Journal of King Saud University – Computer and Information Sciences (2017) 29, 505–519

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

Proposing hierarchy-similarity based access control framework: A multilevel Electronic Health Record data sharing approach for interoperable environment

Shalini Bhartiya [a,*], Deepti Mehrotra [a], Anup Girdhar [b]

[a] Amity School of Engineering and Technology, Amity University, Uttar Pradesh Sector 125, Noida, U.P., India
[b] Sedulity Solutions, 310 Suneja Towers-II, Janakpuri, New Delhi, India

Received 16 May 2015; revised 16 July 2015; accepted 25 August 2015
Available online 2 November 2015

KEYWORDS

Access control policies;
Electronic Health Records (EHR);
Hierarchical Similarity Analyzer (HSA);
Interoperable healthcare environment;
Security

Abstract Interoperability in healthcare environment deals with sharing of patient's Electronic Health Records (EHR) with fellow professionals in inter as well as intra departments or organizations. Healthcare environment experiences frequent shifting of doctors, paramedical staff in inter as well as intra departments or hospitals. The system exhibits dynamic attributes of users and resources managed through access control policies defined for that environment. Rules obtained on merging of such policies often generate policy-conflicts thereby resulting in undue data leakages to unintended users. This paper proposes an access control framework that applies a Hierarchy Similarity Analyzer (HSA) on the policies need to be merged. It calculates a Security_Level (SL) and assigns it to the users sharing data. The SL determines the authorized amount of data that can be shared on successful collaboration of two policies. The proposed framework allows integration of independent policies and identifies the possible policy-conflicts arising due to attribute disparities in defined rules. The framework is implemented on XACML policies and compared with other access models designed using centralized and decentralized approaches. Conditional constraints and properties are defined that generate policy-conflicts as prevalent in the policies.

* Corresponding author at: ED-94, Tagore Garden, New Delhi 110027, India
E-mail addresses: shalinibhartiya69@gmail.com (S. Bhartiya), mehdeepti@gmail.com (D. Mehrotra), anup@sedulitygroups.com (A. Girdhar).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

1. Introduction

Healthcare is a time-bound service. The major advantage of electronic health care record is timely availability of health data at any desired location so that patient can get appropriate treatment. Along with timely retrieval of health data, equally important is the assurance of maintaining the confidentiality and privacy of patient's health records. This is more complex

http://dx.doi.org/10.1016/j.jksuci.2015.08.005
1319-1578

for health environment primary due to frequent shift of roles, departments and duties. Today is an era of distributed computing (Xiao et al., 2009) where users of different organizations need to collaborate and access each other's resources. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule of 1996 establishes guidelines for strengthening the privacy and security protections for individual's Electronic Health Records(EHRs) in such collaborations.

An interoperable health system facilitates use of software applications for exchanging data by maintaining many-to-many relationship between health care provider, patients and data resources. This approach provide better integration and sharing but also demand a framework that ensures privacy and security which can be achieved by designing proper policies for the disclosure and use of health care information. Achieving interoperability in an open and dynamic healthcare environment is a difficult task (Bhartiya and Mehrotra, 2013) and requires a cooperative access control approach to achieve secured sharing of authorized data to the users. Traditional access control framework varies between centralized to decentralized access control approaches and for sharing of EHR among different organization, access for secured sharing can be controlled and managed either through centralized or decentralized approach.

The centralized access control approach (Carmagnola et al., 2000) relies on a central authority for permitting/denying access to the required resources. It results in consistent and uniform supply of data to the legitimate users. The centralized control of access reduces administrative effort of managing the resources but also is vulnerable in terms of security threats. Usually in an interoperable environment, it is not possible to design a centralized access control model. A need exist to design an authorization system (NIST SP 800–162) in order to maintain proper integrity, confidentiality and availability of the data. Decentralized approach (Saltman et al., 2007) distributes the authority to the person nearer to the resource. Each decentralized system has its own conceptual storage and hierarchies of users and resources. The powers of permitting/denying access to the data are distributed to each person who leads one or more team in an organization. This approach is the most sought in ubiquitous computing environments directly exchanging data in peer-to-peer manner. This model lacks consistency controls but ensures quick access to data and other resources.

Accessing data in interoperable environment also experiences contradictory or undefined authorizations necessary for administering the accountability on sharing of data between disparate systems. Another relevant issue while integrating disparate access control policies is the emergence of policy-conflicts where two or more rule may contradict with each other. Information sharing in healthcare environment is usually dynamic. It requires preserving the availability, integrity and confidentiality of EHRs that may differ with each patient's need.

A framework proposed in this paper considers Attribute based access model (ABAC) as its base model. Attribute based access model (ABAC) (Hu et al., 2013) is a logical access control methodology where rule attributes are evaluated to determine the authorization for performing the set of defined operations. The idea is to fine-grain the available access control policies on the basis of the user's hierarchical positions in their respective organizations. It requires designing of framework that follows the principles of least privilege ensuring generation of only the relevant rules. Due consideration is given to preserve the internal consistency and authorization while refining the given policies.

This paper is divided into 6 sections. Section 1 explains the need and significance of interoperable healthcare environment and the problems in integrating disparate access control policies. Section 2 consolidates the work done in past and performs a comparative analysis of various access control models with the proposed framework. Section 3 presents the framework proposed and XACML schema used for designing and verifying the access control policies listed in Appendix A. Section 4 represents the healthcare organizational hierarchies with respect to user and resource attributes. Section 5 deals with verification of the proposed framework using an automated simulator, Access Control Policy Testing (ACPT). The verification is justified through a case study that illustrate the implementation of the framework and its comparison with other approaches. Section 6 concludes and interprets the results obtained that justify the viability of the proposed framework.

2. Literature review

A lot of research has been conducted in past for combining and integrating access control models without exposing the data to illegal and unauthorized disclosure. Each model represent unique features (Karp et al., 2010) that make it different from other models, both, syntactically and semantically. Discretionary Access Control (DAC) model depends on access control lists (ACLs) for determining authorization. In healthcare environment the users experience frequent shift in roles, hence, ACLs need to be optimized (Al-Abdulmohsin, 2009) for quick and secured access to the data. Mandatory Access Control (MAC) model is based on labeling on the resource and the user's credentials. In this environment the variables change once for all and hence cannot respond to dynamically changing environments like healthcare where resource levels change dynamically and require to be in synchronization with the change in user's credentials. Role-based access (RBAC) model (Sandhu et al., 1996; Nyanchama and Osborn, 1999) developed a role-based model using graph theory. It simplifies the security management but challenges the administration of the organizations where several roles are managed for the users simultaneously. The major emphasis is on fine-grain the existing access control policies while designing the secured and interoperable EHR framework.

Various techniques have been deployed to fine-grain access control models with an objective of providing secured and flexible access to the data. Setting up authorization is dependent on the storage mechanism adopted by a particular application. The authorizations may differ in centralized and distributed approach of data storage. Bertino et al. (1994) addresses the semantic data modeling concepts and develops an integrated authorization for interoperable relational and object-oriented databases. Azeez and Venter (2013) propose and simulate RBAC framework that satisfies authorizations and enforces interoperable, scalable and suitable access control for multi-domain grid-based environment. A middleware proposed by Ciampi et al. (2010) evaluates the interoperability facilities in an agent-based architecture where authorizations are

Table 1 Comparative Study of HSA and other access control frameworks/models.

Features	Models					
	The role graph model (Nyanchama and Osborn, 1999)	BPD-ACS (Chandramouli, 2000)	Privacy preserving Model (Yang et al., 2008)	Health Agents system (Xiao et al., 2009)	Open Agent Architecture (OAA)-(Ciampi et al., 2010)	HSA
Type	RBAC	$RBAC_2$	PBAC	Hybrid (DAC, MAC, RBAC)	Virtual Systems	ABAC
Interoperability	X	X	X	√	√	√
Heterogeneity	X	X	X	√	√	X
Authorization	√	√	X	X	X	√
Access relevant data	√	√	√	X	X	√
Dynamism	√	X	√	√	√	√
Resolve policy-conflicts		X	X	X	X	X
Simple to implement	√	√	√	X	√	√
flexibility	√	√	√	√	√	√
Level of granularity	Fine	Medium	Medium	Fine	Low	Fine
Govt. regulations	X	√	√	X	X	X
Computation load	Low	Medium	Medium	Low	High	Low

determined to control the interaction between various agents. This paper focuses on integration of disparate healthcare systems each implementing own data access policies and constraints. Various access control models are compared to identify their robustness and dependability in ascertaining secured sharing of EHR under well-defined authorizations. Table 1 shows a comparative study of our framework with these models on most important features (Bhartiya and Mehrotra, 2013) ascertaining secured sharing of sensitive data among legitimate stakeholders.

How far the proposed framework satisfies above mentioned parameters must be ascertained using relevant testing and verification tool. The comparison process can be light-weight with low computational effort compromising on the accuracy of results or can be computationally expensive with more accurate methods such as Boolean checking or semantic analysis. Testing can also be done by simulating the proposed framework and comparing it with existing models and approaches. Automated testing expands the testing boundaries enabling verification of generated request through an exhaustive state-space search. The literature reveals various verification tools Margrave (Fisler et al., 2005), Cirg (Martin and Xie, 2007), PoliVer (Koleini and Ryan, 2011), ACPT (Hwang et al., 2010) capable of testing similar applications. These and many other such tools can verify the access policies using one or the other fault-detection techniques such as logical formulas (Hu and Kuhn, 2011) of temporal logic (Computational Tree Logic (CTL) and Linear-time Temporal Logic (LTL)). The prerequisite of each tool differs in their requirement for producing the test results.

An algorithm proposed by Lin et al. (2007) iterates through all rules in policy set of each organization and calculates similarities between each rule attribute of both policies. It determines the closeness of two policies concluding the probability that the two policies can securely integrate with each other. The most fundamental requirement is allowing legitimate and authorized access of EHR considering all disparities prevalent in the access policies. In healthcare domain, one user works in different role-capacity at any given point of time. Moreover, there can be various entry and exit points of accessing data at the same time. A doctor in the role of primary doctor for one patient may shift to the role of specialist for other patient at the same time. The access rights must differ in both the situations. Moreover, the authority is not static. A doctor being a part of team handled by a senior consultant may be practicing independently in the same hospital. The accountability and responsibility must differ in both the situations. Hence, it is challenging to determine authorized and consolidated access to EHRs.

3. Proposed framework

With an ever increasing volume of electronic data and advancement in technological resources, it becomes difficult and unmanageable to control and limit access to authorized users. Each system is autonomous comprising unique domain structure or hierarchy and security policies. When a policy conflict arise, it is difficult to give weight-age to any policy for selecting the best choice. Moreover, there is no universal method of resolving policy conflicts (Zidat and Djoudi, 2006).

Bhartiya and Mehrotra (2015) conducted CHAID analysis using questionnaire-based study in real-time health environment of various hospitals and related agencies. Observations revealed the possibility of defining local authorization using positional distances of each healthcare user in the organizational hierarchy. Hence, it strengthened the certainty of identifying similarities between rules attributes of access control policies by calculating the positional distance of each user in their respective organizational hierarchies. It would further

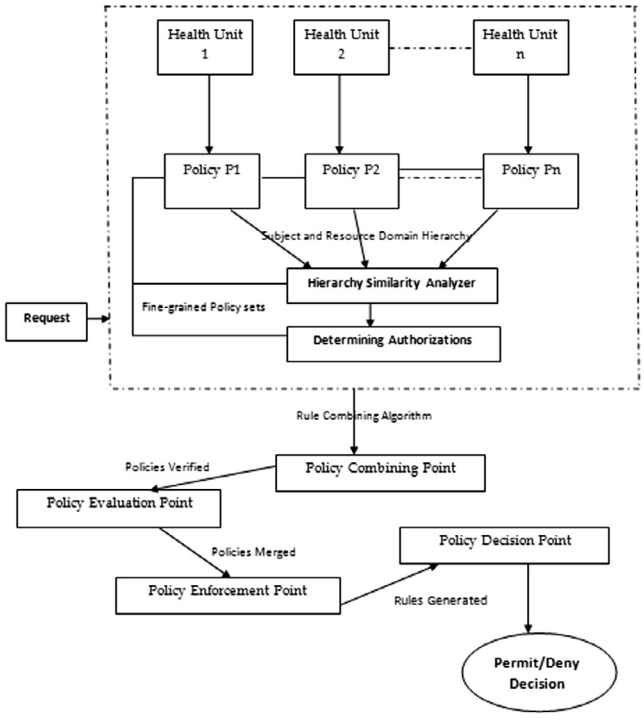

Figure 1 Proposed framework for fine-graining XACML policies using HSA.

impose robust authorization, thereby, enhancing the availability of EHR without compromising its confidentiality and privacy. Each rule comprises multiple attributes that are either categorical or numerical in nature. Thus a system can be designed by deducing similarities between access control policies in sharable health care systems based Lin et al., 2007 approach. The similarities are obtained using Hierarchy Similarity Analyzer[1] (HSA) that finds the unique values from the similarity scores obtained on comparing two distant organizational hierarchies. The values are then assigned to each user as Security_level[2] (SL) thus bridging the interoperability gap between disparate healthcare environments.

The proposed framework (Fig. 1) extends the XACML structure. Two or more health care units collaborate and allow access to each other's data repository. Complexities increase due to heterogeneity of data and storage structure adopted by each unit. The framework comprises of a Hierarchy Similarity Analyzer algorithm that finds similarities between rule attributes defined in disparate policies (***P1, P2. . ..,Pn***). The HSA (***Hierarchy Similarity Analyzer***) calculates the similarity score for all matched and unmatched attributes based on the hierarchical distance of users and resource (EHR) in their respective hierarchies. The rules are fine-grained by allocating a Security_Level (SL) to each user and resource attribute in the given rule set. Authorizations are added in the existing rule-sets by assigning SLs obtained from HSA. Authorizations ensure secured sharing of EHR using simple security rule where a user at lower level can access high-level resource only under the authorization of a higher level user. The user generates a request demanding an access to the data. The refined policies are merged (***Policy Combining point***) using chosen rule combining algorithm. The rules are evaluated (***Policy Evaluation Point***) to satisfy the environmental constraints and set authorization. A reduced rule-set is thus obtained. These rules are then merged, thereby, handling policy conflicts (***Policy Decision Point***) and a final decision (***Permit/Deny Decision***) is obtained to either permit or deny access to the requested data.

Standard such as Extensible Access Control Markup Language (XACML) provide a template for designing flexible and dynamic access control policy framework and is widely used for environment that supports interoperability and also heterogeneity. Basic elements of XACML include Policy Set, Policy, Rule, Target and Condition. Policy set refers to the set of access control policies defined in the organizations. The Policy contains the rules defined in each policy set. Each rule comprise of a set of Subject, Resource and Action described as S, R, and A respectively. Each of these components is associated with a set of attributes having one or more attribute values that are used for taking access control decisions. The Target (T) specifies the user or resource controlling the access through defined rules and policies. The Condition element (C) is optional and imposes constraint on the rules, if required. The Effect (E) in the rule is a decision component for granting or denying an access to the data. An access request is a tuple $\{s, r, a\}$ where $s \subset S$, $r \subset R$, $a \subset A$ have multiple attributes. Whenever an access request is made, it is passed to a software component called Policy Decision Point (PDP) that evaluates the request against the given access control policies and provides permit or deny decisions accordingly. ABAC designed using XACML defines the following possible states of allowing access of EHR to the legitimate users:

Definition 1. An ABAC rule r states: if C then E, i.e. if condition C is satisfied the Effect E is permitted. For ex. *if the access control policy of specialist enlists a rule permitting write operation on the patient's diagnostic records and condition defined allows a write access to the specialist, the decision would be permit.*

Definition 2. An ABAC rule r states: if S and R then E, i.e. *if attribute values of both subject S and resource R is satisfied, the Effect E is permitted.* For ex. if the policy rule allows the Family doctor unconditional access to the Clinical records of the patient, and no property is defined to restrict such access, the decision would be permit.

The above definitions can be expanded to include more relationships between various other components in rule-sets. The problem is that these definitions do represent clear and simple integration of various policies but encompass policy conflicts and rule redundancies. Thus, fine-graining of policies is needed so as to restrict undue disclosure of sensitive health records especially in interoperable environment.

Implementation of proposed framework:

1. Categorizing the rules
   Primarily there are two rules termed as Permit Rules (PR) and Deny Rules (DR). Access control policies comprise PR for permit decisions and DR as denial decisions for

[1] Hierarchy Similarity Analyzer.
[2] Security_Level.

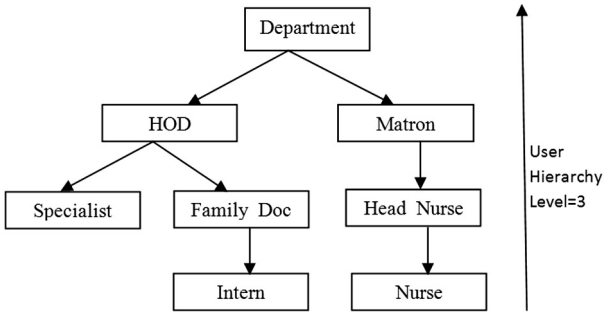

Figure 2 User hierarchy in healthcare domain.

each rule accordingly. Each rule is checked against Effect (E) and store the valid permit and deny rules of all policies participating to share the data.

2. Identifying attribute and assigning them values
   Each PR or DR rule contains attributes $\{a_1, a_2, a_3 \ldots.\}$ having values $(v_{i1}, v_{i2,\ldots\ldots}, v_{in})$ that are of two types-categorical or numerical. For instance, an attribute 'Role' of element Subject contains values like Family_Doc, Matron, and Patient that belong to categorical type. All integers or date/time type values belong to the numeric type like time from 8.00 to 16.00.
3. Calculating the similarity score for attributes with categorical values
   The hierarchical distance between two categorical attributes is calculated for each value of attributes (a_1, a_2) to find the shortest path ($SPath(v_1, v_2)$, Eq. (1)) in the hierarchy (Figs 2 and 3). A compensating score δ is calculated (Eq. (2)) as an average similarity score for all unmatched attributes.

$$S_{cat}(v_{1k}, v_{2l}) = 1 - \frac{SPath(v_{1k}, v_{2l})}{2H} \tag{1}$$

where $SPath(v_{1k}, v_{2l})$ denotes the length of the shortest path between two values v_{1k}, v_{2l} of attributes$(a1, a2)$ in P1 and P2 respectively, and H is the height of the domain hierarchy.

$$\boldsymbol{\delta} = \begin{cases} I\dfrac{\sum_{(v_{1k,-}) \in M_v} \sum_{l=1}^{N_{v_2}} S_{\text{cat}}(V_{1k}, V_{2l})}{N_{v_2}}, & N_{v_1} > N_{v_2} \\ \dfrac{\sum_{(-,v_{2l}) \in M_v} \sum_{k=1}^{N_{v_1}} S_{\text{cat}}(V_{1k}, V_{2l})}{N_{v_1}}, & N_{v_1} < N_{v_2} \end{cases} \tag{2}$$

4. Calculating the similarity score for attributes with numerical valuesThe similarity of two numerical attribute values (v_1, v_2) is based on the difference between the two values. The hierarchical distance between two numerical attributes is calculated for each value using Eq. (3). A compensating score δ is calculated (Eq. (4)) as an average similarity score for all unmatched numerical attributes.

$$S_{num}(v_1, v_2) = \frac{|v1 - v2|}{\max(v1, v2)} \tag{3}$$

$$\boldsymbol{\delta} = \begin{cases} \dfrac{\sum_{(v_{1k,-}) \in M_v} \sum_{l=1}^{N_{v_2}} S_{\text{num}}(V_{1k}, V_{2l})}{N_{v_2}}, & N_{v_1} > N_{v_2} \\ \dfrac{\sum_{(-,v_{2l}) \in M_v} \sum_{k=1}^{N_{v_1}} S_{\text{num}}(V_{1k}, V_{2l})}{N_{v_1}}, & N_{v_1} < N_{v_2} \end{cases} \tag{4}$$

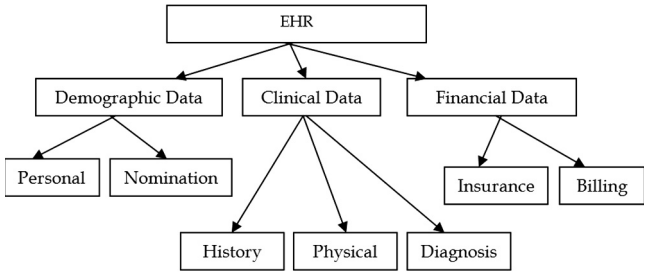

Figure 3 Resource hierarchy in healthcare domain.

5. Implementation of Hierarchy Similarity Analyzer(HSA) algorithm
   Implementation of HSA can be well understood through the flowchart shown in (Fig. 4). After evaluating the positional distances in the observed hierarchies through $s_{cat}(v_1, v_2)$ and $S_{num}(v_1, v_2)$, multiple similarity score are obtained for similar rule attributes of disparate policies. Average of similarity score is then calculated for each attribute values. A unique set of similarity scores is generated and stored in 1-D array. Accordingly assign Security_Level (SL) to the Subject and Resource attribute of each PR (DR) rules in the given policies.

It is assumed that A can return unique set of values irrespective of the type of array i.e. categorical or numerical array. A is an intersection of rows and columns and a similar set of rows and columns are returned in C in sorted order. S returns the position of each value in the array A which is used to assign the unique values obtained in C accordingly.

The above framework can be implemented for any operational scenario and case study is considered where three units of hospital are interacting for sharing of document. The framework is compared with traditional centralized and distributed environment where HSA is not implemented.

4. Operational scenario

Each organization has its own set of guidelines for framing the access control policies for its users. A case is taken where a patient's diagnostic data needs to be accessed by a physician belonging to some other healthcare organization. The health professionals considered for this case study are: Patient, Family Doctor alias attending physician, HOD and Nurse. For identifying the robustness of our framework, three policies are designed in ACPT for each model, i.e. centralized, decentralized and HSA-refined access control framework. A property or a query is generated that is then inputted in all the three models. Figs. 5–7 illustrates the integration of varied policies in each model.

Each hospital unit has users sub-divided into various roles as shown in Fig. 2. One of the hierarchies consists of HOD managing doctors and interns. Other hierarchy identifies paramedical staff headed by Matron. Patient moves in various departments and uses facilities during his visit to the hospital.

Fig. 3 represents the EHR hierarchy assumed to be the same in all hospitals. EHR hierarchy is broadly categorized in three heads, personal, clinical and billing heads. The personal head is represented as '*demographic data*' holding

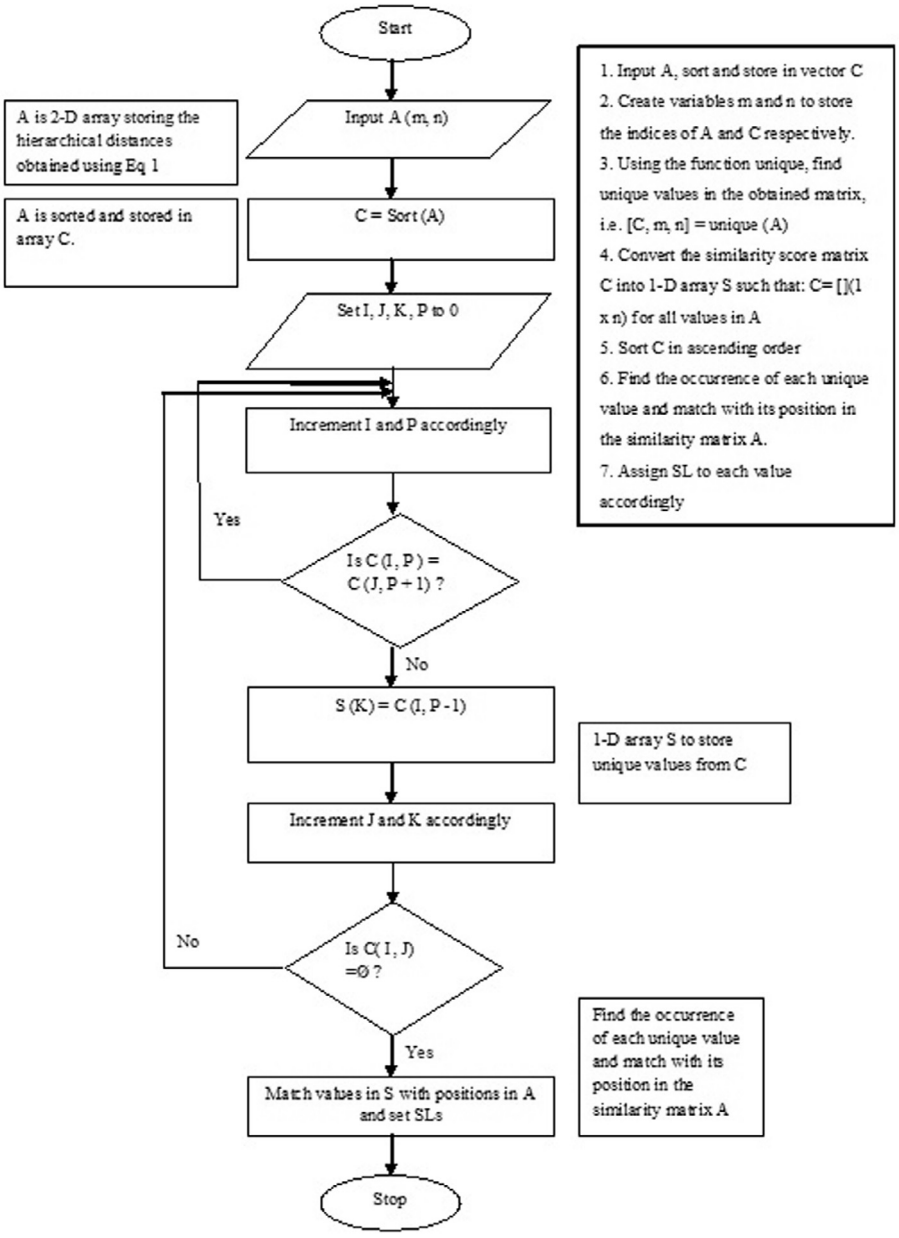

Figure 4 Implementation of HSA-based approach of securely sharing EHR in interoperable environment.

patient's personal and nominee's details. The Clinical head groups the symptoms, laboratory tests, reports and prescriptions under different heads. All billing and insurance details are stored under Financial head.

The user and resource hierarchies in Figs. 2 and 3 are used to define access control policies in centralized, decentralized and HSA-based approaches. Each attribute of a rule in one policy is matched with similar attribute of a rule in other policies within the same approach. Specifically for HSA-based approach, similarity (Range 0–1) is obtained for all attributes exhibiting similar rules in the given policies (P1, P2, P3). Similarity score is converted into security level and assigned to each user/resource attribute defined in the respective rule. The lowest SL begins at value 1 chronologically increasing with higher scores. Evaluating the rules further generates the specific and only relevant rules that meet the specified conditions. One of the hierarchical similarities in the Subject attribute that is categorical type is shown in Table 2.

In order to evaluate the Compensating score δ for non-matching attributes the highest similarity score in $v12$, $v21$, $v31$ (0.66) and $v13$, $v21$, $v31(0.83)$ is considered and δ is obtained. Compensating scores for non-matching attributes in other rules are evaluated similarly.

To simplify the calculations, the similarity scores are converted into integers starting from 1. For instance, the similarity score between different roles in P1, P2 and P3 is 1, 0.83 and 0.67 which is simplified and converted to 3, 2 and 1 respectively. Wherever, no similarity is obtained, the value assigned to SL is 0. The results shown are confined to only those rules that are affected on generation of the request.

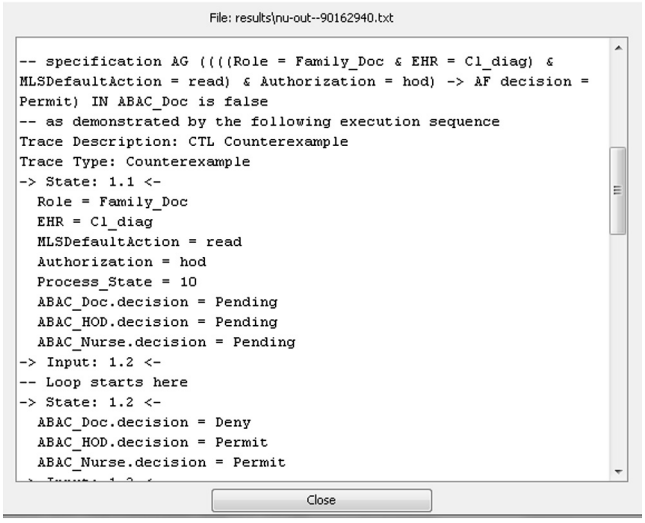

Figure 5 NuSMV verification for centralized access control policy set.

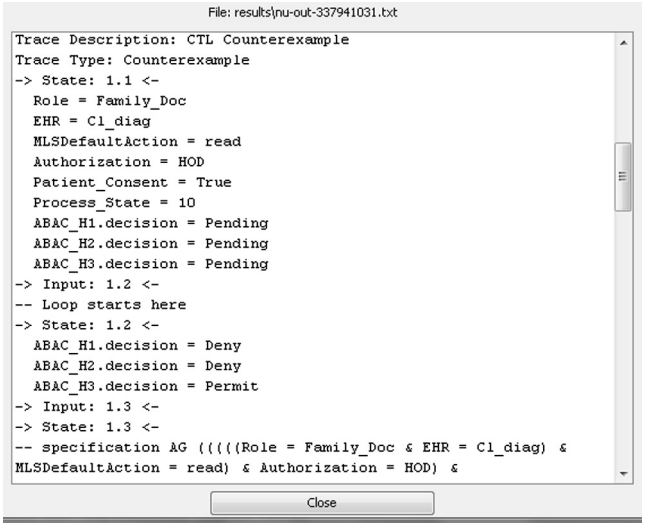

Figure 6 NuSMV verification for decentralized access control policy set.

4.1. Assigning Security_Level (SL) using HSA

HSA is implemented using MatLab, an analytical rule and Security Levels are obtained. SLs assigned to user attribute in all the rules of each policy are shown in Table 3. Precedence of P1 in P2 and P3 and vice versa is checked while assigning the SL to the user or resource attributes for each PR (DR) rules in all the policies.

5. Implementation of HSA

The proposed framework is implemented to identify and eliminate irrelevant roles and unauthorized exposure of data resulting from merging of disparate policies. Analysis focuses on

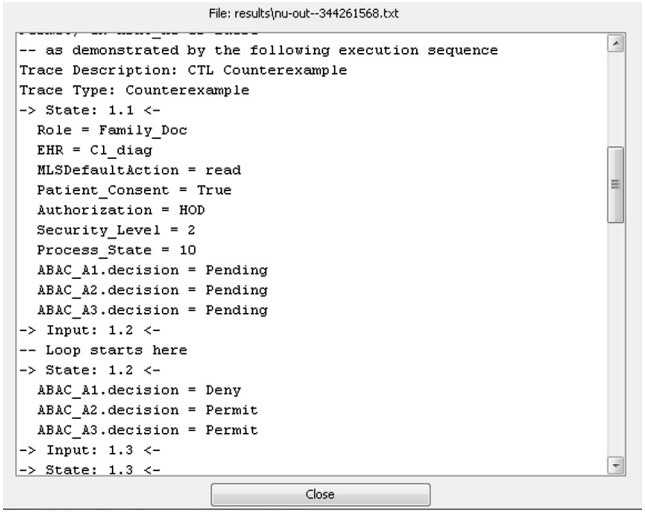

Figure 7 NuSMV verification for HSA-refined policy set.

Table 2 Similarity score between subjects' attributes of P1, P2 and P3.

		*v*11 (HOD)	*v*12 (Nurse)	*v*13 (Family_Doc)
*v*31 (HOD)	*v*21 (HOD)	1	.66	.83
	*v*22 (Nurse)	.66	.66	.50
	*v*23 (Family_Doc)	.83	.50	.83
*v*32 (Nurse)	*v*21 (HOD)	.66	.66	.50
	*v*22 (Nurse)	.66	1	.83
	*v*23 (Family_Doc)	.83	.67	.83
*v*33 (Family_Doc)	*v*21 (HOD)	.83	.50	.83
	*v*22 (Nurse)	.50	.83	.67
	*v*23 (Family_Doc)	.83	.83	1

Absolute similarity pair: $(v11, v21, v31)$, $(v12, v22, v32)$, $(v13, v23, v33)$.

Table 3 Assigning SL to user attribute.

	HOD	Nurse	Family_Doc
HOD	3	2	1
Nurse	2	3	1
Family_Doc	1	1	3

correctness and ability of the policies allowing secured sharing of sensitive data to only the legitimate and authorized users. Access Control Policy Testing (ACPT) tool (Hwang et al., 2010) developed by NIST allows to simulate different policies in different environments. It is cross-platform compatible and written in Java. NuSMv (Cimatti et al., 2002), a verification tool is integrated in ACPT that specifies how a particular rule

complies. NuSMV takes into account the defined or set states and the specified properties as input. NuSMV is linked to a MiniSat SAT solver to detect and falsify defined properties through the generation of counterexample for predefined set of states. Counterexamples illustrate semantic differences between the two policies. More specifically, each counterexample represents a request that evaluates to a different response when applied to selected policy versions.

5.1. Policy coverage

In policy testing, a request is provided as test input that generates matching and non-matching access rules as test outputs. XACML policies comprise of three major components: Policies, Rules and Conditions. A policy tester must thrive to generate requests that achieve 100% policy, rule and condition coverage. The coverage (Martin and Xie, 2007) is defined as the possibility of the stated component contributing to the decision obtained on the generated request.

5.1.1. Policy coverage

The number of policies under test divided by the total number of policies existing in the given environment.

5.1.2. Rule coverage

The number of rules corresponding to the request made divided by the total number of rules existing in the given environment.

5.1.3. Condition coverage

The number of Boolean conditions involved for the policies and rules under test divided by two times the number of conditions.

ACPT is capable to fulfill all three requirements. As multiple rules generate multiple decisions for the same request due to rule overlapping, ACPT specifies the precedence between rules by providing rule combination algorithms, namely, first applicable, permit override and deny override to choose from. First-applicable follows the decision in the first rule to report permit or deny. In Permit override, permit decision takes precedence whereas in Deny override, deny decision takes the precedence.

The framework is verified and tested against policy conflicts and undefined resource access using any of these algorithms. First Applicable Rule combining algorithm is adopted to derive the verification decisions on merging of two policies. It produces verification reports where if the property is true in the policy no test cases are generated. On the other hand if the property is violated, counterexamples are generated.

5.2. Property verification

ACPT generates a query to be verified against the property defined for the policy(s) under test. More generally, it is a method of investigating the behavior of the policy. Though, it is not mandatory to define property for every generated query, due to the large and complex policy rules, it becomes difficult to handle and trace faults leading to security gaps in the existing policy(s). The problem becomes graver when two or more policies are integrated under imposed constraints or conditions.

5.2.1. Centralized access control framework

Centralized access control framework: The healthcare professionals are assigned with a predefined set of access rights. A central manager assigns the authorizations for allowing/denying the access of data among the fellow professionals inside or outside the organization. The access rights are static and updated by the central manager on request of the concerned user. Fig. 5 shows the NuSMV result obtained on verifying the said property applied on three independent policies (P1, P2 and P3 (Fig. 11: Appendix A)) controlled by a central manager. Policy P2 and P3 permits the access of requested data to the intended user whereas policy P1 exhibits conflicting rules resulting in denial of access to the requested data.

Property: *SPEC (Role = Family_Doc) & (EHR = Cl_diag) & (MLSDefaultAction = read) & (Authorization = hod) -> decision = Permit.*

5.2.2. Decentralized access control framework

Decentralized access control framework: The health professionals are assigned with a predefined set of access rights. Access rights and authorizations for the users are set by each local manager under its hierarchy. Change to access rights is locally handled enabling quick access to the required data. Integration of disparate access control policies of three organizations (H1, H2 and H3 (Fig. 10: Appendix A)) is shown in Fig. 6. Access control policy of H3 results in permitting the access of the required data whereas policy conflicts are identified in H1 and H2.

Property: *SPEC (Role = Family_Doc) & (EHR = Cl_diag) & (MLSDefaultAction = read) & (Authorization = HOD) & (Patient_Consent = True) -> decision = Permit.*

5.2.3. HSA refined policy set Hierarchy Similarity Analyzer

The health professionals are assigned with a set of access rights either by central manager or a local manager as per the approach followed in the organization. The user and resource hierarchies of the organizations is provided to HSA that assigns a security level (SL) for each user and resource attribute in the given access control policies. The policies are further refined by setting up of authorization ascertaining permit/deny of data in interoperable healthcare environment. Fig. 7 shows the results generated on integrating access control policies of three different organizations (A1, A2, A3 (Fig. 9: Appendix A)). On merging, policies of A2 and A3 represent more similarity allowing access to the requested data as compared with policy of A1 contradicting in terms of the generated query.

Property: *SPEC (Role = Family_Doc) & (EHR = Cl_diag) & (MLSDefaultAction = read) & (Patient_Consent = True) & (Authorization = HOD) & (Security_Level = 2) -> decision = Permit.*

5.3. Interpretation

A query is generated to identify the robustness and exactness of each model when merged in interoperable environment. The query bounds the policies for finding the exact match by iterating into entire rule-sets. The property is verified using a 3-way covering array that generates test cases based on the first-applicable policy combining algorithm. Table 4 identifies

Table 4 Rules obtained on merging policies in each approach.

Approach	Role	Authorization	SL	Privilege	Permit in P1	Permit in P2	Permit in P3	Decision
Centralized	Nurse	Family_Doc	–	Read	False	False	True	Permit
	Family_Doc	Patient	–		True	False	False	Permit
	HOD	HOD	–		False	True	False	Permit
Decentralized	Patient	Patient	–	Read	True	Undefined	Undefined	Deny
	Family_Doc	Family_Doc	–		True	False	Undefined	Deny
	HOD	Family_Doc	–		True	Undefined	False	Deny
HSA	Patient	HOD	1	Read	Undefined	Undefined	Undefined	Deny
	Family_Doc	HOD	2		False	True	True	Permit
	Family_Doc	Family_Doc	2		True	False	False	Deny
	Family_Doc	HOD	3		False	False	True	Deny
	Family_Doc	Patient	3		True	False	False	Deny

policy-conflicts arising on merging disparate access control policies. Access model based on centralized approach is most vulnerable permitting the access to the data in-spite of non-matching rules in the merged policy-set. Decentralized approach based model depicts non-similarities in the merged policies resulting into non-availability of access, hence, delaying quality treatment to the patient. Authorizations are set between various healthcare systems but are cost-extensive while resetting dynamically. HSA-based model identifies strong similarities between policies P2 and P3. Authorizations are dynamically set between various healthcare systems and the overhead of any change in the security level and authorizations correlates with the change in user or resource hierarchies. The authorizations are set in one or the other policy affecting the confidentiality and privacy of EHRs when shared in an open environment. Table 4 shows the vulnerabilities that either result in no or undue disclosure of data. Moreover, centralized approach defines implicit or static environmental settings. Incorporating changes to achieve interoperability is very difficult and time-consuming. Centralized approach exhibits highest confidentiality in single environment. The confidentiality is compromised when the policies under this approach merged to allow sharing in disparate healthcare environment. Organizations following decentralized approach are not bounded to follow any standard rules and guidelines in framing access rules, hence, results in stringent security measures denying access to the required data. The availability of data is highly affected in this approach. HSA-based models fine-grains the existing poli-

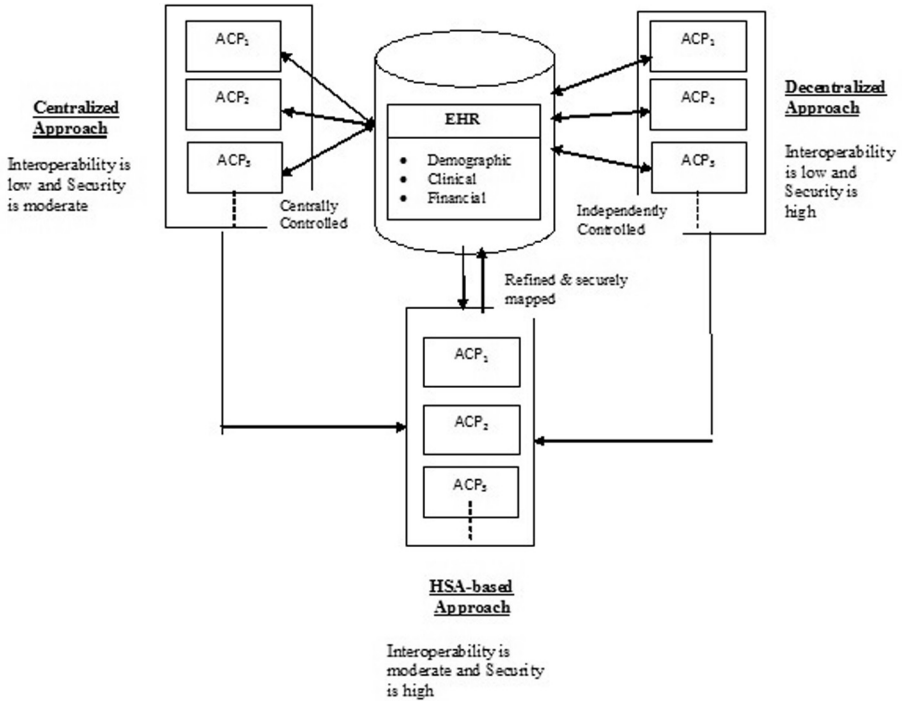

Figure 8 Verifying interoperable sharing of EHR in various approaches.

cies dynamically deciding the amount of data allowed to be accessed by the legitimate users. The confidentiality and availability of data is higher than the other two approaches. Policy-conflicts are minimized through clearly defined authorizations that are dynamically set according to the responsibilities and accountability of the concerned user.

Merging of P1, P2 and P3 in each access model approach reveals substantial decisions for allowing or denying access

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" PolicySetId="CombinedPolicySet"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable">
<Policy PolicyId="A1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
<!--## POLICY START1-->
<!-- ABAC Model: A1-->
    <Rule RuleId="rule_1" Effect="Permit">
     <Target>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
     </Target>    <Condition>          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment" AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Security_Level"  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">3</AttributeValue>
    </Condition>      </Rule>
  <Rule RuleId="rule_3" Effect="Permit">
    <Target>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
     </Target>          <Condition>
       <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Security_Level"  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
    </Condition>      </Rule>
   <Rule RuleId="rule_4" Effect="Permit">
    <Target>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
     </Target>          <Condition>
       <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">HOD</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Security_Level"  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">1</AttributeValue>
    </Condition>      </Rule>          </Policy>      <!--## POLICY 1 END-->
<!--## POLICY 2 START-->
<!-- ABAC Model: A2-->
    <Rule RuleId="rule_5" Effect="Permit">
     <Target>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
```

Figure 9 HSA-refined XACML policies of three disparate healthcare organizations.

```
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
        </Target>              <Condition>
         <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
               <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
              <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Security_Level"  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">3</AttributeValue>
     </Condition>       </Rule>
    <Rule RuleId="rule_7" Effect="Permit">
     <Target>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
     <Condition>
         <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Security_Level"  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">1</AttributeValue>
          </Condition>              </Rule>
    <Rule RuleId="rule_8" Effect="Permit">
     <Target>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
      </Target>           <Condition>
         <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">HOD</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Security_Level"  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
        </Condition>              </Rule>           </Policy>       <!--## POLICY 2 END-->
<!--## POLICY 3 START-->
<!-- ABAC Model: A3-->
    <Rule RuleId="rule_9" Effect="Permit">
     <Target>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
      </Target>           <Condition>
         <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Security_Level"  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">1</AttributeValue>
     </Condition>       </Rule>
    <Rule RuleId="rule_11" Effect="Permit">
     <Target>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
```

Fig. 9 (*continued*)

```
      </Target>     <Condition>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">HOD</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Security_Level"  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
      </Condition>      </Rule>            </Policy>        <!--## POLICY 3 END-->
</PolicySet>
```

Fig. 9 (*continued*)

to the data. In the centralized approach, for instance (highlighted in Table 4), access of the queried data is permitted to nurse in P3 only whereas the decision applies to all the policies merged together. It risks the data to undue disclosure and confidentiality breaches. In certain cases, Health Insurance Portability and Accountability Act (HIPAA, 1996) overrides sharing of records between various agencies even if patient's consent is not available. The verification result identifies such vulnerabilities if existing in the rule sets as shown in Table 4. Decentralized approach on the other hand presents a more stringent security model where only if similar rules exist in each policy, the decision would be permit otherwise it would result in denial of access. The contradiction and policy-conflict are handled by simply denying an access to the data like property stands true in P1 but still the decision is deny. This model has a high rating on maintaining the confidentiality and privacy of data, but lacks timely availability of data that is most crucial with respect to healthcare domain. The decisions obtained for HSA-refined policy identifies denial even when the patient's consent is true and the authorization is HOD. It restricts unauthorized disclosure thereby maintaining confidentiality and privacy and at the same time ensuring availability of data. The verification results detects possible policy-conflicts prevailing in HSA-refined policy set and also provide counter examples to mitigate these conflicts. Thus, our framework proves to strengthen the security policies in dynamic sharable interoperable healthcare environment.

6. Conclusion

Access control policies of three healthcare units incorporating unique access approaches are compared and verified with an objective of achieving secured integration and sharing of EHRs to relevant users. Permit/deny decision are obtained on merging of relevant rules. The framework bridges the interoperable gaps between independent healthcare organizations by ranking user/resource attributes on a similarity factor. Similarity score basically promises to produce justifiable subsets of matching rules and policies for the purpose of sharing data between independent healthcare units. The security level ascertains authorizations that ensure only legitimate and authorized users would be able to access controlled data especially while dynamically collaborating in different environments. Further the framework identifies policy-conflicts popped up on merging of two or more policies. Table 4 identifies the rules resulting in policy conflicts as they contradict with the defined property that impose a conditional constraint allowing the access only when authorization is HOD. The interoperability and security factors are compared (Fig. 8) with respect to sharing of EHR in the discussed approaches. HSA proves to achieve interoperability without compromising the security of data when shared in disparate environments. Also, HSA prevents and eliminates such rules thus minimizing policy conflicts that too are traceable. This justifies the robustness of the proposed framework. Moreover, if the rules obtained on the generated request are not defined in some policies, there exists no difference in decision-making and originality of such policies. Hence, our framework is an extension over the already deployed security stature in an organization.

6.1. Future Scope

The current work enables integration of access control policies of independent healthcare units in a secured manner. Policy-conflicts are detected and removed from final selection of rules permitting/denying access to the required data. The work can be extended to incorporate various types of policy-conflicts categorized into semantic, syntactic, temporal constraints. Further, access to EHR can be categorized on the basis of requirements for different purposes such as, emergencies and contingencies. Federated agencies like HIPAA also propose the guidelines for designing of access control models encompassing well-defined authorizations to handle such cases. Handling of these cases without losing confidentiality and privacy of the records is a major area requiring a robust mechanism satisfying healthcare conditions and course of actions.

Appendix A

XACML Policies in centralized, decentralized and HSA-refined access control policies: Each policy is reduced to show only the rules relevant to the property defined in the paper.

1. HSA-refined policies (P1, P2 and P3) of three disparate healthcare organizations (See Fig. 9).
2. Decentralized approach: Policies (P1, P2 and P3) of three disparate healthcare organizations (See Fig. 10).
3. Centralized approach: policies (P1, P2 and P3) of intra-healthcare units (See Fig. 11).

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" PolicySetId="CombinedPolicySet"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable">
    <Policy PolicyId="H1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable">
<!--## POLICY START1-->
<!-- ABAC Model: H1-->
          <Rule RuleId="rule_2" Effect="Permit">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
      <Condition>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
      </Condition>       </Rule>
    <Rule RuleId="rule_4" Effect="Permit">
      <Target>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">HOD</AttributeValue>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
       </Target>           <Condition>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
      </Condition>                  </Rule>
    <Rule RuleId="rule_6" Effect="Permit">
      <Target>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Nurse</AttributeValue>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
       </Target>           <Condition>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Patient_Consent"  DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">True</AttributeValue>
     </Condition>       </Rule>            </Policy>
<!--## POLICY 1 END-->
<!--## POLICY 2 START-->
<!-- ABAC Model: H2-->
   <!--## POLICY 2 END-->
<!--## POLICY 3 START-->
         <Target/>
<!-- ABAC Model: H3-->
          <Rule RuleId="rule_13" Effect="Permit">
      <Target>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
       </Target>           <Condition>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">HOD</AttributeValue>
     </Condition>       </Rule>            </Policy>
<!--## POLICY 3 END-->
</PolicySet>
```

Figure 10 XACML policies of three disparate healthcare organizations in decentralized approach.

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" PolicySetId="CombinedPolicySet"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable">
    <Policy PolicyId="Doc" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable">
<!--## POLICY START1-->
<!-- ABAC Model: Doc-->
    <Rule RuleId="rule_1" Effect="Permit">
     <Target>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
     </Target>
     <Condition>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
    </Condition>      </Rule>                    </Policy>
<!--## POLICY 1 END-->
<!--## POLICY 2 START-->
<!-- ABAC Model: HOD-->
    <Rule RuleId="rule_6" Effect="Permit">
     <Target>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">HOD</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
     <Condition>
       <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">hod</AttributeValue>
    </Condition>                </Rule>
    <Rule RuleId="rule_7" Effect="Permit">
     <Target>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
     </Target>                <Condition>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">hod</AttributeValue>
    </Condition>                </Rule>            </Policy>
<!--## POLICY 2 END-->
<!--## POLICY 3 START-->
  <!-- ABAC Model: Nurse-->
    <Rule RuleId="rule_10" Effect="Permit">
     <Target>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Nurse</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
     </Target>                <Condition>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
    </Condition>                </Rule>
    <Rule RuleId="rule_11" Effect="Permit">
     <Target>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Family_Doc</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Cl_diag</AttributeValue>
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
    </Target>                <Condition>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="Authorization"  DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">hod</AttributeValue>
    </Condition>      </Rule>            </Policy>
<!--## POLICY 3 END-->
</PolicySet>
```

Figure 11 XACML policies of three healthcare units in centralized approach.

References

Al-Abdulmohsin, I.M., 2009. Techniques and algorithms for access control list optimization. Comput. Electr. Eng. 35 (4), 556–566.

Azeez, N.A., Venter, I.M., 2013. Towards ensuring scalability, interoperability and efficient access control in a multi-domain grid-based environment. SAIEE Africa Res. J. 104 (2), 54–68.

Bertino, E., Kim, W., Rabitti, F., Woelk, D., 1994. A model of authorization model for object-oriented databases, In: Biskup, J., Morgenstern, M., Landwehr, C.E. (Eds.), Database Security, vol. VIII, pp. 199–222.

Bhartiya, S., Mehrotra, D., 2013. Exploring Interoperability and Challenges in Healthcare Data Exchange. In: Smart Health, International Conference, ICSH 2013 Proceedings, Lecture Notes in Computer Science, 8040, pp. 52–65

Bhartiya, S., Mehrotra, D., 2015. Applying CHAID Algorithm to Investigate Critical Attributes of Secured Interoperable Health Data Exchange. Int. J. Electronic. Healthcare 8 (1), 25–50.

Carmagnola, F., Cena, F., Gena, C., 2000. User model interoperability: a survey. User Model. User-Adapted Interact. 21 (3), 285–331.

Chandramouli, R., 2000. Business process driven framework for defining an access control service based on roles and rules. In: Proc. of 23rd National Information Systems Security Conference.

Ciampi, M., Gallo, L., Coronato, A., Pietro, G.D., 2010. Middleware mechanisms for interaction interoperability in collaborative virtual environments. Int. J. Adv. Media Commun. 4 (2), 154–166.

Cimatti, A., Clarke, E., Giunchiglia, E., Giunchiglia, F., Pistore, M., Roveri, M., Sebastiani, R., Tacchella, A., 2002. NuSMV, Version 2: An OpenSource Tool for SymbolicModel Checking, In: Proc. 14th International Conference on Computer-Aided Verification (CAV), pp. 359–364.

Fisler, K., Krishnamurthi, S., Meyerovich, L.A., Tschantz, M. C., 2005. Verification and change-impact analysis of access-control policies, In: Proc. of the 27th Int. Conference on Software Engineering, pp. 196–205.

Health Insurance Portability and Accountability Act of 1996., 1996. PUBLIC LAW 104–191.

Hu, V.C., Kuhn, D.R., 2011. Model checking for verification of mandatory access control models and properties. Int. J. Software Eng. Knowl. Eng. 21 (1), 103–127.

Hu, V., Schnitzer, A., Sandlin, K., 2013. Attribute based access control definition and considerations. NIST Spec. Publ., 800-162

Hwang, J., Xie, T., Hu, V., Altunay, M., 2010. ACPT: A Tool for Modelling and Verifying Access Control Policies.

Karp, A.H., Haury, H., Davis, M.H., 2010. From ABAC to ZBAC: The Evolution of Access Control Models. In: Proc. of the International Conference on Information Warfa, Vol. 202.

Koleini, M., Ryan, M., 2011. A knowledge-based verification method for dynamic access control policies. In: Proceedings of 13th International Conference on Formal Engineering Methods (ICFEM 2011).

Lin, D., Rao, P., Bertino, E., Lobo, J., 2007. An Approach to Evaluate Policy Similarity. In: Proc. of 12th ACM symposium on Access control models and technologies, pp. 1–10.

Martin, E., Xie, T., 2007. Automated test generation for access control policies via change-impact analysis. In: Proceedings of the Third International Workshop on Software Engineering for Secure Systems. IEEE Computer Society, p. 5.

Nyanchama, M., Osborn, S.L., 1999. The role graph model and conflict of interest. ACM Trans. Inf. Syst. Secur. 2 (1), 3–33.

Sandhu, R.S., Coyne, E., Feinstein, H.L., Youman, C.E., 1996. Role based access control models. Comput. Secur. 29 (2), 38–47.

Saltman, RB., Bankauskaite, V., Vrangbaek, K., 2007. Decentralization in Healthcare-Strategies and Outcomes. European Observatory on Health Systems and Policies Series. McGraw Hills, Open University Press, ISBN 0 335 21925 X (pb) 0 335 21926 8 (hb).

Xiao, L., Hu, B., Croitoru, M., Lewis, P., Dasmahapatra, S., 2009. A knowledgeable security model for distributed health information system. Comput. Secur. 29, 331–349.

Yang, N., Barringer, H., Zhang, N., 2008. A purpose-based access control model. J. Inf. Assur. Secur., 51–58

Zidat, S., Djoudi, M., 2006. Task collaborative resolution tool for elearning environment. J. Comput. Sci. 2, 558–564.