ACKNOWLEDGEMENTS

I would like to first of all acknowledge Almighty God who gave me HIS abundance grace to complete my research work. HE gave me wisdom, understanding and knowledge.

I am heartily indebted to my Gurus Dr. Deepti Mehrotra and Dr Anup Girdhar. First and foremost I offer my sincerest gratitude to my Guide Dr Deepti Mehrotra, who has supported me throughout my thesis work with her patience, guidance and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D work.

I extend my gratitude to Dr. Ashok K. Chauhan, Founder President- Amity under whose benign umbrella we are flourishing. Shri. Atul Chauhan, Chancellor AUUP, whose passion for excellence has inspired many and Prof. (Dr.) Balvinder Shukla, Vice Chancellor AUUP for designing flawless processes to make the academic pursuit unproblematic. A special thanks to my existing employers, IITM, for their immense support in pursuing my research.

I am indebted to healthcare institutions and health practitioners for extending their support and opinions during my research work. A special mention, to Dr. Vincent Hu, NIST, who provided an access to the ACPT tool for verification of the proposed framework. My friends and well-wishers who always encouraged me and were positive about my work, I am thankful and grateful one and all who had immense faith in me, to all my contributors who helped me directly or indirectly with their words of encouragement and knowledge sharing.

I would like to thank my husband Dr. Manish Bhartiya, my joy of life; my children, and above all my parents and parents-in-law for the unceasing encouragement, support and belief in me.

SHALINI BHARTIYA
Chapter 1
1. Introduction
   1.1 Major Security Aspects to EHR Sharing
      1.1.1 Interoperability
      1.1.2 Confidentiality
      1.1.3 Integrity
      1.1.4 Availability
   1.2 Rationale of the Study
   1.3 Objectives
Chapter 2
2. Literature Review
   2.1 Dimensions of Interoperability
   2.2 Need of Interoperability in EHR
   2.3 Challenges to EHR sharing in Interoperable Environment
   2.4 Architectures and Models achieving interoperability
   2.5 Data Exchange Mechanisms
      2.5.1 Data Exchange Standards
      2.5.2 Standardization of EHR
      2.5.3 EHR Exchange Standards
      2.5.4 Technical Interoperability Standards for EHR
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6 Recommendations and Proposed Policy Decisions</td>
<td>2-25</td>
</tr>
<tr>
<td>2.7 Security of EHR</td>
<td>2-29</td>
</tr>
<tr>
<td>2.7.1 Related Study</td>
<td>2-30</td>
</tr>
<tr>
<td>2.7.2 Security Controls</td>
<td>2-30</td>
</tr>
<tr>
<td>2.7.3 Security Gaps</td>
<td>2-31</td>
</tr>
<tr>
<td>2.8 Summarization</td>
<td>2-32</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>3-33</td>
</tr>
<tr>
<td>3. Study of Current Scenario</td>
<td>3-33</td>
</tr>
<tr>
<td>3.1 Accessibility Issues- Physician’s Perspective</td>
<td>3-37</td>
</tr>
<tr>
<td>3.1.1 Methodology</td>
<td>3-37</td>
</tr>
<tr>
<td>3.1.2 Implementation and Results</td>
<td>3-42</td>
</tr>
<tr>
<td>3.2 Identifying dependencies between security parameters using CHAID</td>
<td>3-52</td>
</tr>
<tr>
<td>3.2.1 Literature Review</td>
<td>3-54</td>
</tr>
<tr>
<td>3.2.2 Methodology</td>
<td>3-57</td>
</tr>
<tr>
<td>3.2.3 Security Parameters</td>
<td>3-58</td>
</tr>
<tr>
<td>3.2.4 Classification Technique- CHAID</td>
<td>3-62</td>
</tr>
<tr>
<td>3.2.5 Interpretation of Generated Classification Hierarchies</td>
<td>3-64</td>
</tr>
<tr>
<td>3.2.6 Summarize</td>
<td>3-71</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>4-73</td>
</tr>
<tr>
<td>4. Designing of Framework</td>
<td>4-73</td>
</tr>
<tr>
<td>4.1 Access Control Models</td>
<td>4-74</td>
</tr>
<tr>
<td>RBAC in Healthcare Environment</td>
<td>4-76</td>
</tr>
<tr>
<td>4.2 Identifying the most suitable Access Control Model using Fuzzy TOPSIS</td>
<td>4-79</td>
</tr>
<tr>
<td>4.2.1 Alternatives</td>
<td>4-82</td>
</tr>
<tr>
<td>4.2.2 Criteria</td>
<td>4-82</td>
</tr>
<tr>
<td>4.2.3 MCDM Approach</td>
<td>4-84</td>
</tr>
<tr>
<td>4.2.4 Implementation of Fuzzy TOPSIS in Healthcare Environment</td>
<td>4-86</td>
</tr>
</tbody>
</table>
4.2.5 Observation

4.4 Environment for the Proposed Framework
   4.4.1 XACML Structure
   4.4.2 Attribute based Access Control Model (ABAC)

4.5 Similarity Score Algorithm
   4.5.1 Computational Steps
   4.5.2 Case Study- Calculating Similarity Score between policies of two healthcare units

4.6 Gaps in the existing Algorithm

Chapter 5

5. Proposed Framework
   5.1 Hierarchy Similarity Analyzer
   5.2 Setting Authorizations
   5.3 Significance of the Proposed Framework
   5.4 Operational Scenario
      5.4.1 Interoperable Healthcare Environment

5.5 Verification Tool
   5.5.1 Policy Coverage
   5.5.2 Rule Combining Algorithms
   5.5.3 Property Verification

Chapter 6

6. Implementation

6.1 Implementation in Homogeneous Environment
   6.1.1 Case Study
   6.1.2 Verification
   6.1.3 Observation

6.2 Implementation in Heterogeneous environment
   6.2.1 Case Study
List of Figures

Figure 1.1: Stakeholders of Electronic Health Records 1-2
Figure 2.1: Flowchart depicting the categorization of parameters selected for studying Interoperability in Healthcare 2-8
Figure 2.2: Parameters for Interoperable Sharing 2-9
Figure 2.3: Parameters for Challenges to EHR Sharing 2-12
Figure 2.4: Parameters for Interoperability Architectures 2-16
Figure 3.1: Different levels of EHR Communication (Source: [77]) 3-34
Figure 3.2: Frequency of sharing EHR/ Gaining additional Access Permissions 3-43
Figure 3.3: Response time of EHR-System/Level of Satisfaction 3-45
Figure 3.4: Delay in data Access due to Stringent Security Policies 3-47
Figure 3.5: Physician’s Response on Patient Authority of Data 3-49
Figure 3.6: Patients controlling the access to his/her health records 3-66
Figure 3.7: Mandatorily Obtaining Patient’s Consent 3-68
Figure 3.8: Frequent Sharing of EHRs by Doctors 3-70
Figure 4.1: Flowchart for Fuzzy TOPSIS Methodology 4-86
Figure 4.2: Criteria and Alternative Hierarchy Diagram 4-87
Figure 4.3: Sensitivity Analysis obtained on variable-weights of Criteria 4-92
Figure 4.4: XACML Overview (Source: Lorch et al., 2003) 4-94
Figure 4.5: XACML Policy Structure 4-96
Figure 4.6: Flowchart of Rule Similarity Score Computation Algorithm 4-100
Figure 4.7: Organizational Hierarchy in Healthcare Domain 4-107
Figure 4.8: Resource Hierarchy in Healthcare Domain 4-108
Figure 4.9: XACML-based ACP for Hospital A 4-109
Figure 4.10: XACML-based ACP for Hospital B 4-110
Figure 5.1: Proposed Access Control Framework for XACML Policies 5-121
Figure 5.2: HSA Algorithm to obtain Security Level for Health Providers 5-125
Figure 5.3: Algorithm to define Authorization as per the Security level of users and Resource defined in the rule-sets  

Figure 5.4: Integrating policies Pi, Pj and Pk of disparate hospitals  

Figure 5.5: NuSMV CTL Counterexample  

Figure 5.6: NuSMV Verification when the Property is true in the defined policy(s)  

Figure 6.1: ABAC Policies defined using ACPT Tool  

Figure 6.2: XACML Access Control Policy for Lab_Tech in P1  

Figure 6.3: XACML Access Control Policy for Lab_Tech in P2  

Figure 6.4: Data Access between Intra, Inter and Distributed Hospitals  

Figure 6.5: Proposed Framework for fine-graining XACML policies using HSA in heterogeneous systems  

Figure 6.6(a): User Hierarchy in Health Organization H1. (b): User Hierarchy in Health Organization H2  

Figure 6.7: Med_Tech access policy rule in H1  

Figure 6.8: Med_Tech access policy rules in H2  

Figure 6.9: Property Verification Result before applying HSA  

Figure 6.10: Property Verification Result after applying HSA  

Figure 6.11: Implementation of HSA-based Approach of Securely sharing EHR in Interoperable Environment  

Figure 6.12: User Hierarchy in Healthcare Domain  

Figure 6.13: Resource Hierarchy in Healthcare Domain  

Figure 6.14: NuSMV Verification for Centralized Access Control Policy Set  

Figure 6.15: NuSMV Verification for Decentralized Access Control Policy Set  

Figure 6.16: NuSMV Verification for HSA-refined Policy Set  

Figure 6.17: Verifying Interoperable sharing of EHR in various approaches  

Figure 6.18: XACML policies of three healthcare units in centralized approach  

Figure 6.19: XACML policies of three disparate healthcare organizations in decentralized approach  

Figure 6.20: HSA-refined XACML policies of three disparate healthcare organizations  

Figure 7.1: Integration of Policy Conflict Resolution in HSA
Figure 7.2: Detection of the type of policy-conflict 7-187

Figure 7.3: Contradiction: Conflict_Type=Effect for Query Request (Query Id: 1) 7-192

Figure 7.4: Execution of Query_Id=2 7-193
List of Tables

Table 2.1: Generic Architectures to Interoperability Modeled on Healthcare Systems 2-16
Table 2.2: Data Exchange Mechanisms supporting Interoperability 2-20
Table 2.3: National Health Programs for Integrated Health Data Exchange 2-29
Table 3.1: Weight-age of each Security Parameter in the Questionnaire 3-35
Table 3.2: Significance of P-Value in Correlation analysis 3-38
Table 3.3: Categorization and Contribution of each Respondent to the Survey 3-39
Table 3.4: Questionnaire-Detailing of each Security Parameter 3-40
Table 3.5: Opinions(%age) of Physicians agreeing to the stated Hypothesis 3-43
Table 3.6: Responses of Physician under different specialization 3-45
Table 3.7: Delay in availability of data due to Stringent Security Policies 3-46
Table 3.8: Patient having the Ownership of EHR 3-48
Table 3.9: Remote Access Available to various Stakeholders of EHR (HIMSS Survey 2011-2014) 3-52
Table 3.10: Percentage of Security Breaches Observed through HIMSS Survey 3-55
Table 3.11: Cause-Effect Matrix representing the Security Issues in Interoperable Health data sharing 3-56
Table 3.12: Subdivision of Questionnaire based on Categories on Security Concerns 3-58
Table 3.13: Sub-Nodes in each Classification Tree with their Significant Values 3-65
Table 3.14: Significance of Classification Tree for dependent variable-Patient’s Control using T-Test 3-67
Table 3.15: Significance of Classification Tree for dependent variable-Patient’s Consent using T-Test 3-68
Table 3.16: Significance of Classification Tree for dependent variable-Doctors’ Frequent Sharing using T-Test 3-69
Table 3.17: Classification Tree-Doctors’ Frequent Sharing using T-Test 3-71
Table 3.18: Summarized Findings of Classified Dependencies 3-71
Table 4.1: Selection of Access Control Models to be considered as Alternatives 4-80
Table 4.2: Alternatives and criteria Ratings 4-87
Table 4.3: Linguistic Assessment of Each Alternative for each Criterion
Table 4.4: Normalized Fuzzy Decision Matrix
Table 4.5: Weighted Normalized Fuzzy Decision Matrix for Alternatives
Table 4.6: Distance of each alternative from FPIS and FNIS
Table 4.7: Closeness Coefficient for all the alternatives
Table 4.8: Sensitivity Analysis Experiments and Rankings
Table 4.9: XACML Policy Structure
Table 4.10: Hierarchical Distances between Users of A and B
Table 4.11: Similarity Score between Action Attributes in A and B
Table 4.12: Notations (Source: Lin et al. [183])
Table 5.1: Notations/Terminologies for Proposed Framework
Table 6.1: Assigning SL to each Subject Attribute in P1 and P2
Table 6.2: NuSMV verification results before applying HSA
Table 6.3: Verification results on Merging of P1 and Fine-grained P2 Policies
Table 6.4: Notations defining the terms used in the proposed framework
Table 6.5: Similarity Scores of user hierarchies in H1 and H2
Table 6.6: Security_Level (SL) obtained through HSA for each user-pair in H1 and H2
Table 6.7: Permit/Deny Decisions obtained on generated test cases to validate the defined property
Table 6.8: Comparative Study of HSA and other access control frameworks/models
Table 6.9: Similarity Score between Subjects’ Attributes of P1, P2 and P3
Table 6.10: Assigning SL to User Attribute
Table 6.11: Rules obtained on Merging Policies in each Approach
Table 7.1: Hierarchical position obtained from the User Hierarchies of HA and HB.
Table 7.2: Security Level (SL_U) for the users of HA and HB calculated by HSA
Table 7.3: Detection and Resolution of generated policy-conflicts
Table 7.4: Identifying the changes in User’s SL during conflict resolution