Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2019, Vol. 15(6)

DOI: 10.1177/1550147719846050
journals.sagepub.com/home/dsn
SAGE

Privacy-aware relationship semantics–based XACML access control model for electronic health records in hybrid cloud

Tehsin Kanwal[1], Ather Abdul Jabbar[1], Adeel Anjum[1], Saif UR Malik[1,2], Abid Khan[1], Naveed Ahmad[1], Umar Manzoor[3], Muhammad Naeem Shahzad[4] and Muhammad A Balubaid[5]

Abstract

State-of-the-art progress in cloud computing encouraged the healthcare organizations to outsource the management of electronic health records to cloud service providers using hybrid cloud. A hybrid cloud is an infrastructure consisting of a private cloud (managed by the organization) and a public cloud (managed by the cloud service provider). The use of hybrid cloud enables electronic health records to be exchanged between medical institutions and supports multipurpose usage of electronic health records. Along with the benefits, cloud-based electronic health records also raise the problems of security and privacy specifically in terms of electronic health records access. A comprehensive and exploratory analysis of privacy-preserving solutions revealed that most current systems do not support fine-grained access control or consider additional factors such as privacy preservation and relationship semantics. In this article, we investigated the need of a privacy-aware fine-grained access control model for the hybrid cloud. We propose a privacy-aware relationship semantics–based XACML access control model that performs hybrid relationship and attribute-based access control using extensible access control markup language. The proposed approach supports fine-grained relation-based access control with state-of-the-art privacy mechanism named *Anatomy* for enhanced multipurpose electronic health records usage. The proposed (privacy-aware relationship semantics–based XACML access control model) model provides and maintains an efficient privacy versus utility trade-off. We formally verify the proposed model (privacy-aware relationship semantics–based XACML access control model) and implemented to check its effectiveness in terms of privacy-aware electronic health records access and multipurpose utilization. Experimental results show that in the proposed (privacy-aware relationship semantics–based XACML access control model) model, access policies based on relationships and electronic health records anonymization can perform well in terms of access policy response time and space storage.

Keywords

Electronic health records, hybrid cloud, privacy, relationship, access control, cryptography

Date received: 12 October 2018; accepted: 26 March 2019

Handling Editor: Mohsin Raza

Introduction

Recent development in information technology has given a powerful and positive impact toward the improvements in field of medical information. Electronic health records (EHRs) are defined as, "the EHRs means a repository of patient data in digital form, stored and exchanged securely, and accessible by

[1]Department of Computer Sciences, Comsats Institute of Information Technology, Islamabad, Pakistan
[2]Cybernetica AS, Tallinn, Estonia
[3]Department of Computer Science and Technology, University of Hull, Hull, UK
[4]Department of Electrical Engineering, Comsats University Islamabad, Lahore, Pakistan
[5]Department of Industrial Engineering, Faculty of Engineering, King Abdulaziz University, Riyadh, Saudi Arabia

Corresponding author:
Saif UR Malik, Department of Computer Sciences, Comsats Institute of Information Technology, Park Road Chak Shahzad, Islamabad 45550, Pakistan.
Email: saif.rehmanmalik@gmail.com

multiple authorized users."[1] EHRs are increasingly adopted to collect and store various types of patients' data. It includes information about patients' personal details, medical treatments, and laboratory test results. EHRs are generated and maintained,[2] within a healthcare organization (HCO) or community and it is in digital format. EHRs are mainly used by different health professionals and administration staff. Healthcare professionals who use different components of the EHRs are health physicians, nurses, radiologists, pharmacists, laboratory staff, patients, and their dependents. International standards like Health Insurance Portability and Accountability Act (HIPAA) oblige EHRs to provide interoperability to promote information sharing between healthcare institutions and organizations.[3]

The traditional EHR systems work in a centralized database environment where medical information is stored and managed by the hospital itself. This approach is expensive not only in terms of initial system development and maintenance, but such medical information also become incompatible with other healthcare systems.[4] Keeping in mind these inherent issues of traditional EHR system, health organizations are obliged to take the services of cloud service providers (CSPs) to manage the EHRs on their behalf,[5] which has advantages in terms of organizational cost and system scalability as compared to the traditional systems. In cloud deployment models, hybrid cloud is mostly preferred for the HCOs to host their EHR data. Along with the benefits, it creates serious security and privacy issues in terms of EHR access.[2]

Security and privacy issues are imminent while outsourcing personal EHR data to the cloud because of its sensitive nature and "legal and social" repercussions for personal information disclosure. In cloud-based EHRs, on one hand, the patients' information sharing is necessary and beneficial, but on the other hand, it must be performed so immaculately that patients' privacy ought to be preserved. Privacy in cloud-based EHRs is essential as users and data are transparent in the public cloud. Moreover, it is also necessary to give EHR access for improvement in quality of service and EHR data utilization.

Privacy preservation of cloud-based EHR data can be achieved in a straightforward way that is to encrypt the EHR data before transmitting it to the cloud.[2,6,7] Nonetheless, encrypted data processing is not efficient and is limited to certain operations, thereby making it unsuitable for EHR data with multipurpose usage.[8] Most of the cryptographic approaches are computationally expensive, and require complex key management and public key infrastructure (PKI), thereby making them less efficient for the data outsourced to the cloud.[9,10] Attribute-based encryption (ABE) is a prominent scheme that provides a solution to most of above-mentioned problems.[11] ABE is basically a cryptographic access control scheme. Cryptographic access control schemes use cryptography and attribute-based access mechanisms to preserve the privacy of EHRs. However, ABE is computationally expensive and there are also access control policy management issues.[12,13] Even its variant like ciphertext-policy attribute-based encryption (CP-ABE) and key policy attribute-based encryption (KP-ABE) are not sufficient to provide refined access control mechanism, enhanced data utility, and privacy protection in the cloud-based EHRs.

Therefore, an immediate alternative to cryptographic and cryptographic access control–based approaches is a set of these *Privacy-aware anonymity-based techniques*. These privacy techniques are used for protecting persons' private sensitive data when it is publicly released, for example, like generalization, suppression, and Anatomy.[6,14–18] Intel conducted a proof of concept to describe that anonymization technique like generalization and suppression (used in k-anonymity and l-diversity) can be used in cloud computing to achieve anonymity.[19] There are also some partitioning-based techniques[8,20] and differential privacy[21] (to name a few) to the outsourced healthcare data. Zhang et al.[22] a modified MapReduce system is proposed for outsourcing anonymized data to the public cloud while at the same time the sensitive data is stored in the private cloud."Privacy-aware data retrieval system" in the hybrid cloud is also proposed in Zhou et al.[23]

As privacy-aware anonymity-based techniques alone are not sufficient to preserve the privacy, there must be some access control mechanism that can provide fine-grained access control to patient EHRs. Access control is very important for protecting cloud-based EHRs from unauthorized access. However, most recent access control systems for healthcare services are not flexible due to using role-based access control (RBAC) schemes.[24] Moreover, RBAC[25] also fails when the number of potential users is very high and most of users are transparent beforehand. To provide fine-grained access control mechanism to outsource EHRs, we cannot use such access control model like RBAC directly in cloud computing due to lack of scalability and flexibility in attribute management. The diverse access control policies and various access control interfaces can also cause inappropriate interoperability. However, eXtensible Access Control Markup Language (XACML)-ABAC can provide a better solution to most of these access control issues in the cloud.[26–31] There is also another issue of privacy protection of access policies itself. Access control policies in their plain form for cloud-based EHRs create a source of collusion between CSPs and data users; therefore, a mechanism to hide access control policies is also necessary to provide a more robust solution.[32] Access policy anonymization can protect EHR data from being used for malicious

activities for different purposes in healthcare domain. EHRs, when outsourced to the cloud, are vulnerable to more sophisticated attacks. For instance, the data that are outsourced to cloud for multiple users can come under collusion attack, that is, the CSP and data users may collude with each other for various incentives. In these scenarios, a whole data set that is stored in the cloud, along with the privacy mechanism, can be exposed.[8]

Attribute-based access control (ABAC)[33] is the most recent access control mechanism that is used in privacy-preserving solution of cloud-based EHRs.[34,35] However, in almost majority of solutions, major attention is given to provide privacy (using cryptographic and hybrid access control techniques), some limited fine-grained access control solution is provided in these solutions. We have noticed that multipurpose EHR usage and relationship-based access control (Rel BAC) aspect in proposed privacy-preserving solutions need proper and timely attention. In Rel BAC model, access permissions are modeled as relations between users (subjects) and data (objects) while access control rules are the instantiations of relation between specific sets of users and objects. Rel BAC model is represented as an entity relationship (ER) model while permissions are defined as relations between classes of subjects and objects.[36] Moreover as XACML lacks semantic interoperability, the use of semantic-based access control in XACML can simplify the policy specification by incorporating semantic inference in access control process.[37,38]

To provide fine-grained relationship-based EHR access with privacy preservation of EHR data, it is crucial to have an efficient privacy-aware Rel BAC solution. For this purpose, we extend the open and widely accepted XACML standard in relationship semantic access control and privacy preservation context. Our research is mainly about the use of Rel BAC with a privacy-preserving technique Anatomy for enhanced utility. The main purpose of this work is to propose a privacy-preserving access control model (PPX-AC) that will provide privacy-aware fine-grained access control solution that is interoperable and scalable with extended XACML-Rel BAC in the hybrid cloud. Proposed privacy model will provide maximum utilization of patient EHRs to different domain users: original data users (ODU), private data users (P_RDU), and public data users (P_BDU). EHR authorization is given based on their specific domain user permissions in access control policies. The proposed model will provide defense against internal privacy threats with the use of privacy technique Anatomy. Policy anonymization is also used to prevent privacy disclosure and possible collusion attacks in public cloud. Main contributions of our work are given below:

- A research gap in related work is identified and we explore that privacy-preserving (using anonymization techniques and privacy models) and relationship semantics–based access control solutions for cloud-based EHRs are not used to achieve privacy, relationship semantic access control, and EHR data utility.
- A privacy-aware relationship semantics–based XACML access control model (PRSX-AC) for EHRs in hybrid cloud is proposed, and its main features are as follows:
- Provide fine-grained access control for cloud-based EHRs;
- Provide relationship semantics–based access control with XACML that will be semantically interoperable in hybrid cloud;
- Privacy model will use privacy technique Anatomy for EHR anonymization, as it provides high-quality data utilization;
- The proposed solution will provide relationship-based EHR access, and it will also improve information sharing in terms of primary and secondary use of EHRs (medical usage, personal usage, institutional research, data analysis, and information sharing) in the hybrid cloud.
- PRSX-AC model is formally verified, and a prototype that compiles XACML policy to verify its effectiveness is implemented.

In section "Related work," the related work in the cloud-based EHR privacy preservation is given. Section "PRSX-AC" provides description of proposed PRSX-AC, and main design goals of PRSX-AC along with refined conceptual level details and technical description of different components are given. In section "Formal specification, modeling, and verification of PRSX-AC model," we have formally verified the PRSX-AC model properties. Experimental evaluation is given in section "Experimental results and discussion." Finally, section "Conclusion" concludes the whole work.

Related work

There are many approaches that are used to solve security- and privacy-related issues of EHR access in the cloud. In this section, a brief review of the relevant work on privacy preservation techniques of cloud-based EHRs is given. An overview of these privacy-preserving techniques along with the related work in

different cloud deployment models in EHRs will be described.

EHR privacy-preserving techniques and cloud deployment models

This section provides a comprehensive overview and analysis of privacy-preserving techniques used in the cloud-based EHRs. We have categorized the privacy-preserving technique for cloud-based EHRs into *cryptographic techniques, cryptographic hybrid access control techniques*, and *privacy-aware anonymity-based techniques*.

Cryptographic techniques. In these techniques, various cryptographic mechanisms are used for privacy preservation. Some of cryptographic techniques are given here as it will help to understand the privacy-preserving approaches analysis. Symmetric key encryption (SKE) uses the same key for encryption and decryption to secure the data. SKE-based algorithms are currently used as a standard in the Advanced Encryption Standard (AES; standard recommended by NIST). In public key encryption (PKE) technique, we use private and public keys instead of a single key like in SKE. Although, encryption through PKE is secure, it is computationally expensive and not efficient, thus mainly used in combination with the SKE. ABE is another technique that is based on PKE. In ABE, encryption and decryption are performed on user's attributes. ABE allows users to share the specific attribute-based encrypted data and provides fine-grained access.[24,39,40] There are two variants of ABE: CP-ABE and KP-ABE. In ABE, encryption is performed based on access policy. In CP-ABE, user's private key is the set of attributes. CP-ABE usage is limited as it involves specification of access control policies. Management of user's attributes is another issue in CP-ABE.[41] In KP-ABE, access policy is associated with the private key and encrypted text is a set of descriptive user attributes. Decryption is only possible if access policy and user attribute match. There are many variations in cryptographic techniques like multi-authority attribute-based encryption (MA-ABE), searchable encryption, and fully homomorphic encryption (FHE).[42–44]

Cryptographic hybrid access control techniques. Cryptographic hybrid access control–based approaches make use of the combination of various above-mentioned cryptographic techniques with access control mechanisms like RBAC, ABAC, ABE, CP-ABE, and KP-ABE to name a few. In some of hybrid approaches, pseudo-anonymity and statistical data partitioning techniques are combined to get their maximum benefit for the privacy preservation of cloud-based EHRs. Hybrid techniques represent combination of different complex cryptographic, access control, and data partitioning techniques.[2,9,24,34,35,45–52,53–59]

Privacy-aware anonymity-based techniques. Privacy-preserving techniques have different sanitization mechanisms to transform data into anonymized form. Privacy-aware anonymity-based techniques, such as generalization, suppression, Anatomy, Angel, and differential privacy are used to transform microdata to anonymized form. In these privacy techniques, it is also tried to achieve the balance between privacy and data utility. Privacy-preserving techniques are used to prevent identity and sensitive attribute data disclosure when it is publicly released.[12,6,14–18,60] We have tried to give a precise description of privacy-preserving techniques used for EHRs. The above-mentioned privacy-preserving techniques have been used in different cloud deployment models like public, private, and hybrid. Now, we will describe each cloud deployment model and various privacy techniques used to achieve privacy of EHR data.

Public cloud. The cloud deployment model is available to the public users, and it is monitored by the CSP. There can be different EHR recipient's entities, like HCOs, healthcare professionals, and insurance and pharmaceutical companies. The EHRs are stored at the off-premise servers and managed by the CSPs in public cloud.[12,23] Public access to data stored in cloud has made public cloud more vulnerable. There is always high risk for EHR data that malicious activities can be performed by the internal, as well as external, entities. According to security and privacy risks given in Pino and Di Salvo,[61] denial-of-service, man-in-the-middle, eavesdropping, IP-spoofing based flooding, and masquerading are the possible attacks. Consequently, there is strong need of privacy mechanisms to ensure confidentiality of EHRs. Cryptographic techniques and efficient signature verification schemes are already used, but limited work exists to the EHRs' privacy preservation through anonymity-based techniques. Most of the EHRs' privacy preservation work is done at public cloud like *cryptography techniques*[7,32,36,48,49,62–65] and *cryptographic access control hybrid techniques*.[2,9,46,49–51,53,54,56]

Private cloud. Private cloud is managed by the HCOs or a third party, and it may exist on or off the premise of health organization.[12] EHRs stored in the private cloud are considered much secure as compared to the public and hybrid cloud deployment models. Its reason is that EHRs in a private cloud are only accessed by the trusted authority of the HCOs. Some work at the

private cloud for *cryptographic hybrid access control techniques* is given in previous works.[2,55]

Hybrid cloud. Public and private cloud deployment models are combined in hybrid cloud. It is more significant in healthcare scenarios. Healthcare providers that do not have enough infrastructure resources can store the healthcare data in hybrid cloud.[12] Hybrid cloud ensures an efficient and robust solution for future healthcare applications. It effectively uses the maximum advantage of cloud computing and overcome the drawbacks of private and public cloud.[12,66,67] Security and privacy preservation of EHRs are major issues in hybrid clouds, so they need novel solutions in this context. *Privacy-aware anonymity-based techniques* are applied at hybrid cloud[8,38,68] and public cloud.[10] Table 1 presents a comprehensive overview and analysis of privacy-preserving techniques in cloud-based EHRs.

Discussion

We have used the evaluation metrics, namely, relationship-based (RB), data privacy (DP), multipurpose utility (MU), access control (AC), and semantic-based (SB), for evaluation of privacy approaches given in Table 1. We have selected recent studies related to privacy preservation of cloud-based EHRs for comparison. It is clear from Table 1 that cryptographic techniques used in solutions only provide data privacy and all the remaining metrics are not satisfied. Hybrid cryptographic access control approaches are used in majority of the work and shows effectiveness against data privacy, access control, and limited multipurpose utility. These cryptographic hybrid access control approaches fail to provide relationship- and semantic-based features in cloud-based EHRs. Cryptographic hybrid access control solutions use cryptographic and access control mechanisms like RBAC,[25] ABAC,[33] ABE, CP-ABE, and KP-ABE. However, the used techniques have their limitations. RBAC has scalability issue in cloud with increase in number of users and resources. In KP-ABE data owner is not an authority who decides on access control structure, but it is the key distribution center.[9] In CP-ABE, although data owner has a full control over access policy altogether, it also represents a complicated technical solution. It is surely not affordable in all cloud-based EHRs. There are also some privacy-aware anonymity-based solutions[8,10,21,22] that show some potential toward providing an alternative less complicated solution. However, privacy-aware anonymity-based solution alone fails to achieve all other evaluation metrics except data privacy. Data partitioning technique like MapReduce technique is also used, but its emphasis is on data partitioning based on computations, not at providing a privacy-aware defensive solution. There is another direction of semantic-based approaches, these approaches provide semantic access control only and data privacy, and relationship and multipurpose usage are not focused in their solutions. Overall, privacy-preserving solution for cloud-based EHRs lack relationship-based access control with semantic meanings and interoperability. Solutions should also provide data privacy at less computational cost and should support an optimal balance between EHRs' multipurpose utilization. The proposed model differs from existing approaches mainly in terms of evaluation metrics as motioned above. In proposed solution, we have extended XACML authorization architecture that is based on attribute-based access control model (XACML-ABAC).we have innovatively combined relationship-based access control with semantic reasoning and privacy-preserving technique (Anatomy). In addition to satisfying privacy threats, the solution also provides collusion prevention in the public cloud.

PRSX-AC

In this section, first design goals of proposed (PRSX-AC) hybrid cloud model are described. In the next sections, different (PRSX-AC) model phases with detailed logical flow are described. Algorithms of proposed (PRSX-AC) model are also described in detail in last section.

PRSX-AC model: design goals

- Access control: in proposed model, XACML-ABAC provides fine-grained access control; it logically fits to achieve authorization and a flexible policy creation environment in hybrid cloud. When EHR data are outsourced to public cloud, it needs fine-grained access control mechanism to avoid unauthorized EHR access.
- Relationship with semantics: proposed (PRSX-AC) model will provide a novel feature of relationship-based EHR access with semantic reasoning. Relationship-based access and semantics will refine EHR multipurpose usage in hybrid cloud.
- EHR data privacy: EHR data will be anonymized with privacy-preserving techniques Anatomy for its simple and effective mechanism in EHR access and outsourcing scenario. Access policy request will contain requested attributes, and response attributes in their original form will be given. Our solution will provide defense against external threats (policy anonymization) and internal threat as authorized users in public cloud will also get anonymized version of EHR

Table 1. Privacy techniques.

Reference	rivacy techniques	Strength(s)	Limitation(s)	RB	DP	MU	AC	SB
Chase and Chow[42]	Multi-authority attribute-based encryption.	Reduce key management issues, an efficient user revocation	Computational expensive, lack fine-grained access control mechanism.	×	√	×	×	×
Lin et al.[64]	SKE.	Provide integrity, confidentiality, and non-repudiation. Also provide data ownership	Need improved utility, access control list mechanism is not flexible	×	√	×	×	×
Pecarina et al.[69]	Hybrid pseudo-anonymity + ABE, RBAC.	Privacy-preserved data storage and retrieval, improved key management, audit ability, and secure indexing method	Complicated privacy solution, need flexible access control with enhanced usage	×	√	■	■	×
Benaloh et al.[70]	SKE + access control	Provide search ability and access right delegation	Lack of flexibility in privacy-aware access control for EHRs	×	√	×	√	×
Bahga and Madisetti[56]	RBAC + AES-256 + SSO + SSL + MAC	Solution provides interoperability, scalability, portability, and reduced cost	Limited to scalable and interoperable access control	×	√	■	■	■
Li et al.[46]	Symmetric Key Encryption (SKE) + digital signatures.	Unlink ability through identity seed (SID), preserve EMR integrity through digital signature	Access control is not provided simple login password used.	×	√	×	×	×
Hsieh and Chen[34]	ABAC (XACML) + XML security	Providing flexible PHR access control, confidentiality, integrity, and privacy-aware key word search	Lack of refined design of proposed model and prototype implementation	×	√	×	√	×
Narayan et al.[49]	Attribute-based encryption + public-key encryption	Provide confidentiality of data, cloud server will not be able to learn contents from ciphertext and keyword searches	ABE is expensive when number of attributes increases, key management issues need PKI	×	√	×	×	×
Premarathne et al.[57]	RBAC + PKI	Solution provides access control for big EHR data sharing and storage through context and location awareness	Key exchange problem between various parties	×	√	■	√	×
Alshehrsi et al.[50]	CP-ABE–based access control + IBE	Secure scheme for the cloud storage, provide secure communication using IBE	Not efficient for health data with large number of attributes	×	√	×	■	×
Yang et al.[58]	ABAC + time-domain ABE	Providing flexible access control, user's attributes change dynamically	Restricted solution to video data sharing, lack of implementation system	×	√	×	√	×
Takabi[9]	Symmetric Key Encryption (SKE) + commutative encryption–based access control	No need of key distribution mechanism, access control policies change does not cause re encryption, data owner can introduce improved access control policies.	Lack of scalable infrastructure for access policy enforcement, need protection against malicious users in cloud	√	√	×	■	×
Gope and Amin[59]	RBAC + MAC	Solution provide multilevel data flow reference model, it is practical and robust	Inflexible access control	×	■	×	√	×
Alshehrsi et al.[35]	ABAC + ECC + CP-ABE	Provide high performance with time and storage overhead	Lack of non-repudiation, not a practical solution for health data privacy	×	√	×	√	×

(continued)

Table 1. Continued

Reference	rivacy techniques	Strength(s)	Limitation(s)	RB	DP	MU	AC	SB
Xu et al.[31]	Cryptographic + pseudo-anonymity + certificate authority.	Provide patients privacy for general use and secondary use of EHRs, pseudonym scheme uses secret key (MSK) to preserve sensitive information.	Solution is expensive with use of certificate authority for patient's privacy, EHR data linkage privacy attacks are possible.	×	√	■	×	×
Hilia et al.[71]	Semantic approach + XACML architecture	XACML-based access control, semantic-based access decision of heterogeneous resources.	No privacy mechanism used, Increase chances of collusion between CSP and malicious users	×	×	■	√	√
Yang et al.[2]	Statistical analysis, cryptography-based approach.	Provides multiple approaches in vertical data partitioning according to data recipient need. Integrity checks linking, hybrid search facility to EMR recipients.	Solution is expensive in EMR data context, data partitioning techniques can be replaced with privacy techniques	×	√	√	×	×
Joshi et al.[72]	Bell-La Padula rule-based access + semantic web + ORAM encryption techniques	Semantically rich access control, provide documents confidentiality, preserve user identity, document identity	Not interoperable access solution, lack of implementation system	×	■	×	■	√
Mohandas[10]	CP-ABE, k-anonymity	A better hybrid approach, less complicated hybrid solution, provide defense against patient's identity disclosure	CP-ABE is not suitable for high-dimensional data, policies in plain form are vulnerable in public cloud	×	√	×	■	×
Wang et al.[8]	Personalized privacy + differential privacy	Suitable for high-dimensional healthcare data, use personal privacy specific technique for privacy collusion resistant solution	Healthcare data utility is affected with differential privacy, no access control mechanism, it provides the source of collusion in public cloud	×	√	■	×	×
Shrivastva et al.[21]	MapReduce data partitioning	MapReduce technique is used to split data computation, data split is based on security levels	Focus is at the automatic division of tasks by data partitioning not privacy	×	×	√	×	×
Zhang et al.[22]	MapReduce data partitioning	Provide automatic data partitioning, efficient data retrieval through separate storage of sensitive and insensitive data at private and public cloud.	Restricted solution for multipurpose usage of stored data in public cloud, need an efficient privacy-preserving mechanism	×	×	√	×	×

DP: data privacy; MU: multipurpose utility; AC: access control; SB: semantic-based; RB: relation-based; EHR: electronic health record; ABE: attribute-based encryption; RBAC: role-based access control; ABAC: attribute-based access control; PKI: public key infrastructure; CP-ABE: ciphertext-policyattribute-based encryption; CSP: cloud service provider; EMR: electronic medical record; PHR: personal health record; ECC: elliptical curve cryptography; MSK: multi authority symmetric key.
Symbols used for security and privacy metrics; √: Satisfied, ×: Not satisfied, ■ : Limited.

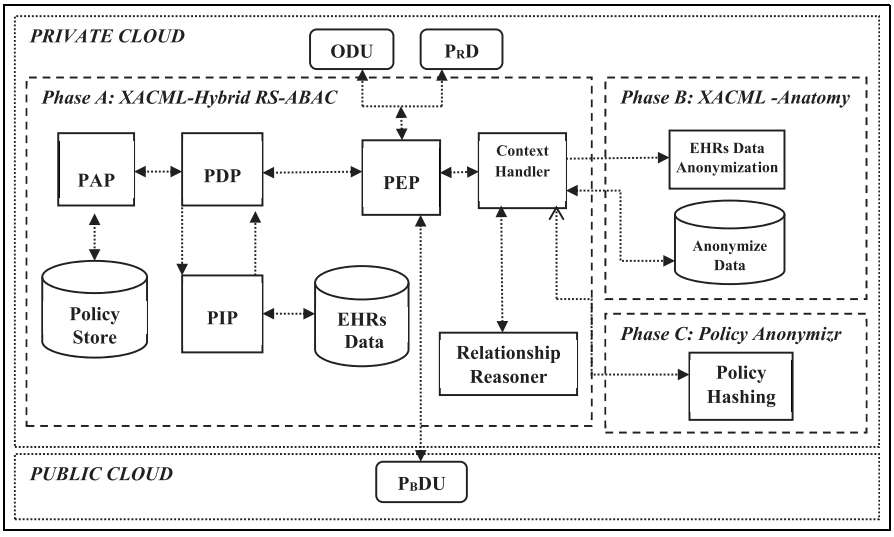

Figure 1. Block diagram of PRSX-AC hybrid cloud model.

data, not original data. Privacy technique Anatomy preserves EHRs' sensitive information on disclosure and provides maximum EHR utility in cloud-based EHRs.

- EHR multipurpose usage: as most of the cryptographic access control solutions are too expensive and complicated, that entity in healthcare domain cannot afford EHR sharing to the public cloud. EHR data owners are also reluctant to share at public cloud due to external threats. Proposed (PRSX-AC) model will provide efficient and improved EHR usage in terms of primary and secondary use with additional relationship-aware access.

PRSX-AC models: description and phase details

A relationship-aware privacy-based access model (PRSX-AC) for EHRs with fine-grained access control mechanism is given in detail in this section. In our proposed privacy model (PRSX-AC), we assume that the EHR data user is authentic, and due to our two levels of privacy preservation, integrity of EHRs is not compromised. Proposed privacy model is an extension of standard XACML- ABAC[33,73] with semantic Rel BAC hybrid approach and EHR privacy mechanism. Moreover, proposed model will also provide protection of access policy during transmission from public to private cloud. The proposed model (PRSX-AC) operates in three main phases as follows:

- Phase A: *XACML-hybrid RS-ABAC*;
- Phase B: *XACML-EHR anonymization*;
- Phase C: *XACML-policy anonymization*.

In our proposed (PRSX-AC) model, we have divided EHR data users into three levels of domain users: ODU (hospitals, health professionals, family, and patients), P_RDU (friend, relatives, and colleagues), and P_BDU (medical research and institutions, pharmaceutical companies, and public users). We present the PRSX-AC model information flow with our proposed extension in hybrid cloud in Figure 1; however, we will briefly explain each phase in next sections. It is important to note that all three phases of proposed model are performed at private cloud. Its benefit is that HCOs can be relieved from all infrastructure and storage operations due to performing all such operations at private cloud. Another benefit is that the public cloud vulnerability becomes reduced due to this processing shift.

First, HCO uploads Original EHR data to the private cloud. Domain users (ODU, P_RDU, P_BDU) send EHR access request to policy enforcement point (PEP). The PEP sends the access request to the context handler. Context handler converts it into an XACML request context and sends it to the policy decision point (PDP). The PDP requests subject or resource attributes (EHRs) from the context handler. The context handler requests the remaining missing attributes from a policy information point (PIP). The PIP obtains the requested attributes from EHR data. The PIP returns the requested subject/resource attributes to the context handler. (a) If access request is from ODU, the context handler sends the request to PDP, it evaluates the access policy and access response is given to PEP; then, it sends response to ODU users. (b) For P_RDU access request, the context handler sends the request to relationship reasoner to get semantics of relationship; once obtained, relationship semantics are given to context

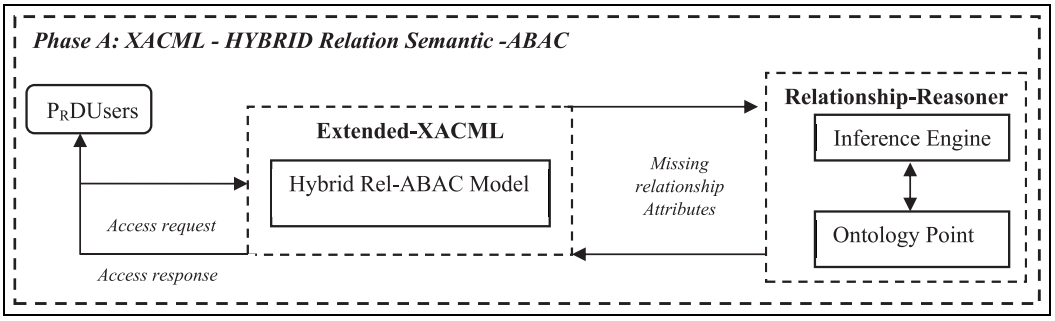

Figure 2. XACML-hybrid RelS-ABAC policy evaluation with relationship-based semantics.

handler, and it sends access request to Phase 2 for EHR attribute anonymization; after receiving response from Phase 2, context handler forwards it to the PDP through PEP. The PDP evaluates the access policy, and access response is given to PEP; then, it sends access response to P_RDU users. (c) For P_BDU, policy access request is given to context handler and it further sends access request to Phase 2 and receives the response from it. Next, context handler sends access policy with anonymized response to Phase 3, where access policy is anonymized with hashing. Phase 3 returns response to context handler and it follows same steps as given above in (Phase 2) and access response is given to P_RDU users.

Phase A: XACML-Hybrid RS-ABAC. We have extended XACML-attribute-based access control model[33,73] in relationships and semantic context in *XACML-Hybrid RelS-ABAC*. In proposed model, we are using Rel BAC model[36] concept in EHR access scenarios. In our proposed (PRSX-AC) model, we have used hybrid relationship semantics–based and ABAC model for access control decisions of all requests that come from EHR users. Access requests from ODU and P_BDU will get access response from XACML-ABAC in hybrid model. However, access request from P_RD users will be processed by relationship semantics–based approach in proposed model. In this category, different patient relationships are introduced as shown in Figure 3(a). Patient relationship access request will not be interpreted with their semantic meaning in XACML. For this purpose, we have used relationship reasoner in PRSX-AC model. When P_RD users request EHRs, then it is forwarded to hybrid Rel ABAC model in extended XACML. Next, missing relation attributes are requested to relationship reasoner, and Ontology Point contains ontology for various relationships. As given in Giunchiglia et al.,[36]"An ontology is capable of describing concepts, e.g. persons, which exist in a certain domain and relationships among them." Ontologies are described in the Semantic Web in Web Ontology Language (OWL). The process of drawing conclusions and new information gain through ontology's takes place through inference engines. Simple inferences can be made with Resource Description Framework Schema (RDFS) and OWL, for instance, through inheritance; however, complex custom inference rules require some special rule language like Semantic Web Rule Language (SWRL). In our proposed model, the inference engine performs relationship reasoning based on logical inferences rules. Extended XACML decides about the access response and gives it to P_RDU. The process of XACML policy evaluation with relationship semantics is given in Figure 2.

We have assumed Subject, Object, and Permission hierarchies in our proposed EHR access approach. For this purpose, we present a mapping of subject-to-patient relationships, object-to-EHR data, and permissions-to-EHR permissions and present their hierarchies. For access control decisions, we are using the Rel BAC logic, which allows us to express and reason about patient relationships with objects (EHR data) to form permissions and rules. We are presenting a short description of how we can use it to express more expressive relationship-based access control policies for EHR access scenarios. We have sets of users and objects formalized as atomic concepts. Permissions are formalized as description logics (DL) roles (not to be confused with the RBAC roles)

$$Ui, \ldots, Un|(Users) \in Ui(i = 1, \ldots, n)$$
$$Oj, \ldots, Um|(Objects) \in Oj(j = 1, \ldots, m)$$
$$Pk, \ldots, Px|(Permissions) \in Pk(k = 1, \ldots, x)$$

where $Ui(i = 1, \ldots, n)$ are concepts for users, such as Relatives or Friends; $Oj(j = 1, \ldots, m)$ are concepts for objects, such as Original EHRs or Anonymized EHRs; $Pk(k = 1, \ldots, x)$ are roles for permissions defining user-object pairs. Examples of permissions are EHR-based operations such as Read, Write, and Modify under Special permission, Emergency permission, and Selective permission hierarchies. Similarly, Subject and Object hierarchies are given in Figure 3. In Rel BAC, we declare hierarchies as $Ai \sqsubseteq Ak$ where Ai and Ak can

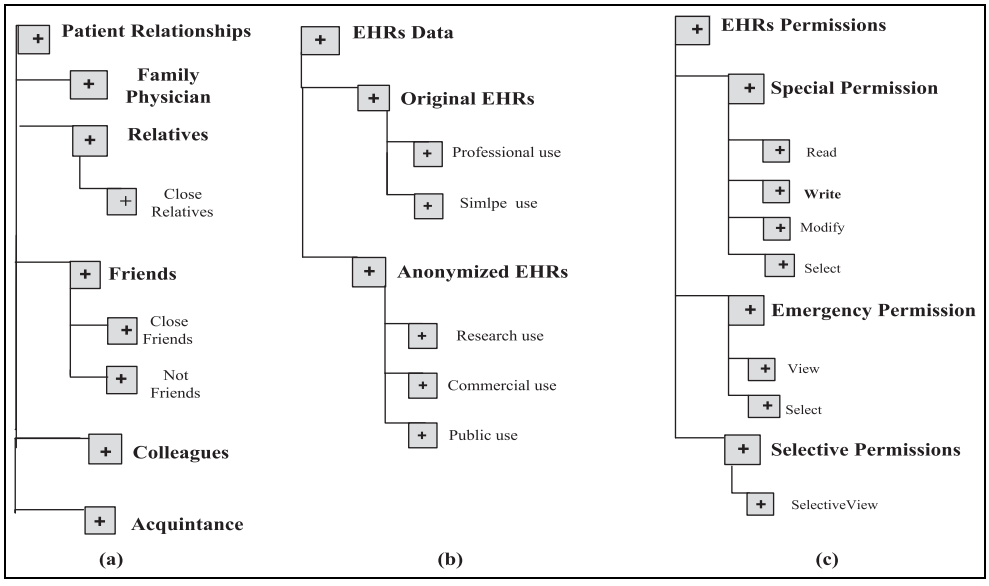

Figure 3. (a) Subject (patient relationship), (b) object (EHR data), and (c) permission (EHR permissions) hierarchies.

Table 2. RelS-BAC rules and description.

Rule	Description	Rule	Description
$\boldsymbol{U_i}, \boldsymbol{U_j}$	Atomic concepts for user or object	$\forall Pr_k.C$	Value restriction
$\boldsymbol{P_k}$	Atomic permission	$\exists Pr_k.T$	Number restriction
T	Universal concept	$\geqslant Pr_k.C$	Negation of arbitrary complex concept
$\perp$	Empty concept	$\leqslant Pr_k.C$	Negation of permission
$\neg \boldsymbol{O_i}, \neg \boldsymbol{O_j}$	Atomic negation	$\neg C$	Inversion of permission
$\boldsymbol{A} \sqcap \boldsymbol{B}$	Conjunction	$\neg P_k$	limited existential quantification
$\boldsymbol{A} \sqcup \boldsymbol{B}$	Disjunction	P_k^{-1}	Full existential quantification

Table 3. RelS-BAC: EHR policy rules and representation.

Subsumption formulas	Policy rules	Representation
$\boldsymbol{U} \sqsubseteq \forall \boldsymbol{P}.\boldsymbol{O}$	Family Physician can Modify patients Original EHRs.	Family Physician $\sqsubseteq \exists$ *Read*. Professional use
$\boldsymbol{U} \sqsubseteq \exists \boldsymbol{P}.\boldsymbol{O}$	Close relatives can Read some of Original EHRs.	Close Relatives $\sqsubseteq \exists$ *Read*. Simple use
$\boldsymbol{O} \sqsubseteq \exists \boldsymbol{P}^{-1}.\boldsymbol{U}$	Some Acquaintance can selectively view Anonymized EHR for public use.	Anonymized EHRs $\sqsubseteq \forall selectiveview^{-1}$. Acquaintance
$\boldsymbol{U} \sqsubseteq \forall \boldsymbol{P}.\boldsymbol{O}$	All colleagues of patients are allowed to selectively view the public use of Anonymized EHRs.	Colleagues $\sqsubseteq \forall$Slective view.Public use
$\boldsymbol{O} \sqsubseteq \exists \boldsymbol{P}^{-1}.\boldsymbol{U}$	Simple view of Original EHRs can be selected by Close friend.	Simple Use $\sqsubseteq \forall select^{-1}$. Close Friend
$\boldsymbol{U} \sqsubseteq \geqslant \boldsymbol{nP}.\boldsymbol{O}$	Each colleague can select at least once the simple use of Original EHRs.	Colleagues $\sqsubseteq \geqslant 1 Select.Simpleuse$
$\boldsymbol{O} \sqsubseteq \leqslant \boldsymbol{nP}.\boldsymbol{U}$	Professional use of Original EHRs can be modified by Family Physician at least three times.	Professional Use $\sqsubseteq \leqslant 3 Modify$. Family Physician
$\boldsymbol{U} \sqsubseteq \boldsymbol{P}.\boldsymbol{o}$	Not friends can view Selective view of Anonymized EHRs.	Not Friend $\sqsubseteq$ View: Selective view

EHR: electronic health record.

be users, objects, or permissions. We can represent some paths in hierarchies in Figure 3, in axiomatic forms as follows: Family Physician $\sqsubseteq$ Patient Relationships, Anonymized EHRs $\sqsubseteq$ EHR Data, and Modify $\sqsubseteq$ Special Permission. Rules usually take the form of subsumption formulas. Rel BAC formation rules are given in Table 2. These rules are used in subsumption formulas. Table 3 presents policy rules and their representation in EHR access scenarios according to the corresponding subsumption formulas.

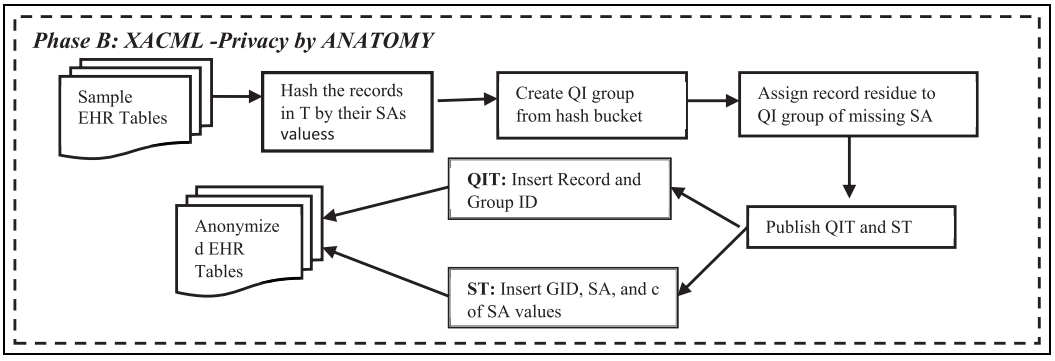

Figure 4. The process of EHR anonymization in XACML-privacy by Anatomy.

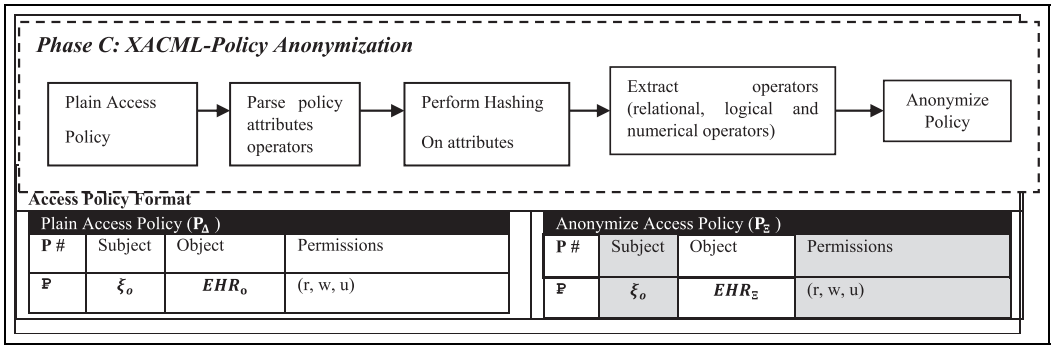

Figure 5. The process of access policy anonymization with hashing and policy format.

Phase B: XACML-EHR anonymization. The privacy technique Anatomy is developed to overcome the defects of generalization and to achieve better utility in data publishing. Anatomy[14] produces two tables: A *Quasi Attribute Table* (QAT) and a *Sensitive Attribute Table* (SAT); the two tables separates QI-values from sensitive values. Anatomy does not modify the quasi-identifier or the sensitive attribute, but it separately releases QAT and SAT to disassociate the relationship between the two tables. The QAT contains the quasi attributes, SAT contains the sensitive attributes, and both QAT and SAT have one common attribute Group-ID. All records in the same group will have the same value of Group-ID in both tables so that it will help in linking the sensitive attribute values in the group. Every group must have distinct sensitive attribute values and each distinct sensitive value occurs exactly once in the group. In generalization, quasi attribute values are generalized, whereas in Anatomy, QAT values are in original form; therefore, the Anatomy is considered a better approach then the generalization. Figure 4 shows the process of EHR anonymization performed with privacy technique Anatomy. The anatomization process that we perform on EHR data tables is described in Algorithm 2 with complete details in next section.

Phase C: XACML-policy anonymization. After EHR data anonymization, policy anonymization is performed in PRSX-AC model. Although EHR data at public cloud will be in anonymized form, transmission access policy without anonymization will provide a source of collusion between CSP and unauthorized malicious entity. In this case after anonymization, CSP and unauthorized data user at public cloud will not be able to gain information that can be used for malicious purposes. In proposed model, policy anonymization is performed with MD5 hash function. First, access policy is parsed to extract logical, relational operators; then, the remaining attributes are anonymized using hashing algorithm. Figure 5 shows the process of access policy anonymization and policy format before and after policy anonymization.

PRSX-AC model: access control and anonymization algorithms

In this section, we will define three (PRSX-AC) model-based algorithms with their complete details. PRSX-AC model includes privacy-aware relation-based access control (PR-AC) algorithm, XACML anonymization algorithm, and XACML-policy anonymization

Algorithm 1: PR-AC Algorithm

Input: EHR_o, ξ
$\xi = \{\xi_o, \xi_{pr}, \xi_{pb}\}$
Output: EHR_o, EHR_Ξ, P_Ξ
Procedure: Privacy_ Access (ξ, EHR_o)

► Lines 1 − 9 shows (EHR_o) storage and XACML access request processing
1. Private Cloud ← Outsourc(EHR_o) ► EHR_o outsourced to private cloud
2. PEP ← Access − Reqst(ξ) ► ξ_o/ξ_P request is given to policy enforcement point
3. CntxtHndlr ← PEP ► PEP forwards request to context handler
4. PDP ← CntxtHndlr ► Context handler sends XACML context request to the PDP
5. Cntx Hndlr ← ReqstATB(PDP) ► PDP requests subject or resource attributes from the context handler
6. O − EHR_o ← Private Cloud ► Lines 6 − 8 shows that EHR_o is given to context Handler through PIP
7. PIP ← O − EHR_o
8. CntxtHndlr ← PIP ► PIP returns the requested subject/resource attributes to the context handler
9. PDP ← Cntxt − Hndlr ► Context handler sends the requested attributes to the PDP
10. **if**($\xi \in \xi_o$)**then** ► Lines 10 − 13 shows access request response of original entity ξ_o
11. O − Acs Resp ← PEP
12. ξ_o ← GrantAcs(O − Acs Resp)
13. **endif**
14. **if**($\xi \epsilon \xi_{pr}$)**then** ► Lines 15 − 25 shows access request response of private entity ξ_{pr}
15. Cntxt Hndlr ← **Rel** − **Reasoner**(ξ_{pr})
16. **Procedure:** Rel-Reasoner (ξ_{pr}) ► Procedure Rel-Reasoner return semantic meaning of ξ_{pr}
17. Ontology-point (ξ_{pr}) = Ont − op
18. ξ_{pr}Rel ← Infer − Engin(Ont − op)
19. **return** ξ_{pr}Rel
20. PIP ← Cntxt − Hndlr
21. Pr − EHR_Ξ ← **XACML** − **Anatomy**(O − EHR_o) ► EHR_o anonymization process
22. PEP ← Pr − EHR_Ξ
23. Pr − Acs Resp ← PEP
24. ξ_{pr} ← GrantAcs(Pr − Acs Resp)
25. **endif**
26. **if**($\xi \in \xi_{pb}$)**then** ► Lines 27 − 35 shows access request response of public entity ξ_{pb}
27. Pb − EHR_Ξ ← **XACML** − **Anatomy**(O − EHR_o) ► EHR_o anonymization process
28. Pb − EHR_Ξ ← PEP
29. P_Δ ← Cntxt − Hndlr
30. Cntxt − Hndlr ← **XACML** − **PolicyAnonymizr**(P_Δ) ► Policy anonymization process
31. P_Ξ ← Cntxt − Hndlr
32. Public Clod ← Send(Pb − EHR_Ξ, P_Ξ) ► EHR_Ξ and P_Ξ is stored in the public cloud
33. P b − Acs Resp ← Public Clod ► Public cloud sends an EHR_Ξ data and P_Ξ to Pb -Acs Resp
34. ξ_{pb} ← GrantAcs(Pb − AcsResp) ► Pb − AcsResp is given to ξ_{pb}
35. **endif**
36. **return** EHR_o, $EHR_{\Xi,,P_\Xi}$ ► returns original EHR_o, anonymized EHR_Ξ and anonymized policy P_Ξ
37. **End**

algorithm. We will present formal specification and modeling of the algorithmic details in the next section.

In Algorithm 1, first, Original EHR outsourcing from HCO to the private cloud is performed. EHR original entities (ξ) send access request to PEP. The PEP sends the access request to the context handler. Context handler converts it into an XACML request context and sends it to the PDP. The PDP requests subject or resource attributes from the context handler. The context handler requests the remaining missing attributes from a PIP. The PIP obtains the requested attributes from EHR data. The PIP returns the requested subject/resource attributes to the context handler. The context handler sends the requested subject/resource attributes to the PDP. Then, it evaluates the access policy if access request is from ξ_o and then response is given to PEP, which sends EHR_o−based access response to ξ_o. If access request is from ξ_{pr}, it is forwarded to procedure Rel-Reasoner() and output is given to PIP. The Original EHR_o anonymization process is performed with XACML − Anatomy procedure; after that, access response is given to the ξ_{pr}. If access

request is from ξ_{pb}; then, EHR_o anonymization takes place as given above and response is given to PIP. After this, plain access policy P_Δ is taken from context handler and is anonymized with procedure XACML – PolicyAnonymizer(), anonymized policy is stored in P_Ξ. The Anonymized EHR data $Pb - EHR_\Xi$ and policy P_Ξ are stored in public cloud. From public cloud, access response is given to ξ_{pb} through procedure GrantAcs(). The algorithm returns Original EHR_o, Anonymized EHR data EHR_Ξ, and anonymized policy P_Ξ.

In Algorithm 2, given an EHR data table ET and a parameter l, we obtain a pair of tables QAT and SAT for publication. First, an l-diverse partition of ET is computed, and then, the QAT and SAT from the l-diverse partitions are produced. After that, it hashes the tuples of ET into hash buckets by their sensitive values S_V so that each bucket includes the tuples with the same S_V value. The *QI-group-creation* step is performed in iterations and continues as long as there are at least l non-empty hash buckets. In new QI-group Q_{Gc}, first, algorithm obtains a set S_l consisting of the l hash buckets that *currently* have the largest number of tuples. Then, from each hash bucket in S_l, a random tuple is selected and added. Therefore, Q_{Gc} contains l tuples with distinct S_V values. Next step is *Tuple-residue-assignment*, which is performed for each residue tuple t. Algorithm collects a set S_O of QI-groups (produced from the previous step), where no tuple has the same S_V value. Then, at last, anonymized QAT and SAT tables are published.

XACML-policy anonymization algorithm, given with plain access policy PΔ, anonymizes policy Pá with hashing method. First, access policy PΔ attributes are checked if attributes are not in S_{OP}. After that only, non-S_{OP} attributes are given to hash function for anonymization.

Formal specification, modeling, and verification of PRSX-AC model

In this section, we tried to minimize the level of abstraction through detailed modeling and formal analysis of the proposed PRSX-AC model. We have used high-level Petri nets (HLPN) and Z language for the modeling and analysis of the proposed model. In Malik et al.,[74] it is given that we can use HLPN for two reasons: (a) to simulate the proposed systems and (b) to provide the mathematical representation, so that we can analyze the behavior and structural properties of the proposed model. We can summarize the benefits of presenting formal model and analysis of the proposed systems as (a) the interconnection of the model components and processes, (b) the fine-grained details of the flow of information among various processes, and (c) how the information processing takes place. The verification of proposed model is performed using SMT; for this purpose, the Petri net models are first converted into SMT with the specified properties. After that, Z3 solver is used to check either the model satisfies the required properties or not. In this study, we use HLPN to

Algorithm 2: XACML-EHR anonymization (MT, l)
Input: MT
Output: QAT, SAT

```
1. QAT = ϕ; SAT = ϕ; Gc = 0
2. hash the tuples in MT by their sensitive values SV (each bucket per SV)
3. HB = the hash bucket per SV values
4. while there are at least l non-empty HB                ► Lines 4-9 are the QI -group-creation step
5.     Gc = Gc + 1; QGc = ϕ;                                  ► Lines 5-9 form a new QI-group
6.     Sl = the set of l largest buckets
7.     for each bucket in Sl
8.        remove an arbitrary tuple t from the HB
9.        QGc = QGc U {t}
10. for each non-empty HB                                 ► Lines -13 are the Tuple -residue tuple assignment step
11.    t = the only remaining tuple of the HB
12.    S0 = the set of QI-groups that do not contain the SV value t[d + 1]
13.    assign t to a random QI-group in S0
14. for j = 1 to Gc                                       ► Lines 14-20 populate QAT and SAT
15.    for each tuple t ϵ Qj
16.       insert tuple (t(1), …, t(d), j) into QAT
17.    for each distinct SV value v in Qj
18.       cj(s) = the number of tuples in Qj with SV values
19.       insert record (j, s, cj(s)) into SAT
20. return QAT and SAT
```

Algorithm 3: XACML-policy anonymization
Input: Plain Access Policy PΔ
Output: Anonymize Policy P⋈

1. S_{OP} = {relational operator, logical operator, numeric values}
2. **for** each access policy P Δ **do**
3. **if** (Atbs $\notin S_{OP}$) **then**
4. Atbs = Hash(Atbs)
5. **end if**
7. **end for**
8. **return** P⋈

perform formal specification and modeling of proposed algorithms. HLPN *is a set of 7-tuple, N = (P, T, F, φ, R, L, M0)*:

1. P is a set of finite places;
2. T represents a set of finite transitions, such that $(P \cap T = \Phi)$;
3. F denotes the flow relation from place to transition or transition to place, such that $F \subseteq (P \times T) \cup (T \times P)$;
4. φ represents the mapping function that maps places to data types, such that $\varphi : P \rightarrow Data\ Types$;
5. R represents the set of rules that maps T to logical formulas, such that $R : T \rightarrow Formula$;
6. L denotes the labels that are mapped on each flow in F, such that $L : F \rightarrow Label$;
7. $M0$ represents the initial state where the flow can be initiated, such that $M : P \rightarrow Token$.[74]

To represent a system in HLPN, we first define a set of P (Places) and the associated data types; after that, we define set of rules involved in HLPN. Figure 6

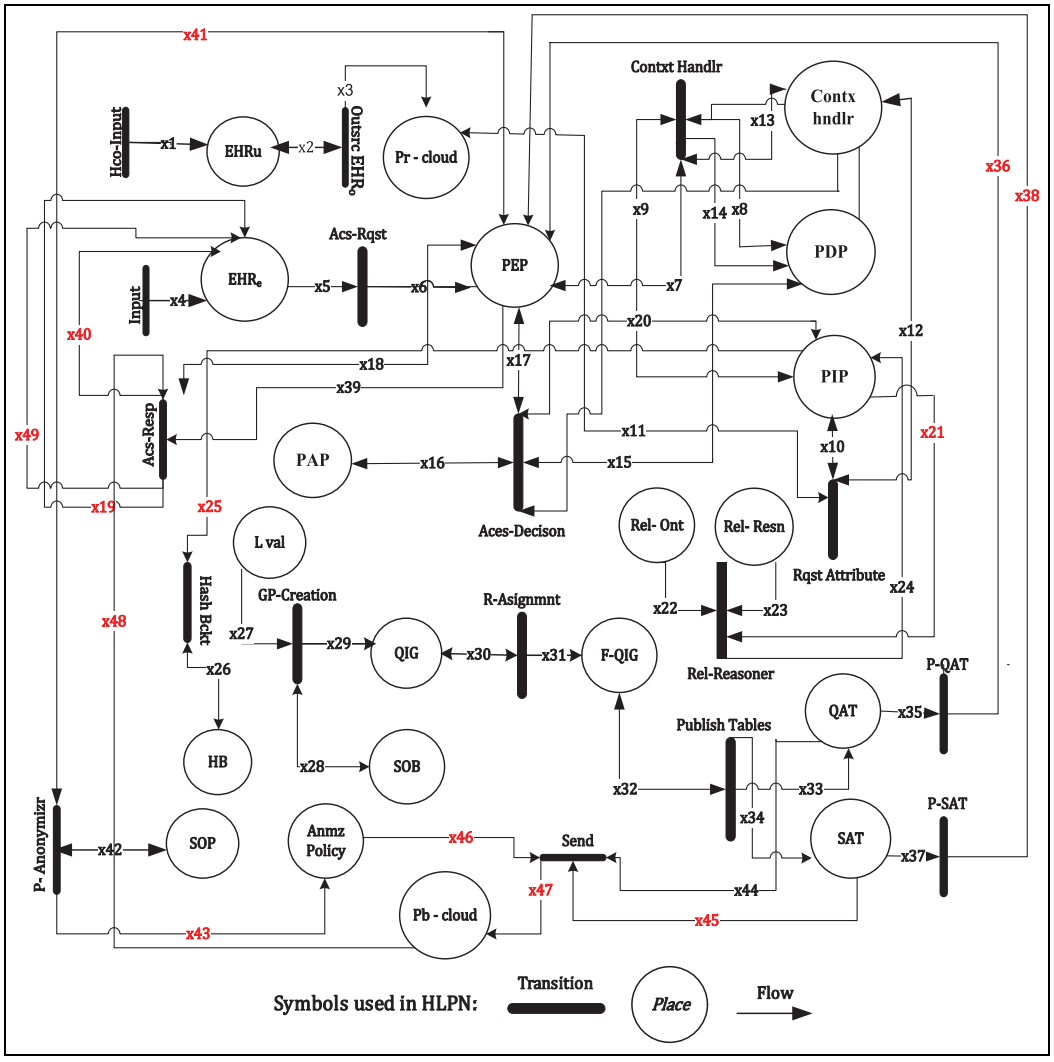

Figure 6. HLPN for privacy aware relationship semantics-based XACML access control model (PRSX-AC).

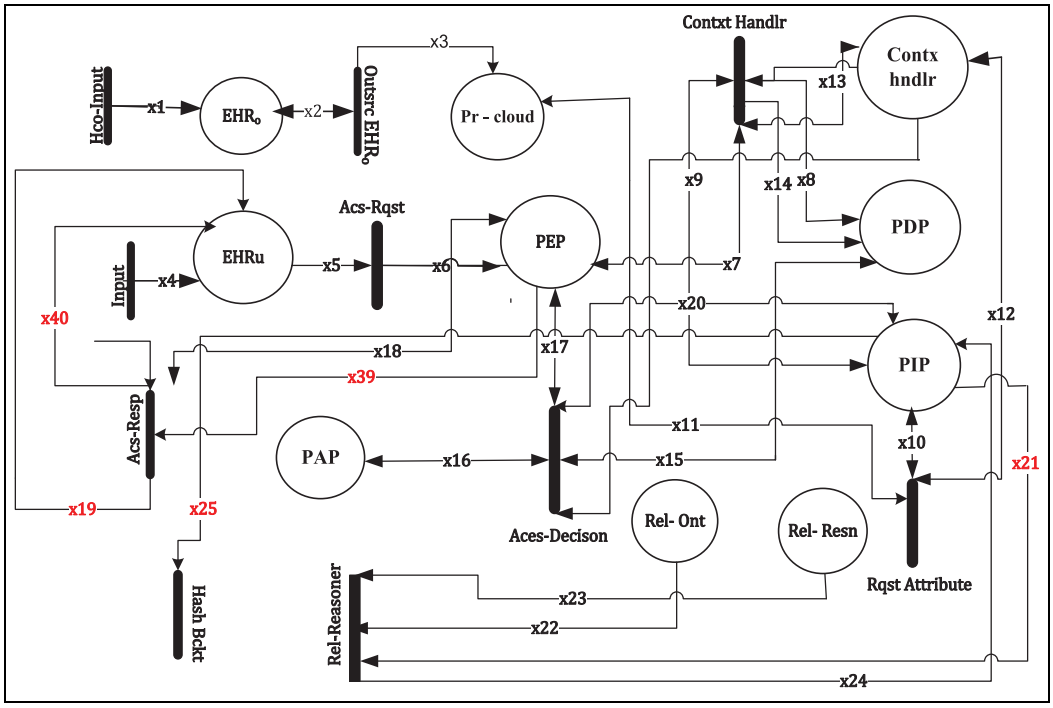

Figure 7. HLPN of Phase A-XACML-hybrid RS-ABAC.

Table 4. Summary of notations.

Symbol	Description	Symbol	Description
EHR_u	EHR users.	EHR_o	Original EHR data.
Pr cloud	Private cloud.	EHR_{An}	Anonymized EHR data.
Pb cloud	Public cloud.	QI	Quasi-identifier.
PEP	Policy enforcement point.	SA	Sensitive attribute
Cntx hnd	Context handler.	*P*	Places.
PIP	Policy information point.	*T*	Transitions.
PDP	Policy decision point.	*F*	Flow.
R_n	Rules for transition.	φ	Data types.
Rel-Ont	Relationship ontology	Anmz policy	Anonymized policy
HB	Hash bucket	Rel-Resn	Relationship reasoner
QIG	Quasi-identifier group	SOP	Set of logical, relational operators and numeric values
EQ_g	EHR quasi-identifier group	F-QIG	Final quasi-identifier group
GID	Group-ID	ESa	EHR Sensitive attributes
QAT	Quasi-identifier table	C	Sensitive value count
		SAT	Sensitive attribute table

EHR: electronic health records.

depicts the HLPN of the PRSX-AC model. The notations used are presented in Table 4. Table 5 shows the places, mapping, and the description involved in the PRSX-AC model HLPN. As shown in Figure 7, there are 20 places and 18 transitions involved in the PRSX-AC Model, so we have divided its HLPN model into Phase A, Phase B, and Phase C, same like we did in previous section. We have already described the proposed model with its logical details in previous section. In this section, our focus will be at the specification and modeling of PRSX-AC model phases.

Modeling and analyzing: Phase A-XACML-hybrid RS-ABAC

The HLPN model of PRSX-AC model starts by taking inputs from HCO and storing it in EHR_o. The transition *Outsrc* EHR_o stores EHR in the private cloud. EHR domain users (EHR_u) send access request to PEP; in this Phase A, original users' (O_u) request is described; however, the remaining users (Pr_u and Pb_u) can also send request in the same way. PEP sends that access request the context handler as given in equations (1)

Table 5. Places and mapping used in PRSX-AC HLPN.

Places	Mapping	Data types	Description
φ(EHR$_u$)	$\mathbb{P}$ (O$_u$ × Pr$_u$ × Pb$_u$)	A string-type value for entities.	Holds EHRs' original and private entities
φ(Pr cloud)	$\mathbb{P}$ (Attb$_{EHRo}$)	A string- and integer-type value for attributes	Holds Original EHR attributes
φ(Pb cloud)	$\mathbb{P}$(An policy × An QAT × An SAT)	A string- and integer-type value	Holds anonymize policy, anonymize QAT and SAT Tables
φ(PEP)	$\mathbb{P}$(Req × xacml-Req × Rsp × An QAT × An SAT × policy)	A string- and integer-type values	Holds EHR access request, XACML-based request, Access policy response
φ(Cntx hnd)	$\mathbb{P}$(xacml-Req × Attb$_{oe}$ × Attb$_{pe}$ × Attb$_{pbe}$ × Attb$_{EHRs}$)	A string- and integer-type values for attributes	Holds XACML request, Original and Private entity attributes
φ(PIP)	$\mathbb{P}$(Attb$_{ou}$ × Attb$_{pru}$ × Attb$_{pbu}$ × EQa × ESa)	A string- and numeric-type values for entity attributes and quasi and sensitive attributes values	Holds original entity attributes, Private entity attributes
φ(PAP)	$\mathbb{P}$(Policy)	A string-type value for Policy	Holds plain Access policy
φ(PDP)	$\mathbb{P}$(xacml-Req × Rsp)	A string-type value for Req, Rsp	Holds XACML-based request/ response
φ(EHR$_o$)	$\mathbb{P}$(Attb$_{EHRo}$)	A string- and integer-type value for EHRo attributes	Holds patient Identifier, Original EHR attributes
φ(Rel-Ont)	$\mathbb{P}$(R-ont)	A string-type value for ontology	Holds relationship ontology
φ(Rel-Resn)	$\mathbb{P}$(R-resn)	A string-type value for Relationship meaning	Holds relationship meaning
φ(HB)	$\mathbb{P}$(EQ$_g$ × ESa)	A string- and integer-type values for EQ$_g$ and ESa	Holds EHRs with same sensitive attributes
φ(SOB)	$\mathbb{P}$(EQ$_{gl}$)	A string- and integer-type values for EQ$_{gl}$	Holds set of L largest group bucket
φ(L-val)	$\mathbb{P}$(L)	A numeric-type value for L	Holds L value for diversity
φ(QIG)	$\mathbb{P}$(EQ$_G$ × Rtp × GID)	A string- and integer-type value for EQ$_G$,, Rtp and GID	Holds quasi attribute group with residue tuple value
φ(F-QIG)	$\mathbb{P}$(FQg × ESa × GID)	An integer- and string-type value for FQg,, ESa and GID	Holds Final Quasi group, sensitive value and group identifier
φ(SOP)	$\mathbb{P}$ (Op × Nmv)	Alpha numeric and numeric values for Op and Nmv	Holds relational operators, logical operators and numeric values
φ(Anmz policy)	$\mathbb{P}$ (A$_{nm}$ – P)	A string-type for anonymize policy	Holds anonymize policy
φ(QAT)	$\mathbb{P}$ (EQg×GID)	An integer value for quasi group and GID	Holds quasi-identifier group and Group-ID
φ(SAT)	$\mathbb{P}$(GID × ESa × C)	Numeric- and string-type value for GID, ESa and C	Holds Group-ID, sensitive attribute values, and sensitive value count

PRSX-AC: privacy-aware relationship semantics–based XACML access control model; HLPN: high-level Petri nets; EHR: electronic health records; QIG: quasi-identifier group; F-QIG: final quasi-identifier group; QAT: quasi attribute table; SAT: sensitive attribute table.

and (2). *Contxt Handlr* converts user request into an XACML request context and sends it to the PDP; in addition, *Contxt Handlr* also performs request forward activities for PDP, PEP, and PIP. However, the main functionality is given in equation (3). The HLPN of Phase A-XACML anonymization is shown in Figure 7

$$\begin{aligned} &\boldsymbol{R}(\boldsymbol{Outsrc\ EHRo}) = \forall i2 \in x2 \wedge \forall i3 \in x3| \\ &i3[1] := Store(i2[1]) \wedge x3 := x3' \cup \{i3[1]\} \end{aligned} \quad (1)$$

$$\begin{aligned} &\boldsymbol{R}(\boldsymbol{Acs - Rqst}) = \forall i5 \in x5 \wedge \forall i6 \in x6| \\ &i6[1] := UserReqst(\{i5[1]\}) \\ &\wedge x6' := x6 \cup \{i6[1]\} \end{aligned} \quad (2)$$

$$\begin{aligned} &\boldsymbol{R}(\boldsymbol{Cntxt\ Handlr}) = \forall i7 \in x7 \wedge \forall i8 \in x8| \\ &i8[1] := XACMLCntxt(\{i7[2]\}) \\ &\wedge x8' := x8 \cup \{i8[1]\} \end{aligned} \quad (3)$$

The PDP requests attributes from the ***Cntxt Handlr***, and it requests the remaining missing attributes from a PIP. The PIP contains Attb$_{ou}$, Attb$_{pru}$, and Attb$_{pbu}$ (attributes of original, private, and public users). The ***Rqst Attribute*** transition also receives Original EHR attributes Attb$_{EHR}$ from private cloud; after that, the PIP returns these requested subject/resource attributes to the ***Cntxt Handlr***. It sends the requested attributes to the PDP (equation 4). Transition ***Aces Decison***

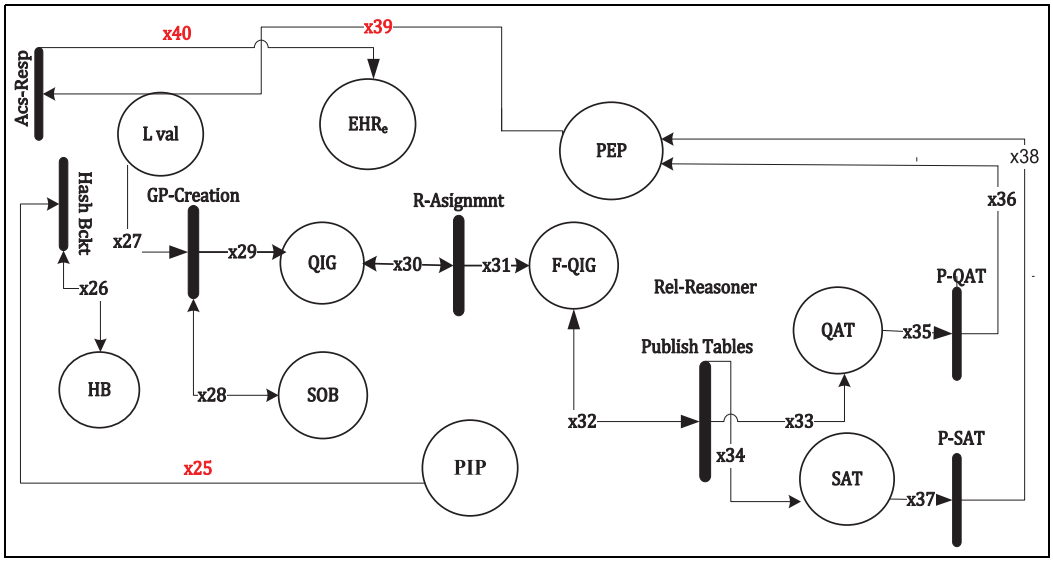

Figure 8. HLPN of Phase B-XACML-EHR anonymization.

evaluates the access policy as given in equation (5); for original users attributes ($Attb_{ou}$), policy access response is given to PEP, and it sends access response to original users O_u. Access request from Pr_u and Pb_u involves EHR data anonymization, and we will describe it in detail in Phase B, given in the next section

$$\begin{aligned}&\boldsymbol{R}(\boldsymbol{RqstAttribute}) = \forall i \in x \wedge \forall i11 \in x11 \wedge \forall i12 \in x12|\\ &i11[1] := User\ Reqst(\{i[2]\})\\ &\wedge\, i12[2] := Store\ atb(\{i11[1]\})\\ &\wedge\, x12 := x12 \cup \{i12[2]\}\end{aligned} \tag{4}$$

$$\begin{aligned}&\boldsymbol{R}(\boldsymbol{Aces\ Decison}) = \forall i15 \in x15 \wedge \forall i16 \in x16 \wedge \forall i17 \in x17, i20 \in x20|\\ &[i17[3] := Acs - Dcsn(\{i15[1], i16[1]\} \wedge i20[1]\})\\ &\wedge\, x17' := x17 \cup \{i17[3]\}]\\ &\vee\, [i20[1] := Acs - Dcsn\{(i15[1], i16[1]) \wedge (i20[2]) \vee (i20[3])\}\\ &\wedge\, x20' := x20 \cup \{i20[1]\}]\end{aligned} \tag{5}$$

In equation (6), transition $\boldsymbol{Acs - Rspn}$, perform request response to different user requests (O_u, Pr_u, and Pb_u). In this Phase A, we are only giving O_u request response, whereas other users response will be presented in Phase B and Phase C. Simple response of O_u based on XACML decision. In case of private users (Pr_u), access request is given to ***Cntxt Handlr*** and it further sends access request to transition $\boldsymbol{Rel - Reasoner}$. Relationship meaning of Pr_u is returned with function ***Rlshp***() to PIP as shown in equation (7)

$$\begin{aligned}&\boldsymbol{R}(\boldsymbol{Acs - Rspn}) = \forall i25 \in x25 \wedge \forall i26 \in x26, i35 \in x35, i36 \in x36|\\ &i19[1] := Respns(\{i18[3]\})\\ &\wedge\, x19' := x19 \cup \{i19[1]\}\end{aligned} \tag{6}$$

$$\begin{aligned}&\boldsymbol{R}(\boldsymbol{Rel - Reasoner}) = \forall i21 \in x21 \wedge \forall i22 \in x22, i23 \in x23, i24 \in x24|\\ &i24[2] := Rlshp(\{i22[1], i23[1]\})\\ &\wedge\, x24' := x24 \cup \{i24[1]\}\end{aligned} \tag{7}$$

Modeling and analyzing: Phase B-XACML-EHR anonymization

In Phase A, we have modeled XACML-based request/response when ODU and P_RDU are participating in PRSX-AC model. ODU will get Original EHR data XACML-based response. When a request is received from P_RDU, the relationship semantics are resolved as XACML lacks semantic interpretation of participating entities. The HLPN of Phase B-XACML anonymization is shown in Figure 8.

In Phase B, EHR data anonymization modeling is performed as follows. EHRs from PIP having same sensitive values are hashed and stored in HB as shown in equation (8). After that, tuples are taken from set of l largest buckets SOB and quasi groups are formed with the union of tuples to quasi groups in function ***GPC***(); moreover, tuples from SOB are checked with ***Residue***(), and single residue tuple is stored in QIG. GID is obtained from ***count***() of quasi groups as given in equation (9)

$$\boldsymbol{R}(\boldsymbol{HashBckt}) = \forall i25 \in x25 \wedge \forall i26 \in 26| \{(i25[4])i_{\forall i25[4] \in i} = i25[5]\} \vdash i26[1] := HashB\left(i25[4]i_{\forall i25[4] \in i}\right) \wedge i26[2] := HashB\left(i25[4]i_{\forall i25[4] \in i}\right) \wedge x26' := x26 \cup \{i26[1], i26[2]\} \quad (8)$$

$$\boldsymbol{R}(\boldsymbol{GP\_Creation}) = \forall i27 \in x27 \wedge \forall i28 \in 28 \wedge \forall i29 \in 29| i29[1]l_{\forall i28[1] \in l} := GPC\left(i28[1]l_{\forall i28[1] \in l}\right) \wedge i29[2] := Residue\left(i28[1]l_{\forall i28[1] \in l}\right) \wedge i29[3] := = count\left(i29[1]l_{\forall i28[1] \in l}\right) \wedge x29' := = x29 \cup \{i29[1], i29[2], i29[3]\} \quad (9)$$

In residue assignment process, ***R_Assignment*** transition given in equation (10) is used to assign residue tuple from SOB to quasi attribute group that have no sensitive value. QAT table which contains quasi-identifier group EQg and GID and SAT table which contain GID, sensitive attributes ESa and count of distinct sensitive attributes C are published as given in equation (11). After anonymization, ***P_QAT*** and ***P_SAT*** transitions store the anonymized tables AnQAT and AnSAT to PEP as shown in equations (12) and (13)

$$\boldsymbol{R}(\boldsymbol{R\_Assignment}) = \forall i30 \in x30 \wedge \forall i31 \in 31| (i30[1] \in (\nexists (i30[2])) \rightarrow i31[1] := i30[2] \wedge i31[3] := i30[3] \wedge x31 := x31 \cup \{i31[1], i31[3]\} \quad (10)$$

$$\boldsymbol{R}(\boldsymbol{PublishTables}) = \forall i32 \in x32 \wedge \forall i33 \in x33 \wedge \forall i34 \in x34| i33[1] := \left(i32[1]l_{\forall i32[1] \in l}\right) \wedge (i33[2] := i32[3]) \wedge x33' := = x33 \cup \{i33[1], i33[2]\}(i34[1] := (i32[3])) \wedge (i34[2] := = i32[2]) \wedge (i34[3] := count(i32[2])) \wedge x34' := = x34 \cup \{i34[1], i34[2], i34[3]\} \quad (11)$$

$$\boldsymbol{R}(\boldsymbol{P\_QAT}) = \forall i35 \in x35 \wedge \forall i36 \in 36| (i36[4]) = AnQAT(i35[1], 35[2]) \wedge x36' := x36 \cup \{i36[4])\} \quad (12)$$

$$\boldsymbol{R}(\boldsymbol{P\_SAT}) = \forall i37 \in x37 \wedge \forall i38 \in 38| (i38[5]) = AnSAT(i37[1], 37[2], 37[3]) \wedge x38' := x38 \cup \{i38[5]\} \quad (13)$$

Modeling and analyzing: Phase C-XACML-policy anonymization

We have modeled XACML anonymization algorithm in Phase B in this Phase C, we will model policy anonymization algorithm. Access policy anonymization is necessary to prevent privacy disclosures that may occur when policy is transmitted from private to public cloud. Access policy is received from PEP as shown in HLPN of Phase C-XACML-policy anonymization. Transition *P-Anonymization* compares operators from SOP with the policy and performs hashing of compared policy attributes as given in rule (equation (14)). Figure 9 shows the HLPN of Phase C-XACML-policy anonymization.

In equation (15), transition Send-Data sends anonymized EHR tables AnQAT, AnSAT, and An Policy to the public cloud. Phase C completes when access response is given to EHR_e in the last transition Acs-Resp as given in equation (16)

$$\boldsymbol{R}(\boldsymbol{PolicyAnonymizr}) = \forall i41 \in x41 \wedge \forall i42 \in x42 \wedge \forall i43 \in x43| i41[6] \notin (x42[1] \vee i42[2]) \vdash i43[1] := (\{hash(i41[6])\}) \wedge x43' := x43 \cup \{i43[1]\} \quad (14)$$

$$\boldsymbol{R}(\boldsymbol{Send-Data}) = \forall i44 \in x44 \wedge \forall i45 \in x45 \forall i46 \in x46 \wedge \forall i47 \in x47| i47[1] := send(i46[1]) \wedge i47[2] := send(i44[1]) \wedge i47[3] := = send(i45[1]) \wedge x47' := x47 \cup \{i47[1], i47[2], i47[3], \} \quad (15)$$

$$\boldsymbol{R}(\boldsymbol{Acs-Resp}) = \forall i48 \in x48 \wedge \forall i49 \in x49| i49[2] := A - Rsp(\{i48[2]\}) \wedge x49' := x49 \cup \{i49[2]\} \quad (16)$$

Formal verification of PRSX-AC model

We have presented the formal modeling and analysis of proposed (PRSX-AC) model in previous section. In this section, we will present the security and privacy property verification of PRSX-AC model. In verification process, we demonstrate the correctness of the base system. We need system specification and properties to verify a proposed model or a system.[74] In this work, we use the bounded model checking[75,76] technique to perform the verification, using SMT-Lib and Z3 solver. In bounded model checking, we verify the system description, in this process, it is checked whether there are any of the valid inputs that drive the system into a state where the system always terminates after a finite number of steps. We perform various tasks during the process of bounded model checking: *Specification*, the properties or rules, which must be satisfied by the system to prove its correctness; *Modeling*, representation of the system; *Verification*, we use a tool to check whether the specifications have been satisfied by the model. The definition of bounded model checking[74] is given as, "Formally, given a Kripke Structure $M = (S, S_O, R, L)$ and a k-bound, the bounded model checking problem is to find $\{M \models_k Ef\}$, where S is the finite set of states, $S_{O,}$ is a set of initial states, R is the set of transitions, such that $R \subseteq S \times SL$ is the set of labels." In bounded model checking problem, an execution path is searched in a Kripke structure M of length k that satisfies a formula f. We have verified the PRSX-AC model by proving the correctness of

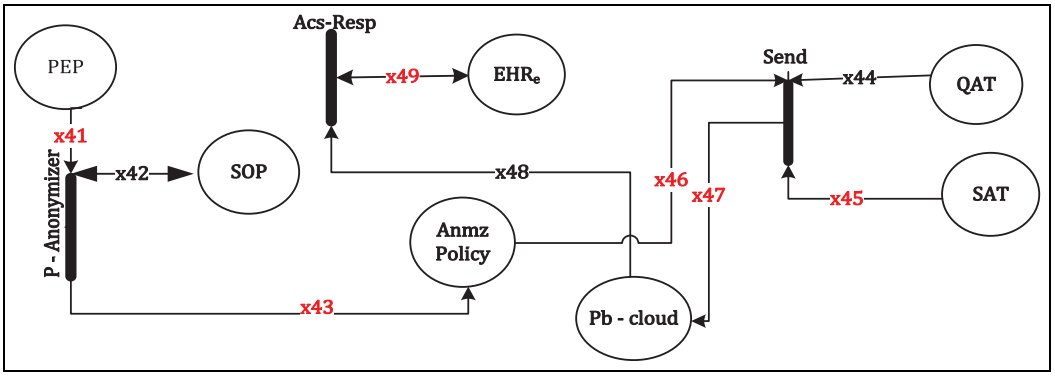

Figure 9. HLPN of Phase C-XACML-policy anonymization.

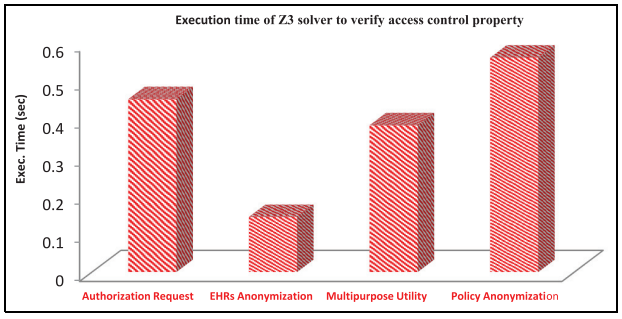

Figure 10. Verification results of PRSX-AC model.

privacy-aware relationship-based access control (PR-AC) algorithm, XACML anonymization algorithm, and XACML-policy anonymization algorithm. We have modeled the algorithms using HLPN, and the Z formal language is being used to define the transition rules in previous section. We will use the same bounded model checking technique to perform the verification of our proposed (PRSX-AC) model using SMT-Lib and Z3 solver. We have verified the following algorithms specific properties of proposed (PRSX-AC) model:

- *Property 1*. Authorization request: access request from ODU or PRDU for EHR data is given to private cloud. Any EHR access attempt from un authorize user at public and private cloud will be denied.
- *Property 2*. EHR anonymization: EHR data will be anonymized through Anatomy and stored in anonymized EHR repository. EHR anonymization property will anonymize EHR data so that it can preserve patients sensitive attributes against privacy attacks like identity disclosure and attribute disclosure.
- *Property 3*. Multipurpose utility: PDP evaluates the access request against stored access policy in PAP and permissions will be given depending upon type of user:
  - If access request come from OD users, it will get response from Original EHR data at private cloud.
  - If access request come from P_RD users, it will get specific permission response, based on relationship from anonymized EHR data at public cloud.
  - If access request come from P_BD users, it will get permissions response from anonymized EHR data at public cloud.
  - Access request from any other unauthorized users like if P_RD users request Original EHR data, it will result in response Deny/Not Applicable.
- *Property 4*. Policy anonymization: access policy will be anonymized before transmission to public cloud. This property avoids possible attacks like data spoofing, unintended EHR data modification, and collusion attacks at public cloud.

The verification results of PRSX-AC model are given in Figure 10.

Experimental results and discussion

In this section, we present the experimental results to check the effectiveness of proposed (PRSX-AC) model-based approach. The performance and optimization parameters are evaluated in terms of response time and space requirement.

Preparation and settings

To evaluate our idea, we implemented a prototype that compiles XACML policy into MSSQL ACLs. For this purpose, we designed a resource database (hospital) that is populated with random data because of lack of enough information. The Patient attribute table consists of 50,000 patients EHRs with 25 attributes (attr0–attr24) each.[77] All the experiments were carried out on

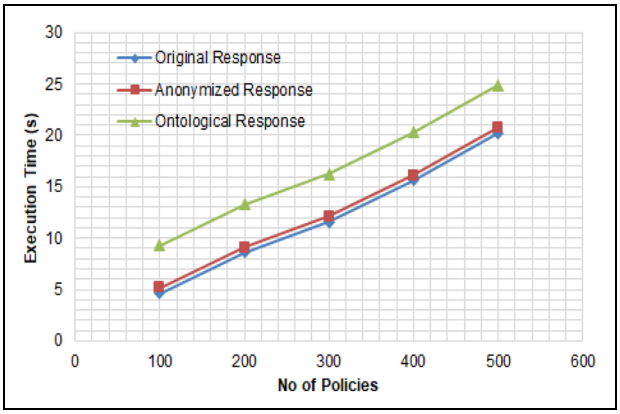

Figure 11. Policy response time.

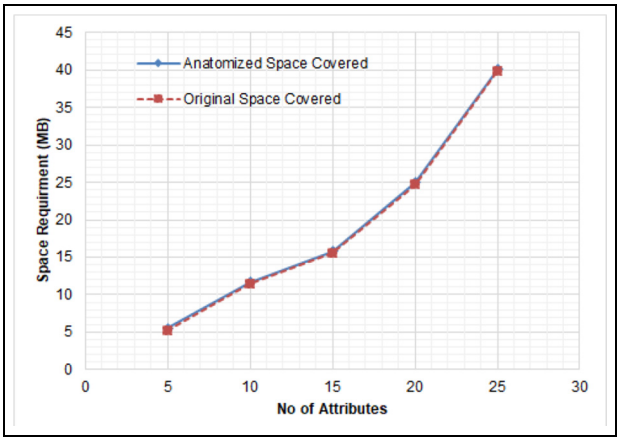

Figure 12. Space requirement for EHRs.

a 2.4 GHz Intel Core™ i3 with 8 GB memory and running Windows 10. We have used the database server MSSQL version 12.0.2000.8 in our experimental verification.

Access policy response time

When different domain users access EHR data, in such context, access response time is critically important factor for HCOs. In Figure 11, we have taken execution time in seconds on y-axis and number of policies on x-axis .We can deduce from Figure 11 that if we increase the number of records, then the retrieval time will also increase linearly. It can be easily shown from Figure 11 that there is noticeable increase in response time of P_RDU as compared to ODU and P_BDU. As given in Esposito,[78] the ontological response produces performance overhead, so in our case of hybrid Rel ABAC model, the ontological representation and inference create approximately the same overhead. However, anonymization of EHR data imposes less overhead as compared to P_RDU due to the use of privacy technique Anatomy. We have taken execution time of Anatomy as given in Shyamala and Christopher.[79] In our proposed model, we are giving access to different other domain users also, so it will improve multipurpose EHR usage in health scenarios.

Space requirement

For space requirement, we take an average in each analysis and round it to the nearest integer. Here, the space requirement is increasing linearly with the number of attributes; in this case, it is scalable. Figure 12 represents the space storage (in MBs) on the y-axis and the number of attributes (n) on the x-axis. It can be stated from Figure 12 that there is negligible difference of space requirement between original attributes and anonymized attributes. As in Anatomy, we have original attributes even after applying the privacy technique and there is no increase in space of anonymized attributes. However, it must be noted that generalization-based privacy techniques application to EHR data records prominently increases the space requirement. It can be used to support a more useful fact that such types of privacy techniques can be used more effectively in EHR privacy-aware access scenarios.

Discussion

Experimental results show that we have successfully achieved the design goals for proposed (PRSX-AC) model. Proposed approach design goals are explained in detail in section "PRSX-AC model: design goals." It is shown in response time that different data user entities can get their required response depending upon their request. Access control mechanism prevents unauthorized access to EHR data; moreover, it saves system overhead in case of full EHR data retrieval. However, it is noted that ontological response time in terms of relationships is higher as compared to anonymized and original response. This increase in execution time is due to use of ontology in relationships. Anonymized response time introduces a minor delay that is acceptable against EHR personal sensitive information disclosure. Although number of requested attribute in access policy affects response time (access time increases with increase in number of attributes), in our proposed approach, we are using hybrid ABAC model in PRSX-AC. Its advantage is that we can selectively anonymize requested attributes so access time will not directly depend upon total number of EHR attributes. Multipurpose EHR usage is achieved as response from different data user entities and is given depending upon their specific requirement. Privacy preservation of EHR data is performed through anonymization technique Anatomy. Our solution provides defense against

external threats through policy anonymization and internal threat as authorized users in public cloud will also get anonymized version of EHR data with access control mechanism. Privacy technique Anatomy preserves EHRs' sensitive information disclosure. Space requirement shows that the use of Anatomy is highly suitable as it is not creating any space overhead as compared to other privacy-preserving techniques.

Conclusion

To provide privacy-aware fine-grained EHR access in cloud is a challenging task. Cloud-based EHR system has shown great potential to improve the quality of service and utilization of EHR data across medical institution. However, privacy preservation with multipurpose EHR usage in hybrid cloud is not completely focused in most of the proposed solutions. A comprehensive analysis of privacy-preserving solutions of cloud-based EHRs shows that although hybrid cryptographic access control schemes provide highly developed solutions, however, still it is not sufficient to support privacy preservation with multipurpose EHR data utility. The solutions also lack fine-grained relationship semantics for EHR access with an efficient privacy preservation mechanism. Our proposed (PRSX-AC) model is based upon exploratory research from related work. We have innovatively extended XACML-attribute-based access control mechanism with (Rel BAC) semantics, privacy technique Anatomy, and access policy anonymization in hybrid cloud. Our (PRSX-AC) model provides privacy with maximum EHR data utility. We have given relationship-based EHR access scenarios in PRSX-AC model, as it will enhance model understanding. The proposed model (PRSX-AC) is formally verified along with its security and privacy-preserving properties. Our experimental results show that implemented prototype of PRSX-AC model is effective in terms of performance and optimization parameters.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Adeel Anjum https://orcid.org/0000-0001-5083-0019
Saif UR Malik https://orcid.org/0000-0001-8195-1630

References

1. Häyrinen K, Saranto K and Nykänen P. Definition, structure, content, use, and impacts of electronic health records: a review of the research literature. *Int J Med Informat* 2008; 77(5): 291–304.
2. Yang J-J, Li JQ and Niu Y. A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generat Comp Syst* 2015; 43: 74–86.
3. van der Linden H, Kalra D, Hasman A, et al. Inter organizational future proof EHR systems: a review of the security and privacy related issues. *Int J Med Inf* 2009; 78(3): 141–160.
4. Simon SR, Kaushal R, Cleary PD, et al. Correlates of electronic health record adoption in office practices: a state wide survey. *J Amer Med Inform Assoc* 2007; 14(1): 1–117.
5. Ratnam KA and Dominic PDD. Cloud services–enhancing the Malaysian healthcare sector. In: *2012 International Conference on Computer & Information Science*, June 2012, pp.604–608, https://ieeexplore.ieee.org/document/6297101
6. Cao N, Wang C, Li M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data. In: *Proceeding of the IEEE INFOCOM* (2011), https://ieeexplore.ieee.org/document/6674958
7. Yuan J and Yu S. Efficient privacy-preserving biometric identification in cloud computing. In: *Proceedings of the IEEE INFOCOM* (2013), https://ieeexplore.ieee.org/document/6567073
8. Wang W, Chen L and Zhang Q. Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation. *Comp Netw* 2015; 88: 136–148.
9. Takabi H. Privacy aware access control for data sharing in cloud computing environments. In: *Proceedings of the 2nd international workshop on security in cloud computing*, ACM, 2014, https://dl.acm.org/citation.cfm?id=2600076
10. Mohandas A. Privacy preserving content disclosure for enabling sharing of electronic health records in cloud computing. In: *Proceedings of the 7th ACM India computing conference*, ACM, 2014, https://dl.acm.org/citation.cfm?id=2675753
11. Wang G, Liu Q and Wu J. Achieving fine-grained access control for secure data sharing on cloud servers. *Concurrency Comput Pract Exp* 2011; 23(12): 1443–1464.
12. Abbas A and Khan SU. e-Health Cloud: privacy concerns and mitigation strategies. In: Gkoulalas-Divanis A and Loukides G (eds) *Medical data privacy handbook*. London: Springer, 2015, pp.389–421.
13. Zhao F, Nishide T and Sakurai K. Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems. In: *Seventh inter-national conference on information security practice and experience (ISPEC)*, 2011, pp.83–97, https://link.springer.com/chapter/10.1007/978-3-642-21031-0_7
14. Xiao X and Tao Y. Anatomy: simple and effective privacy preservation. In: *Proceedings of the 32nd international conference on very large data bases (VLDB Endowment)*, 2006, http://www.vldb.org/conf/2006/p139-xiao.pdf

15. Li T, Li N, Zhang J, et al. Slicing: a new approach for privacy preserving data publishing. *IEEE Trans Knowledge Data Eng* 2012; 24(3): 561–574.
16. Tao Y, Chen H, Xiao X, et al. ANGEL: enhancing the utility of generalization for privacy preserving publication. *IEEE Trans Knowledge Data Eng* 2009; 21(7): 73–87.
17. Ganz N. *Data anonymization and its effect on personal privacy*. Dissertation, State University of New York, Albany, NY, 2015, https://www.albany.edu/honorscollege/files/Ganz_Thesis-final.pdf
18. Dwork C. Differential privacy: a survey of results. In: Gopal TV and Watada J (eds) *Theory and applications of models of computation*. Berlin; Heidelberg: Springer; 2008, pp.1–19.
19. Sedayao J. Enhancing cloud security using data anonymization. *White Paper, Intel Corporation*, 2012, https://media12.connectedsocialmedia.com/intel/07/8814/Intel_IT_Best_Practices_Enhancing_Cloud_Security_Data_Anonymization.pdf
20. Pandilakshmi KR and RashithaBanu G. An advanced bottom up generalization approach for big data on cloud, 2014; 3: 54–59, https://www.semanticscholar.org/paper/An-Advanced-Bottom-up-Generalization-Approach-for-Pandilakshmi-Banu/cf6d29f3e0b3ab3f0b0bc109c9ef35f7488d18da
21. Shrivastva KM, Rizvi MA and Singh S. Big data privacy based on differential privacy a hope for big data. In: *2014 international conference on computational intelligence and communication networks (CICN)*, IEEE, 2014, https://ieeexplore.ieee.org/document/7065587
22. Zhang K, Zhou X, Chen Y, et al. Sedic: privacy-aware data intensive computing on hybrid clouds. In: *Proceedings of the 18th ACM conference on computer and communications security*, ACM, 2011, https://dl.acm.org/citation.cfm?id = 2046767
23. Zhou Z, Zhang H, Du X, et al. Prometheus: privacy-aware data retrieval on hybrid cloud. In: *2013 INFOCOM proceedings*, IEEE, 2013, https://ieeexplore.ieee.org/document/6567072
24. Abbas A and Khan SU. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE J Biomed Health Inform* 2014; 18(4): 1431–1441.
25. Sandhu R, Ferraiolo D and Kuhn R. The NIST model for role-based access control: towards a unified standard. In: *Proceedings of ACM workshop role-based access control*, July 2000, pp.1–11, https://dl.acm.org/citation.cfm?id = 344301
26. Jin X. Attribute-based access control models and implementation in cloud infrastructure as service. Dissertation, the University of Texas at San Antonio, San Antonio, TX, 2014.
27. Takabi H, Joshi JBD and Ahn GJ. Security and privacy challenges in cloud computing environments. *IEEE Security Privacy* 2011; 8(6): 24–31.
28. Younis YA, Kifayat K and Merabti M. An access control model for cloud computing. *J Informat Security Appl* 2014; 19(1): 45–60.
29. Tianyi Z, Weidong L and Jiaxing S. An efficient role based access control system for cloud computing. In: *2011 IEEE 11th international conference on computer and information technology (CIT)*, IEEE, 2011, https://ieeexplore.ieee.org/document/6036597
30. Fung B, Wang K, Chen R, et al. Privacy-preserving data publishing: a survey of recent developments. *ACM Comp Surv* 2010; 42(4): 14.
31. Xu L, Cremers AB and Wilken T. Pseudonymization for secondary use of cloud based electronic health records, 2015, https://www.semanticscholar.org/paper/Pseudonymization-for-Secondary-Use-of-Cloud-Based-Xu-Cremers/c705c8e2b3d1fb608cf3464d24cbfcb22e267ea3
32. Sabitha S and Rajasree MS. Access control based privacy preserving secure data sharing with hidden access policies in cloud. *J Syst Architect* 2017; 75: 50–58.
33. Jin X, Krishnan R and Sandhu R. A unified attribute-based access control model covering DAC, MAC and RBAC. In: *Proceedings of 26th annual IFIP WG 11.3 working conference on data and applications security and privacy (DBSEC 2012)*, Paris, 11–13 July 2012. New York: ACM.
34. Hsieh G and Chen RJ. Design for a secure interoperable cloud-based personal health record service. In: *4th IEEE international conference on cloud computing technology and science proceedings*, 2012, https://ieeexplore.ieee.org/document/6427582
35. Alshehrsi S, Radziszowski SP and Raj RK. Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In: *2012 IEEE 28th international conference on data engineering workshops*, 2012, https://ieeexplore.ieee.org/abstract/document/6313671
36. Giunchiglia F, Zhang R and Crispo B. Relbac: relation based access control. In: *Fourth international conference on semantics, knowledge and grid*, 2008, https://ieeexplore.ieee.org/document/4725889
37. Lu Y and Sinnott RO. Semantic-based privacy protection of electronic health records for collaborative research. In: *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016, https://ieeexplore.ieee.org/document/7846988
38. Priebe T, Dobmeier W and Kamprath N. Supporting attribute-based access control with ontologies. In: *The first international conference on availability, reliability and security*, 2006, https://ieeexplore.ieee.org/document/1625344
39. Sahai A and Waters B. Fuzzy identity-based encryption. In: Cramer R (ed.) *Advances in cryptology–eurocrypt*. Berlin; Heidelberg: Springer, 2005, pp.457–473.
40. Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: *Proceedings of the 13th ACM conference on computer and communications security*, 2006, https://eprint.iacr.org/2006/309.pdf
41. Bethencourt J, Sahai A and Waters B. Ciphertext-policy attribute-based encryption. In: *IEEE symposium on security and privacy*, 2007, https://ieeexplore.ieee.org/document/4223236
42. Chase M and Chow SSM. Improving privacy and security in multi-authority attribute-based encryption. In: *Proceedings of the 16th ACM conference on computer and communications security*, 2009, https://ieeexplore.ieee.org/document/8327591
43. Song DX, Wagner D and Perrig A. Practical techniques for searches on encrypted data. In: *2000 IEEE symposium*

on security and privacy, 2000, https://ieeexplore.ieee.org/document/848445
44. Gentry C. Fully homomorphic encryption using ideal lattices. In: *STOC*, 2009, https://dl.acm.org/citation.cfm?id=1536440
45. Chen Y-Y, Lu JC and Jan JK. A secure EHRS system based on hybrid clouds. *J Med Syst* 2012; 36(5): 3375–3384.
46. Li Z-R, Chang EC, Huang KH, et al. A secure electronic medical record sharing mechanism in the cloud computing platform. In: *2011 IEEE 15th international symposium on consumer electronics (ISCE)*, 2011, https://ieeexplore.ieee.org/document/5973792
47. Achieving forward secrecy and unlink ability in cloud-based personal health record system, https://ieeexplore.ieee.org/document/7345421
48. Zhang R and Liu L. Security models and requirements for healthcare application clouds. In: *IEEE 3rd international conference on cloud computing (CLOUD)*, 2010, https://ieeexplore.ieee.org/document/5557983
49. Narayan S, Gagné M and Safavi-Naini R. Privacy preserving EHRS system using attribute-based infrastructure. In: *Proceedings of the 20 ACM workshop on cloud computing security*, 2010, http://courses.cs.vt.edu/cs6204/Privacy-Security/Papers/Crypto/Privacy-EHR-ABE.pdf
50. Alshehrsi S, Radziszowski S and Raj RK. Designing a secure cloud-based EHRs system using ciphertext-policy attribute-based encryption. In: *Proceedings of the data management in the cloud workshop*, Washington, DC, 2012, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.6819
51. Barua M, Liang X, Lu R, et al. ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing. *Int J Security Netw* 2011; 6(2–3): 67–76.
52. Peleg M, Beimal D, Dori D, et al. Situation-based access control: privacy management via modelling of patient data access scenarios. *J Biomed Informat* 2008; 41(6): 28–40.
53. Tong Y, Sun J, Chow SSM, et al. Cloud-assisted mobile-access of health data with privacy and auditability. *IEEE J Biomed Health Inform* 2014; 18(2): 419–429.
54. Riedl B, Grascher V, Fenz S, et al. Pseudonymization for improving the privacy in e-health applications. In: *Proceedings of the annual Hawaii International conference on system sciences*, 2008, pp.1–9, https://ieeexplore.ieee.org/document/4438959
55. Huang LC, Chu HC, Lien CY, et al. Privacy preservation and information security protection for patients' portable electronic health records. *Comput Biol Med* 2009; 39(9): 743–750.
56. Bahga A and Madisetti VK. A cloud-based approach for interoperable electronic health records (EHRs). *IEEE J Biomed Health Informat* 2013; 17(5): 894–906.
57. Premarathne U, Abadbba A, Alabdulatif A, et al. Hybrid cryptographic access control for cloud-based EHR systems. *IEEE Cloud Comp* 2016; 4: 58–64.
58. Yang K, Liu Z, Jia X, et al. Time-domain attribute-based access control for cloud-based video content sharing: a cryptographic approach. *IEEE Trans Multimedia* 2016; 18(5): 940–950.
59. Gope P and Amin R. A novel reference security model with the situation based access policy for accessing EPHR data. *J Med Syst* 2016; 40(11): 242.
60. Sweeney L. Achieving K-anonymity privacy protection using generalization and suppression. *Int J Uncertainty Fuzziness Knowledge Based Syst* 2002; 5: 571–588.
61. Pino C and Di Salvo R. A survey of cloud computing architecture and applications in health. In: *International conference on computer science and electronics engineering*, 2013, https://www.semanticscholar.org/paper/A-Survey-of-Cloud-Computing-Architecture-and-in-Pino-Salvo/d2eeed3f76fd352e7358c44fe1568f6630ca2f7e
62. Danwei C, Chen L, Fan X, et al. Securing patient-centric personal health records sharing system in cloud computing. *Comm China* 2014; 11(13): 121–127.
63. Naehrsig M, Lauter K and Vaikuntanathan V. Can homomorphic encryption be practical? In: *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, 2011, https://eprint.iacr.org/2011/405.pdf
64. Lin H, Shao J, Zhang C, et al. CAM: cloud-assisted privacy preserving mobile health monitoring. *IEEE Trans Inf Foren Security* 2013; 8(6): 985–997.
65. Ruj S, Stojmenovic M and Nayak A. Privacy preserving access control with authentication for securing data in clouds. *2012 12th IEEE/ACM international symposium on cluster, cloud and grid computing (CCGRID)*, 2012, https://ieeexplore.ieee.org/document/6217466
66. Chandrasekaran S, Mohan S and Natarajan R. Survey on HealthCloud characteristics. *Health Tech* 2015; 5(2): 135–146.
67. Zhang R, Liu L and Xue R. Role-based and time-bound access and management of EHRS data. *Security Comm Netw* 2014; 7(6): 994–915.
68. Ali M, Khan SU and Vasilakos AV. Security in cloud computing: opportunities and challenges. *Informat Sci* 2015; 305: 357–383.
69. Pecarina J, Pu S and Liu JC. SAPPHIRE: anonymity for enhanced control and private collaboration in healthcare clouds. In: *2012 IEEE 4th international conference on cloud computing technology and science (CLOUDCOM)*, 2012, https://ieeexplore.ieee.org/document/6427488
70. Benaloh J, Chase M, Horvitz E, et al. Patient controlled encryption: ensuring privacy of electronic medical records. In: *Proceedings of the 2009 ACM workshop on cloud computing security*, 2009, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.147.8299
71. Hilia M, Chibani A, Winter T, et al. Semantic based authorization framework for multi-domain collaborative cloud environments. *Procedia Comp Sci* 2017; 9: 718–724.
72. Joshi M, Mittal S, Joshi KP, et al. Semantically rich, oblivious access control using ABAC for secure cloud storage. In: *2017 IEEE international conference on edge computing (EDGE)*, 2017, https://ieeexplore.ieee.org/document/8029268
73. eXtensible Access Control Markup Language (XACML) (version 3.0.), 2013, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
74. Malik SUR, Khan SU and Srinivasan SK. Modeling and analysis of state-of-the-art VM-based cloud management platforms. *IEEE Trans Cloud Comp* 2013; 1: 50–63.

75. Ali M, Malik S and Khan S. DaSCE: data security for cloud environment with semi-trusted third party. *IEEE Trans Cloud Comp* 2015; 5: 642–655.
76. Malik SUR, Bilal K, Member S, et al. Modeling and analysis of the thermal properties exhibited by cyber physical data centers. *IEEE Syst J* 2015; 11: 163–172.
77. Jahid S, Gunter C, Hoque I, et al. MyABDAC: compiling XACML policies for attribute-based database access control. In: *Proceedings of the first ACM conference on data and application security and privacy*, 2011, https://experts.illinois.edu/en/publications/myabdac-compiling-xacml-policies-for-attribute-based-database-acc
78. Esposito C. Interoperable, dynamic and privacy-preserving access control for cloud data storage when integrating heterogeneous organizations. *J Netw Comp Appl* 2018; 108: 124–136.
79. Shyamala SV and Christopher T. Anatomisation with slicing: a new privacy preservation approach for multiple sensitive attributes. *Springerplus* 2016; 5(1): 964.