Chapter 8

8. Conclusion and Future scope

This research is an effort to reduce the security issues prevalent in sharing of Electronic Health Records in interoperable healthcare environment. The objective is to design a framework for sharing EHR which preserve confidentiality and privacy of EHR from unauthorized and illegitimate access in interoperable environment. This research work is limited to statically determine secured sharing of EHRs between disparate healthcare organizations. The environment considered in study is health units within a hospital (Homogenous) or health units of two disparate hospitals (Heterogeneous).

Gaps in the existing system are identified by both extensive literature survey and study of a real time scenario. Literature survey identified the existing models, mechanisms, standards and vocabularies used for sharing of health records. The study concludes that with all the standards and approaches, there is still a need of customization and user-specific modelling for interoperable health data exchange. The system design should be with accordance to the suitability of environment and its users. Sharing consistent patient information must become more transparent.

Real-time analysis in chapter 3 gives a clear insight towards the difficulties and challenges in enforcing security controls for sharing EHRs. Correlation between standard security parameters and healthcare services and needs was obtained based on doctor’s opinions. Increase in confidentiality inversely affected availability, for instance, is one of the conclusions drawn from this analysis. The analysis was further expanded to include the opinions of various stakeholders with an objective of further strengthening the possible causes and effects weakening security of EHR when shared in interoperable environment. Multi-variant analysis technique, CHAID, is utilized to generate classification trees depicting dependencies of healthcare factors with the security parameters. The study expressed the importance of access control techniques and authorizations as the most important factors that should be addressed and reviewed in every dimension to find their suitability in the aforementioned objective.
Studying and exploring the suitability of various access controls in perspective of health data security is included in chapter 4. Fuzzy TOPSIS, a MCDM approach, utilized for this study reveals ABAC as the most suitable model satisfying the need of the healthcare environment. ABAC allows independent identification and evaluation of each attribute as per the behaviour and constraints set in respective environment. Also, the model has an implicit flexibility in providing access to multiple users in heterogeneous environments. The policies devised in ABAC are designed using XACML that encourages the flexibility and scalability of the model in interoperable environments.

The study of requirements and prerequisites of ABAC and XACML structures enabled to create a basic framework enabling flow of information between two or more healthcare organizations or units. A conceptual approach that identifies similarities between disparate access control policy sets is studied and implemented on a case study of two healthcare units having independent set of access control policies and rules. This signifies higher probability of authorize and permitted access to the resources in independent but collaborative environments. The observations made with respect to the stated problem of research, were confined into properties or constraints quantifying the feasibility and limitations of the similarity approach. As an advantage, similar policies proved to be a good candidate for sharing data in spite of dissimilarities in their rules but limiting the access to relevant and selective data still remains to be resolved. Moreover, equally important was to define an authority for controlling the access between users especially where the data holds higher level of confidentiality.

Considering the limitations and constraints of the tested similarity approach, the framework in figure 5.1 is proposed that devises Hierarchy Similarity Analyser (HSA) algorithm to ensure secured access of sensitive health records by health providers in disparate healthcare organizations. HSA fine-grains existing access control policies and generates security levels for the required attributes, especially, user and resource attributes on the basis of hierarchical distances calculated from the organizational hierarchies of collaborative organizations. The framework is capable to handle variations in user hierarchies but needs to be expanded to include variations in resource hierarchies.

The framework further instigates second level of control through an Authorization algorithm formalizing a user to authorize other users, usually at a lower level, to permit or deny access to the specified resource. With the basic knowledge gathered through the literature review
and surveys, HSA is devised with a belief to achieve the desired objectives laid in the beginning of the research. To reiterate, a secured framework had to be designed for sharing electronic health records of patients among health professionals and simultaneously prevent its confidentiality and privacy during transit in interoperable environment. The argument to prove its feasibility in interoperable healthcare domain is justified using NIST developed testing tool.

The interoperable healthcare environment to implement and test the proposed framework is designed using XACML based healthcare schema and organizational hierarchies (figure 4.7 and 4.8) are designed for users and resources. The verification tool, ACPT designed by NIST is explored to identify the testing environment and designing prerequisites that must be incorporated in access control policies for successful and viable verification of the proposed framework.

The proposed framework is implemented in varied environments and tested accordingly to justify its robustness in achieving the desired objective. Implementation of HSA in homogeneous healthcare environment the user and resource hierarchies of two healthcare units are compared for similarities between their attributes. Table 6.3 represents verification of the policies under the generated request. The results identify rule-reduction and identification of matching and non-matching rules when merged to allow or reuse sharing of records between authorized users of both the health units.

Table 6.7 enlist the results on similar implementation and verification in heterogeneous healthcare environment with disparate user hierarchies but similar resource hierarchies. The framework proves to fine-grains the access control policies and exposes data access to only authorized and legitimate users. Figure 6.11 demonstrates the verification of the framework, centralized and decentralized approach of data storage. The framework adopts the advantages of both the approaches such that if the similarity exist, the rules are matched and if no similarity exists between the rule attributes, counterexamples are generated to statically modify the rule sets, if found feasible.

Dissimilar rules identified on verifying the proposed framework is further fine-grained (figure 7.1) to resolve conflicts arising due to dissimilarities in rule attribute values. Three algorithms are devised for different categories of policy conflicts. The algorithms are tested on access control policies designed in SQL server. The results in table 7.3 handle conflicts
and incorporate it with the proposed framework. It proves to enhance data availability without compromising its confidentiality and privacy, which is an important achievement in healthcare environment. The proposed framework thus proves to be a feasible solution in achieving secured sharing of sensitive health records to only authorized users belonging to disparate healthcare organizations.

**Future Directions**

Our framework handles data that is textual in nature. It can be extended further to incorporate images and scanned reports frequently required by the doctors to diagnose and prescribe appropriate medication. The framework can also be extended to incorporate sharing of health data using cloud computing technologies. A research [219] conducted for sharing EHRs in chronic diseases and finding the feasibility of cloud-based approach strengthens the probability of our belief. Future work needs to incorporate the semantic dissimilarities embedded in distributed and parallel systems that should be handled to achieve scalability and portability of required data across physical boundaries and disparities of healthcare systems. Mobile app is another dominating area in current environment that needs to be explored in making the data available to the health providers under robust authorization and control. The devised framework can be optimized to include larger and complex hierarchies than the one considered in this research.