UNDERSTANDING ATTRIBUTE-BASED ACCESS CONTROL FOR MODELLING AND ANALYSING HEALTHCARE PROFESSIONALS' SECURITY PRACTICES

Project Reference No.: *48S_BE_5438*

College : Shridevi Institute of Engineering and Technology, Tumakuru
Branch : Computer Science and Engineering
Guide(s) : *Mr. Suthan R* ***B.E,M.Tech.,***
Student(s): *Ms. Sowmyashri S*
Ms. P A Niveditha
Ms. Suma M T
Ms.Saranya B

Keywords:

Ontology-Based Data Structuring ,Medical Record Management ,Role-Based Access Control (RBAC) ,Secure Health Data Exchange ,Flask Web Application

Introduction:

The Ontology-Based Medical Record Storage and Exchange System is a secure and structured platform designed to modernize how patient health records are stored, managed, and shared. Traditional healthcare systems often suffer from fragmented data, delays in information access, and lack of continuity in patient care. Our system addresses these issues by organizing medical data using an ontology-driven approach, enabling structured, meaningful, and interoperable records.

At the first point of contact, a patient's complete health data—including symptoms, diagnosis, lab reports, prescriptions, and treatment plans—is stored securely. This information is then made accessible to the next treating healthcare professional, ensuring continuity of care. The system implements strict role-based access control: doctors access full medical records, nurses view treatment and medication history, and patients see only relevant details like prescriptions and appointments.

To maintain privacy and security, different authentication methods are used: doctors and nurses log in with user IDs and passwords, while patients authenticate via email and OTP. The system is built using Python and Flask for the backend and HTML, CSS, and JavaScript for the frontend, offering a clean and user-friendly interface.

By reducing redundancy, improving data accessibility, and enabling real-time updates, the system enhances clinical decision-making and improves patient outcomes. This project contributes meaningfully to healthcare digitization by offering a scalable, secure, and role-specific record management solution.

Objectives:

- To securely store and manage patient medical records using an ontology-driven data structure.
- To enable seamless and role-specific access to medical data for doctors, nurses, and patients.
- To ensure continuity of care by allowing real-time sharing of patient records across healthcare providers.
- To enhance data interoperability and reduce redundancy in medical record-keeping.
- To implement strong authentication and access control mechanisms based on user roles.
- To improve patient outcomes and clinical decision-making through efficient data availability.

Methodology:

Requirement Analysis:

Conducted a detailed analysis of existing medical record systems to identify key pain points such as data fragmentation, redundancy, and lack of interoperability.

System Design:

Designed a modular architecture incorporating frontend, backend, and database layers. Emphasis was placed on role-based access and secure authentication methods tailored to each user group.

Ontology Development:Created a medical ontology to define relationships among healthcare entities such as symptoms, diagnoses, treatments, test results, and prescriptions. This structured format ensures consistency and semantic understanding across the system.

Backend Implementation:

Developed the backend using Python and Flask to handle data processing, storage, user authentication, and communication with the frontend.

Frontend Development:

Built a responsive and user-friendly interface using HTML, CSS, and JavaScript, providing distinct dashboards for doctors, nurses, and patients based on their access level.

Role-Based Access Control:

Implemented access policies where:

Doctors have full access to all patient records.

Nurses can view limited treatment and medication information.

Patients access only relevant personal health information through OTP-based authentication.

Data Storage and Security:

Patient data is stored securely in a structured format to prevent redundancy and enable efficient querying. Encryption and secure session handling are used to protect sensitive data.

Testing and Validation:

Performed extensive testing to ensure data integrity, access control enforcement, and system responsiveness. Functional, integration, and security tests were conducted.

Deployment:

Hosted the system on a local or cloud-based server for real-time usage, enabling healthcare providers and patients to interact with the system seamlessly.

Feedback and Iteration:

Gathered feedback from users and healthcare professionals to refine functionalities, improve usability, and ensure alignment with healthcare standards and regulations.

Result and Conclusion:

The Ontology-Based Medical Record Storage and Exchange System was successfully developed and implemented, demonstrating significant improvements in the management and accessibility of medical data. The ontology-driven data structure enabled consistent organization and eliminated redundancy across patient records. Role-based access control functioned effectively, ensuring that users could only view information pertinent to their responsibilities, thus maintaining data privacy and security.

Doctors reported enhanced efficiency in diagnosis and treatment planning due to immediate access to comprehensive patient histories. Nurses were able to streamline patient care by quickly retrieving medication and treatment information, while patients appreciated the secure and easy-to-use interface for viewing test results, prescriptions, and appointments.

Authentication mechanisms tailored to each role—password-based for medical staff and OTP-based for patients—proved both secure and user-friendly. Real-time record sharing reduced delays in treatment, supporting continuity of care across different healthcare providers.

The system also highlighted the benefits of digitizing healthcare through structured, interoperable data exchange. Overall, the project successfully met its objectives and has the potential to be scaled or integrated into larger healthcare IT ecosystems to further improve medical decision-making and patient outcomes.

Project Outcome & Industry Relevance:

This project highlights the growing relevance and efficiency of Attribute-Based Access Control (ABAC) in securing e-health systems, particularly for managing Electronic

Health Records (EHRs) and Personal Health Records (PHRs). By conducting a thorough survey of existing literature, it illustrates the suitability of ABAC in healthcare, where flexible, fine-grained, and context-aware access control is crucial. The paper proposes that ABAC not only enhances security and privacy but also enables dynamic, role-independent access decisions—especially vital in emergency medical scenarios. It also introduces the concept of leveraging ABAC access logs for modelling and analyzing healthcare professionals' security practices. This has real-world implications for compliance monitoring, insider threat mitigation, and improving the security culture within healthcare institutions. The project's insights are particularly applicable for hospitals, cloud service providers, and regulatory bodies working toward HIPAA-compliant systems with adaptive and auditable security mechanisms.

Working Model vs. Simulation/Study:

This project is primarily a theoretical study and literature survey, not a working physical model. It synthesizes existing approaches and technologies related to ABAC in healthcare, categorizes them, and discusses their practical implications and future challenges. While it provides valuable frameworks and conceptual use-case models, it does not involve developing or testing a working implementation.

Project Outcomes and Learnings:

Key outcomes of the project include:

- A comprehensive classification of ABAC implementations in EHR and PHR systems.
- Identification of common privacy-preserving techniques, notably ciphertext-policy Attribute-Based Encryption (ABE).
- Recognition of cloud platforms as the prevalent storage method, despite concerns over trust and security.
- Highlighting ABAC's flexibility in emergency access scenarios and its capability to support efficient log analysis due to its rich attribute data.

Learnings:

- ABAC provides a more scalable and secure alternative to Role-Based Access Control (RBAC), particularly in dynamic healthcare environments.
- Incorporating multiple attributes (user, environment, resource) into access decisions allows for more nuanced security.
- There is a need for future studies to consider untrusted service providers, to further fortify patient data privacy.
- The integration of ABAC logs into security behavior modelling opens up new avenues for research and policy development in healthcare IT.

Future Scope :

1. AI-Powered Disease Prediction & Recommendations
2. Blockchain for Secure & Decentralized Data Storage
3. Integration with IoT-Based Medical Devices
4. Telemedicine & Video Consultation
5. Multi-Hospital & Cross-Border Data Sharing