concept of provenance thereby, maintain the confidentiality and integrity of the data. Our work will empower medical research thereby this work will develop a privacy-preserving Electronic Health Data federation system.

The rest of the paper is organised as follows. Section 2 describes the contribution from academic and practical view and section 3 describes an intensive analysis of existing security and privacy preserving mechanisms. Section 4 describes the methodology and conceptual framework and section 5 as conclusion.

2. Contributions

Here we discuss the academic contribution and practical contribution of this research towards privacy preservation of healthcare records.

2.1. Contribution to Knowledge

The significance of the research is that it provides a practical solution to privacy-preserving data mining over EHD database federations, which will have important and comprehensive impacts. In particular, it will improve protection from insider attacks. As existing solutions are very vulnerable to insider attacks due to unauthorised access our research will provide protection based on access control models, making it impossible for medicare personnel along with employees of other organisations to jointly breach the system. The other significant factor is that it will reduce the cost of managing access control to encrypted EHDs. This will also empower medical research. The main innovation of the research is twofold. One is, joint authentication by a federation of organisations, immune to insider attacks: we will develop an EHD system with no authentication centre but a joint authentication mechanism by t out of n parties; in this way, individual parties, administrators do not have access to the encrypted EHDs and effectively block unauthorised access by insider attacks. Second innovation is to develop an access control mechanism for privacy protection of EHRs thereby securing data in Healthcare Information system.

2.2. Statement of Significance

Privacy and security of Big Data is gaining prominence nowadays due to its high proliferation and utility as a result of recent developments in Information and Communication Technology(ICT) such as social networking, IoT (Internet of things) Big data analytics and Cloud computing. Nowadays, cyber-attacks are on the rise, and it affects more in the area of health care sector at an alarming rate. Criminals and cyber threat actors often look to exploit the vulnerabilities that are associated with life-critical services that are aimed to improve the treatment and patient care, especially, with new technologies. These issues range from malware attacks that compromises the integrity of systems and privacy of patients to distributed denial of service (DDoS) which can disrupt facilities' ability to provide patient care. In healthcare systems, for instance, cyber-attacks like Ransomwares can have ramifications beyond financial loss and breach of privacy. In this context, the current project focuses on protecting the privacy of patients by strengthening security to prevent possible breach of data. The proposed work will build a system that effectively and securely share confidential patient data among several organisations that protects the data from both outsider and insider attacks. The main significance of the research is that it provides a practical solution to privacy-preserving data sharing over EHD database federations that could lead to improved comprehensiveness, coordination, efficiency, effectiveness, value of care, as well as the satisfaction of patients and providers. This work focusses on providing patient-centred care and primary care meeting important needs of patients, service providers and General Practitioners (GPs). This will also ensure excellent patient care and privacy i.e. paramount for healthcare organisations, including hospitals, medical centres, independent physicians' groups and insurance providers. Another main aspect is that protection of EHD that is stored in third party cloud can be achieved

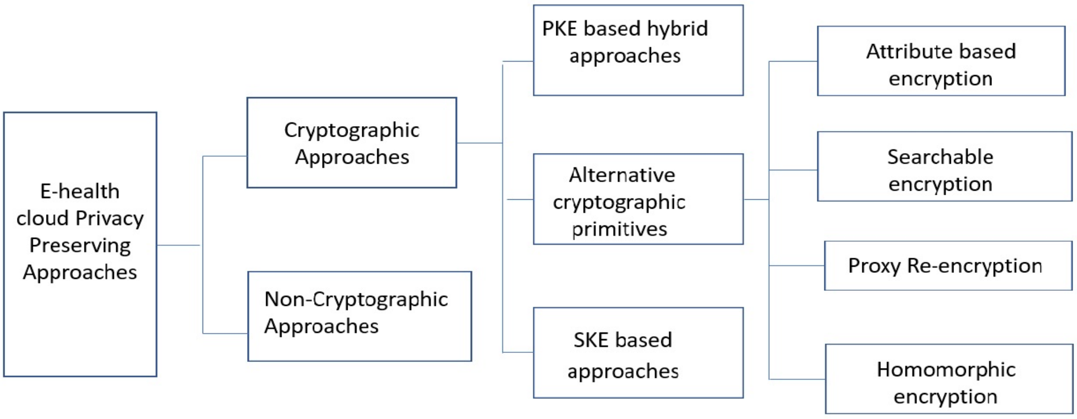

E-health cloud Privacy Preserving Approaches
Cryptographic Approaches
Non-Cryptographic Approaches
PKE based hybrid approaches
Alternative cryptographic primitives
SKE based approaches
Attribute based encryption
Searchable encryption
Proxy Re-encryption
Homomorphic encryption

Figure 1. Taxonomy of the privacy preserving approaches in the e-Health cloud

by ensuring privacy and security, and this will in turn enhance the overall welfare of patients and population.

3. Literature Review

EHDs, also known as electronic or computerised patient records, refer to a whole range of data including demographics, medical histories, medication and allergies, immunisation status, laboratory test results, radiology images and billing information [1]. As most of this EHD contain sensitive data, data breach is a major concern. Therefore, in order to protect the confidential data from possible data breaches, strict privacy preserving mechanisms have to be employed. To protect the privacy of patient data, access control [13] mechanisms and encryption techniques are being used nowadays. Taxonomy of the privacy preserving approaches in the e-Health cloud is portrayed in Fig. 1

There are several research investigations conducted in my study area by leading scientists, and the prominent ones that are reported in the literature, for instance, by Xun Yi et al. This work provides a solution to protect the privacy of patient data under multiparty framework where all EHRs are encrypted with common public key and an encrypted EHR can be decrypted only by the cooperation of all parties. This solution is built on Public Key Infrastructure (PKI) based on EIGamal Threshold public key encryption scheme [1]. This scheme uses modular exponentiation which is less expensive and re-encryption is not required. This prevents any server and collusion of up to N-1 servers and therefore can succeed from inside attack and outside attacks. This scheme achieves n server joint authentication over only one database. Attribute-based encryption (ABE)presented by Sahai et al [14] is a cryptographic primitive based on the Public Key Encryption where the messages can be encrypted and decrypted on the basis of user attributes. In this, a cipher text can be decrypted only when the attributes and the decryption keys [15]are available. It is a public key encryption in which Secret key of the user and Cipher text are dependent upon attributes. Decryption of cipher text is possible if the attributes of CT matches with attributes of secret key. In KP-ABE, using the master key, owner encrypts the data such that a cipher text is labelled with a set of attributes. In KP-ABE, keys associated with the access structure should be equal to the user's secret key for decryption. In cipher text-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a cipher text specifies an access policy over a defined universe of attributes within the system. In CP-ABE, Cipher text will have the access structure embedded in it and users can have their attributes saved in their secret keys. Multiauthority attribute-based encryption (MA-ABE) allows the users keys to be collectively generated by multiple trusted authorities that are responsible for governing the subsets of the users attributes. Broadcast cipher text-policy attribute-based encryption (bABE) is effective in direct revocation of the user keys without the need of refreshing system parameters or data encryption. bABE ensures the health data confidentiality, but it causes increased computational overheads in enforcing the access policies [6]. Yu et al [16] addressed the issues of concurrently achieving the fine-grained access, scalability and confidentiality of the outsourced data. Here the data encrypted by a single user is shared with multiple users by distributing the keys. In the proposed approach the tasks of re-encrypting the data files and updating of the secret keys are delegated to the cloud servers [17]. To deal with the heavy computation overheads caused by re-encryption of data files and update of secret key, the KP-ABE, PRE and lazy reencryption are combined.

Narayan et al [18] proposed an attribute-based infrastructure for the EHR where the patients encrypt their EHR files using the bABE. This approach solves the key management issues by using the users attribute for data encryption allowing every user to have only one private key for their attribute set for decryption. This approach also allows users to carry and healthcare providers to perform keyword-based searches on the encrypted patients' records without revealing the keywords or partial matches to the cloud system. The keyword search functionality is provided by combining the bABE and the Public-Key Encryption with Keyword Search (PEKS). Ibraimi et al [19] proposed a multi-authority scheme for protecting EHD across different domains. The limitation of the work is that they are not designed for database federations of many medical organisations. Li et al [20] used ABE to manage access control [21] over the health data in multi-owner, multi-authority and multiuser cloud environment. The study was performed in which patients are capable of setting their own preferences, generating the decryption keys using the MA-ABE and distributing keys to the authorized users. The proposed scheme is claimed to be flexible in supporting efficient and on-demand revocation of user access rights and also suffers from excessive computational overhead at the data owner side. To encrypt the patient health record, ABE can be used. The disadvantage is that it is unable to handle the situations where data access rights are granted based on the users' identities instead of the attributes [22]. From this discussion it is succinct that the non-cryptographic approaches can never be truly secure in public clouds because they are susceptible to information disclosure by some insiders or other hackers. This can be applicable only in private clouds to a desired level because the infrastructure in such cases is trusted [6].

Narayan [18]proposed a patient centric cloud based EHR system by incorporating symmetric key cryptography, public key cryptography and an attribute based architecture. This method includes encrypting the patient health data being encrypted by the patient using a symmetric key and also a metadata file which includes description of the file, attribute based access policy, location information encrypted using broadcast CP-ABE and stored in a cloud platform. This method supports direct revocation without re-encryption of data but has a higher computational cost on patient end where all re-encryption and updating of access policies are handled by the patient side [18]. Another downside is that the Trusted Authority can access all the encrypted files. Barua et al [23] used the mechanisms of proxy re-encryption and ABE to develop a more sophisticated cloud based solution. However it does not required external party for key distribution, it leads to a single point of failure and also creates key escrow while managing all attributes with a single authority. In order to resolve the issue Li et al [24] introduced a cloud based health record sharing scheme using both KP-ABE and MA-ABE schemes. This solution exerts some level of computational cost on the user side. Comparison of privacy preserving cryptographic approaches and non-cryptographic approaches is portrayed in Table I and II respectively.

In Table I and II, ✓, ✗ symbols represent whether a particular privacy-preserving requirement is fulfilled or not, and - represents that a particular requirement is not discussed. The Abbreviations such as IN-Integrity, CO - Confidentiality, AU - Authenticity, NR-Nonrepudiation, AC - Accountability , AN - Anonymity, UN - Unlinkability. In EHR systems as most of the data are strictly confidential and stored in a third party cloud, Access control mechanisms are equally ineludible and vital as Encryption techniques. Access control is a fundamental security barrier for data privacy in a healthcare information [13] system which limits who can access and operate the documents in an EHR system. Harsha et al [25] proposed a patient-centric attribute based scheme in which each PHR (personal health record) file is encrypted and stored in a healthcare cloud along with an attribute based access policy which controls the access to encrypted resource and also utilizes a proxy re-encryption scheme to facilitate the authorized users to decrypt the required PHR files. This scheme is resistant against attacks mounted via attribute collusion as well as capable of provisioning on-demand user revocation. Suhair and Rajendra [26] presented a framework which eliminates the limitations of RBAC (Role based access control) and ABAC(Attribute-Based Access Control). This work proposed a BiLayer Access control(BLAC) to integrate attributes with roles in which an access request is checked against pseudoroles before checking the rules within the policy. R.Sandhu et al [27] [28] proposed RBAC [29] in which subjects are assigned to roles and roles are associated with permissions that defines which operations can be performed over which objects. This scheme has several drawbacks of expensive process to define and structure roles, supports only predefined and static policies, cannot support dynamically changing environments [30], and also RBAC's coarse-granularity causes inside attacks [31] . Yuan and Tong [32] proposed ABAC in which each subject's specific attributes are used to define access policies for access permission. ABAC resolves issues of RBAC but it has two problems. First, ABAC is complex due large number of rules that needed to be checked for access decisions and secondly for n attributes ABAC may require $2n$ possible rules [30].

Table 1. Comparison of Privacy Preserving Cryptographic Approaches

Sl No.	Technique(s)	Strength	Weakness	Privacy Requirements							Ref.
				IN	CO	AU	NR	AC	AN	UN	
1	KP-ABE, PRE, Lazy Re-encryption	Scalable access control	Computational overhead at server	✗	✓	-	✗	✓	-	-	[10]
2	bABE. PKE with keyword search	Efficient revocation	Inflexible access control	✗	✓	✗	✓	✗	-	-	[11]
3	ABE	Hides the identities of data storing entities	Cloud is aware of access policy about each record	✗	✗	✓	✗	✓	✓	-	[9]
4	MA-ABE	Scalable access control	Management overhead	✗	✓	✓	✗	✗	✗	✗	[5]
5	SKE	Solves key distribution among multiple users	Difficult to manage multiple user roles	✓	✓	✓	-	✗	-	-	[5]
6	Threshold cryptography	Stored crypto key tables not required	Existence of trusted authority	✗	✓	✗	✓	-	-	-	[5]
7	Broadcast ABE	Direct revocation capability	TA can access all encrypted files	✗	✓	✗	✓	-	-	-	[5]
8	IBE, ABE	Resistant against collusion and eavesdropping	Care provider encrypts the data according to the access tree	✓	✓	✗	✗	-	-	-	[13]
9	MA-ABE, KP-ABE	Flexible access with private and public domains, Eliminate single point of failure	User must obtain one attribute from each authority	✗	✓	✗	✓	-	-	-	[14]

Table 2. Comparison of Privacy Preserving Non-Cryptographic Mechanisms

Sl No.	Technique(s)	Strength	Weakness	Privacy Requirements							Ref.
				IN	CO	AU	NR	AC	AN	UN	
1	RBAC	Simpler access administration	Expensive process to define roles	✗	✗	✗	✗	✗	-	-	[18]
2	ABAC	Dynamic access control policy	Requires large no: of rules	✗	✓	✓	✓	✓	-	-	[22]
3	BLAC	Combines advantages of RBAC and ABAC	Security threats	✗	✓	✓	✓	✓	-	-	[17]
4	Policy based authorization	Selective sharing of health data	Lack of confidentiality	✗	✗	✗	✗	✗	-	-	[5]

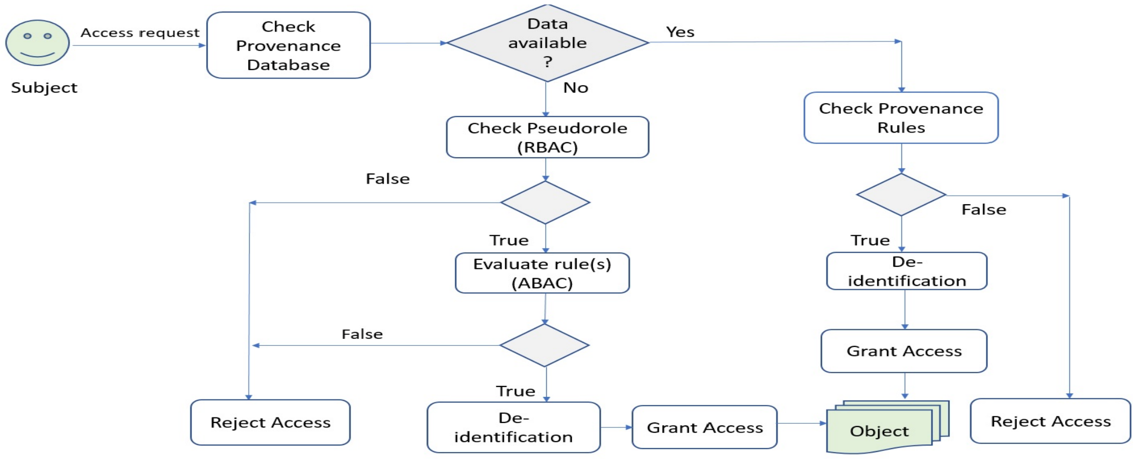


Figure 2. Overview of MLAC Model

4. Methodology and Conceptual Framework

This work proposes a multi-layer access control mechanism, MLAC Model to construct a secure and privacy-preserving EHR system that enables patients to share their data among stakeholders in a cloud environment. This framework proposes a novel access control mechanism for preserving the privacy of EHRs, which incorporates integrity and privacy issues to make access control decisions in the cloud environment.

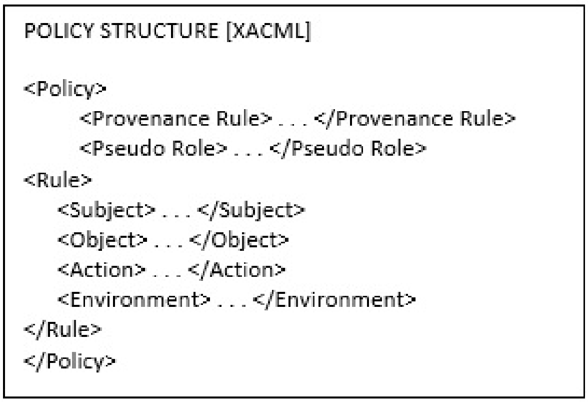
We propose a novel Pseudo-Role Attribute based access control mechanism (PR-ABAC) which is a multi-layer mechanism that combines the advantages of both Role based access control (RBAC) mechanism[24] and Attribute based access control (ABAC) [28]. This multi-layer access control model being proposed integrate attributes with roles combining the advantages of RBAC and ABAC and also uses the concept of provenance thereby aims at assuring two fundamental security properties confidentiality and integrity of the sensitive data in the healthcare domain.

4.1. An overview of MLAC Model

The proposed MLAC model uses the concept of pseudorole, which is defined as a set of static attributes of subjects (users). A pseudorole can be defined as a job function. Subjects' attributes are categorized as static (when attributes values typically do not change) such as Name, ID, Gender, Provider, Department, Location and dynamic (when attribute values change frequently) such as age etc. This model uses static attributes to generate the pseudoroles, and static as well as dynamic attributes are used in policies to constrain pseudoroles. Fig. 2 presents an overview of the PR-ABAC model.

In PR-ABAC, subjects are associated with pseudoroles, which includes a set of static attributes and objects are associated with policies, which specify how attributes are considered for access requests. When an access request is made, the policy associated with the requested object is first checked with the Provenance database to see whether the corresponding data is available to grant access according to Provenance rules and if not, it checks with the (first layer) to see whether the requester has the required pseudorole or not. If so, rules within the policies are then checked for additional fine-grained constraints (second layer) to approve or deny the access request. Initially, the policy will check whether the subject requesting access to an object holds the needed Provenance rules to grant or deny access. Then the policy associated with the requested object checks to see whether the requester has the required pseudorole or not . If so, next each rule is checked to see if the access conforms to the specified values for subject, object, action and environment attributes, otherwise access is denied. This three-step process inspires the name Multi-Layer access control policy which permits fine-grained decisions. This work will demonstrate the applicability of PR-RBAC model to healthcare information sharing environments.

MLAC model is formally described using the tuple: M = (S, O, E, A, PR, P, SPR, OP), Where S is a set of subjects(users) with a predefined set of attributes in which SATT could be provider, department, location etc, O is a set of objects that are accessed by subjects with a set of attributes OATT that could be patient name, medical record number, E is the environment with a predefined set of attributes EATT could be access time, system mode. A is a set of actions with a predefined set of attributes AATT could be read, write, modify etc. PR is a set of pseudoroles that are composed of n attributes that is described in section 4.2. P is a set of policies for fine-grained access control consists of two elements: a Boolean function named Pseudorole, Provenance rule and a set of zero or more rules. A policy structure is shown in Fig. 3, and components of the MLAC model is shown in Fig. 4. SPR is the subject-pseudorole assignment that is a one-to-many mapping from pseudoroles to subjects and OP is the object-policy assignment relation that is a one-to-many mapping from policies to objects. A General Algorithm for the MLAC model is described in Fig. 5.



```
POLICY STRUCTURE [XACML]

<Policy>
        <Provenance Rule> . . . </Provenance Rule>
        <Pseudo Role> . . . </Pseudo Role>
<Rule>
    <Subject> . . . </Subject>
    <Object> . . . </Object>
    <Action> . . . </Action>
    <Environment> . . . </Environment>
</Rule>
</Policy>
```

Figure 3. Policy Structure

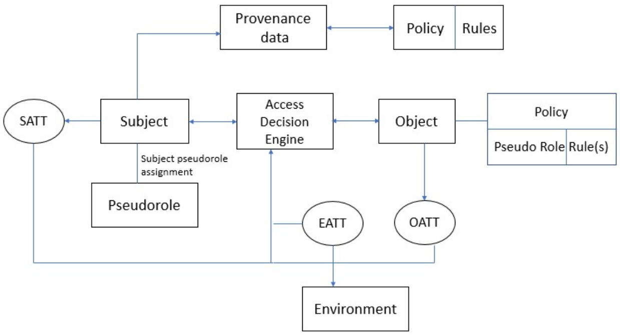


Figure 4. Components of MLAC Model

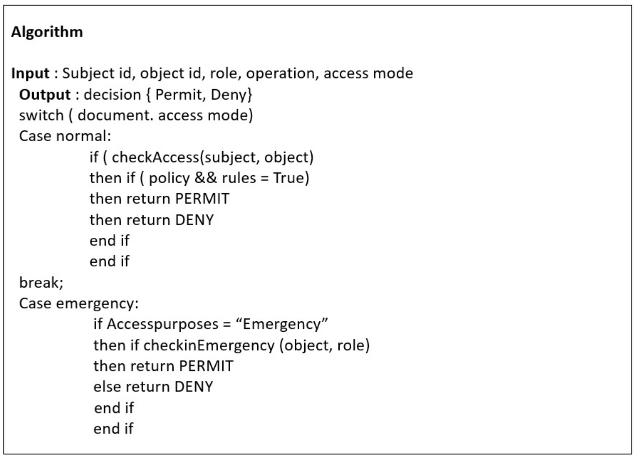
4.2. Algorithm for the Management of Access Control

This algorithm shows the ability of our MLAC model to precisely define the customized policies for the management of Access Control that uses this model. The algorithm shown in Fig. 5 allows or denies access to an object on the basis of the inputs that it receives. The possible inputs are Object identifier (object id) i.e. the identifier of the clinical document in the EHR system, to which access is required, user identifier (subject id) is the identifier of the subject who requires to operate on the object, role indicates the role associated with the user in the EHR system, Operation is the action required on the object and access mode is the mode of access such as normal and emergency mode. The output of the algorithm is PERMIT only if all the access conditions are satisfied.

Each user (clinician) is associated with a private key Sk and a common public key PK associated with the cloud server. The steps are as follows.
●Access Req (AReq): Takes as Input the identity of clinician Cid, the XACML query as the access structure specifying the finer attributes (T), common public key

Table 3. Subject's Attributes

Name	ID	Gender	Provider	Department	Location
E. Robert	345-765	Female	Physician	OB/GYN	A
A. Mark	526-874	Male	Physician	OB/GYN	A
H. John	231-938	Female	Nurse	OB/GYN	A
M. Martin	657-923	Female	Administrative Staff	OB/GYN	B
D. Lee	102-581	Male	Administrative Staff	Billing	B
J. Fox	437-348	Male	Physician	PCP	B



```
Algorithm

Input : Subject id, object id, role, operation, access mode
 Output : decision { Permit, Deny}
 switch ( document. access mode)
 Case normal:
          if ( checkAccess(subject, object)
          then if ( policy && rules = True)
          then return PERMIT
          then return DENY
          end if
          end if
 break;
 Case emergency:
          if Accesspurposes = "Emergency"
          then if checkinEmergency (object, role)
          then return PERMIT
          else return DENY
          end if
          end if
```

Figure 5. Algorithm for Access Control

Pk, Private key Sk of the clinician, which outputs the access request, AReq= Areq(Cid, (T,Pk),Sk)
•Access Response (ARes): Takes as input the access request AReq, the database D, public key of clinician Pk, Access Structure T, Ares= Ares (AReq, D,(Pk,T))
•Response Retrieval (RRet): Takes as input the access response Ares and private key Sk of clinician and outputs associated EHR, R=RRet (Ares,Sk)

4.3. Pseudorole Generation

In PR-ABAC, pseudoroles will be generated from static attributes [33] of subjects. Here we use the values of the attributes associated with all subjects to generate pseudoroles. Table 3 shows the Subjects' Attributes and Fig. 4 shows how corresponding pseudoroles will be generated. Depending on the number of attributes used for generating pseudoroles, a tree based structure is used to identify the number of pseudoroles. If *n* attributes are used to generate pseudoroles, m1 x m2 x m3 x . . . x mn is the total number of generated pseudoroles where mn is the number of total different values for attribute n. However, the meaningful pseudoroles is a subset of these pseudoroles. Example in Table 3 used three attributes (Provider, Department, Location) as static subject attributes that generates 18 distinct pseudoroles as shown in Fig. 6.

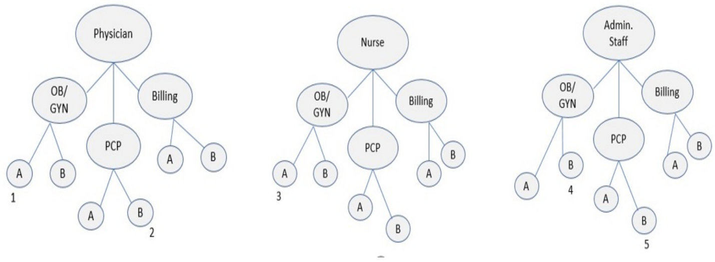
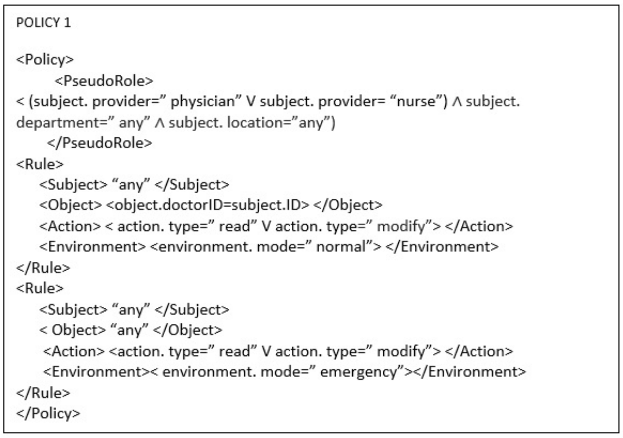


Figure 6. Pseudorole generation in MLAC Model

To preserve the privacy of patient records, a few access control rules are defined in this use case as follow: Health records are split into three sections: (1) demographic, (2) clinical, and (3) billing.

1) Subjects are not allowed to delete records in any section 2) Physicians and nurses are allowed to read and modify records within demographic and clinical sections for patients who are under their responsibility in normal and emergency situations 3) Physicians and nurses are allowed to read and modify records within demographic and clinical sections for non-patients in emergency situations 4) Adminisitrative staff are allowed to grant access to authorized users 5) Billing staff are allowed to read and modify records within billing section



```
POLICY 1

<Policy>
      <PseudoRole>
< (subject. provider=" physician" V subject. provider= "nurse") Λ subject.
department=" any" Λ subject. location="any")
     </PseudoRole>
<Rule>
    <Subject> "any" </Subject>
    <Object> <object.doctorID=subject.ID> </Object>
    <Action> < action. type=" read" V action. type=" modify"> </Action>
    <Environment> <environment. mode=" normal"> </Environment>
</Rule>
<Rule>
    <Subject> "any" </Subject>
    < Object> "any" </Object>
     <Action> <action. type=" read" V action. type=" modify"> </Action>
     <Environment>< environment. mode=" emergency"></Environment>
</Rule>
</Policy>
```

Figure 7. Policy within Clinical Section

The five meaningful pseudoroles used here are(1) Physician OB/GYN A, (2) Physician PCP B, (3) Nurse OB/GYN A, (4) Administrative Staff OB/GYN B (5) Adminsitrative Staff PCP B. we have to define some access control rules according to the requirement of the organisation to preserve the privacy of health records.

4.4. Development of Access Policies

To preserve the privacy of patient records, access control rules are defined. Based on the rules and the structure of health records, some access policies are defined. To enforce the access rules, we can create access policy accordingly such as health records within the clinical section, health record within clinical section associated to psychiatric data with separate access policy, health records within the demographic section are associated with another policy, billing section with another policy and so on according to the requirement of organisation. An example of an access policy within the clinical section is given in Fig. 7.

4.5. Implementation and Evaluation

To demonstrate the feasibility of our approach, we develop a secure EHR sharing system in cloud environment based on our design discussed in figure 6. The core EHRs aggregation and sharing logic will be implemented using ASP.NET framework using C*sharp* programming technologies. This framework is supported with an implementation using extensible access control markup language(XACML) for deploying access control policies. Here we use MySQL server as database server.

A Authentication
Authentication between healthcare providers and EHR sharing cloud is achieved through a PKI (Public Key Infrastructure) managed by EHR cloud application. Each communication between them is signed with sender's private key so that the receiver can verify the signature. Any request from an unregistered party, not participating in the EHR sharing cloud, trying to communicate with a healthcare provider will be rejected.

B Authorization and Access Control
Authorization and Access Control are enforced by giving the requesting healthcare providers access to only the EHR information requested. This work uses RBAC and ABAC access control paradigm for authorization.

C Confidentiality
This framework is planning to use a symmetric key encryption by means of a symmetric key to encrypt and decrypt patients' shared EHR information to preserve confidentiality. The requesting healthcare provider will generate the symmetric key.

D Integrity
Integrity will be achieved by using 'Data Provenance'.

E Privacy Analysis
For the EHR database D, we say that our access control preserves data privacy of each EHR in D is accessible to authorized clinicians only. Our access control protocols and SQL preserve data privacy for the EHR Database D.

4.6. Evaluation

In this work, we are planning to evaluate the performance of our framework in terms of System Time Overhead, Number of Pseudoroles to generate, Number of policies required for efficient electronic health record access, Computational complexity and cost required for the implementation.

5. Conclusion

Data Privacy and Security are facing innumerable challenges nowadays due to recent advances in Information and Communication Technology (ICT) viz Social networking, IoT (Internet of Things), Big Data analytics, Cloud Computing etc. The breach of data in Healthcare is more critical since it compromises the privacy and security of individuals at stake. Hence there is an imminent need to protect the EHR against security breaches by strengthening the security infrastructure in healthcare to ensure the patient confidentiality. This research develops a secure and flexible multi-layer framework based EHR sharing scheme in a cloud environment which satisfies the intended privacy and integrity requirements. To ensure patient centric EHR sharing, it is important to achieve fine-grained access, our scheme uses a multi-layer access control mechanism which facilitates the EHR users to transfer and share the resources effectively. In addition, the proposed scheme introduces the concept of Provenance to ensure Data Integrity.

References

[1] Yi, X., Miao, Y., Bertino, E. and Willemson, J. (2013) Multiparty privacy protection for electronic health records. In *Global Communications Conference (GLOBECOM), 2013 IEEE* (IEEE): 2730–2735.

[2] Kruse, C.S., Mileski, M., Vijaykumar, A.G., Viswanathan, S.V., Suskandla, U. and Chidambaram, Y. (2017) Impact of electronic health records on long-term care facilities: systematic review. *JMIR medical informatics* **5**(3).

[3] Griebel, L., Prokosch, H.U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., Engel, I. *et al.* (2015) A scoping review of cloud computing in healthcare. *BMC medical informatics and decision making* **15**(1): 17.

[4] Li, P., Guo, S., Miyazaki, T., Xie, M., Hu, J. and Zhuang, W. (2016) Privacy-preserving access to big data in the cloud. *IEEE Cloud Computing* **3**(5): 34–42.

[5] Wang, H., Jiang, X. and Kambourakis, G. (2015) Special issue on security, privacy and trust in network-based big data. *Information Sciences: an International Journal* **318**(C): 48–50.

[6] Abbas, A. and Khan, S.U. (2014) 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.

[7] Shu, J., Jia, X., YANG, K. and Wang, H. (2018) Privacy-preserving task recommendation services for crowdsourcing. *IEEE Transactions on Services Computing* .

[8] Ahmed, M. and Ullah, A.S.B. (2017) False data injection attacks in healthcare. In *Australasian Conference on Data Mining* (Springer): 192–202.

[9] AbuKhousa, E., Mohamed, N. and Al-Jaroodi, J. (2012) e-health cloud: opportunities and challenges. *Future internet* **4**(3): 621–645.

[10] Kabir, E., Hu, J., Wang, H. and Zhuo, G. (2018) A novel statistical technique for intrusion detection systems. *Future Generation Computer Systems* **79**: 303–318.

[11] Sun, L., Wang, H., Yong, J. and Wu, G. (2012) Semantic access control for cloud computing based on e-healthcare. In *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (IEEE): 512–518.

[12] Wu, R., Ahn, G.J. and Hu, H. (2012) Secure sharing of electronic health records in clouds. In *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on* (IEEE): 711–718.

[13] Wang, H., Sun, L. and Bertino, E. (2014) Building access control policy model for privacy preserving and testing policy conflicting problems. *Journal of Computer and System Sciences* **80**(8): 1493–1503.

[14] Sahai, A. and Waters, B. (2005) Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer): 457–473.

[15] Cheng, K., Wang, L., Shen, Y., Wang, H., Wang, Y., Jiang, X. and Zhong, H. (2017) Secure k-nn query on encrypted cloud data with multiple keys. *IEEE Transactions on Big Data* .

[16] Yu, S., Wang, C., Ren, K. and Lou, W. (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In *Infocom, 2010 proceedings IEEE* (Ieee): 1–9.

[17] Kabir, E., Mahmood, A., Wang, H. and Mustafa, A. (2015) Microaggregation sorting framework for k-anonymity statistical disclosure control in cloud computing. *IEEE Transactions on Cloud Computing* .

[18] Narayan, S., Gagné, M. and Safavi-Naini, R. (2010) Privacy preserving ehr system using attribute-based infrastructure. In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop* (ACM): 47–52.

[19] Ibraimi, L., Asim, M. and Petković, M. (2009) Secure management of personal health records by applying attribute-based encryption. In *Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on* (IEEE): 71–74.

[20] Li, M., Yu, S., Ren, K. and Lou, W. (2010) Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *International conference on security and privacy in communication systems* (Springer): 89–106.

[21] Wang, H. and Sun, L. (2010) Trust-involved access control in collaborative open social networks. In *2010 Fourth International Conference on Network and System Security* (IEEE): 239–246.

[22] Zhang, Y., Shen, Y., Wang, H., Zhang, Y. and Jiang, X. (2018) On secure wireless communications for service oriented computing. *IEEE Transactions on Services Computing* **11**(2): 318–328.

[23] Barua, M., Lu, R. and Shen, X. (2013) Sps: Secure personal health information sharing with patient-centric access control in cloud computing. In *Global Communications Conference (GLOBECOM), 2013 IEEE* (IEEE): 647–652.

[24] Li, M., Yu, S., Zheng, Y., Ren, K. and Lou, W. (2013) 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.

[25] Pussewalage, H.S.G. and Oleshchuk, V. (2016) A patient-centric attribute based access control scheme for secure sharing of personal health records using cloud computing. In *Collaboration and Internet Computing (CIC), 2016 IEEE 2nd International Conference on* (IEEE): 46–53.

[26] Alshehri, S. and Raj, R.K. (2013) Secure access control for health information sharing systems. In *2013 IEEE International Conference on Healthcare Informatics (ICHI)* (IEEE): 277–286.

[27] Sandhu, R.S., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (1996) Role-based access control models. *Computer* **29**(2): 38–47.

[28] Sandhu, R., Ferraiolo, D., Kuhn, R. *et al.* (2000) The nist model for role-based access control: towards a unified

standard. In *ACM workshop on Role-based access control*, **2000**: 1–11.

[29] Wang, H., Cao, J. and Zhang, Y. (2005) A flexible payment scheme and its role-based access control. *IEEE Transactions on knowledge and Data Engineering* **17**(3): 425–436.

[30] Kuhn, D.R., Coyne, E.J. and Weil, T.R. (2010) Adding attributes to role-based access control. *Computer* **43**(6): 79–81.

[31] Chickowski, E. (2012) Healthcare unable to keep up with insider threats. *Dark Reading (May 2012)* .

[32] Yuan, E. and Tong, J. (2005) Attributed based access control (abac) for web services. In *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on* (IEEE).

[33] Sun, X., Sun, L. and Wang, H. (2011) Extended k-anonymity models against sensitive attribute disclosure. *Computer Communications* **34**(4): 526–535.