AI DATALOCK: Blockchain & ABE For Healthcare

Mr R.Ramakrishnan[1], U.Nivetha[2]
[1]Associate Professor, Dept of Computer Applications
[2]Dept of Computer Applications
[1, 2] Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India

Abstract- *Healthcare Using Blockchain and ABE Technologies focuses on securing sensitive health data such as Electronic Medical Records (EMRs) and real-time physiological metrics (e.g., heart rate, ECG, temperature) from wearable sensors. These data streams are critical for patient care but are increasingly vulnerable to unauthorized access and cyber- attacks, particularly when stored in cloud environments. Existing security protocols often fail to provide sufficient protection, leading to risks like weak encryption, limited access control, and a lack of accountability in the event of data breaches. To address these challenges, the AI DataLock framework is proposed, integrating Hierarchical Key – Attribute-Based Encryption (HE-ABE) and Blockchain technology. HE-ABE ensures that only authorized individuals with the correct attributes can access patient data, while Blockchain provides tamper-proof logging for data sharing activities. This combination enhances data confidentiality, enforces fine- grained access control, and strengthens the overall integrity of healthcare systems.*

Keywords- Electronic Medical Records (EMRs), Wearable Sensors,Health Data Security,Hierarchical Key – Attribute-Based Encryption(HE-ABE),Blockchain Technology,Fine-Grained Access Control,Data Privacy,Cybersecurity in Healthcare.

I. INTRODUCTION

This section outlines the essential hardware and software requirements as well as the functional and non-functional specifications required for the effective development and deployment of the Health DataLock Web App. The system is designed to operate within a secure, scalable, and performance-optimized environment, ensuring reliability across a range of healthcare settings. It defines the system's operating environment, including server configurations, supported web browsers, and necessary third-party integrations. The user roles include patients, medical professionals, administrators, and system auditors—each with specific access levels governed by fine-grained policies. Performance expectations include low-latency data access, high system availability, and support for concurrent users without degradation in response time. To meet the increasing demands for privacy in healthcare, security constraints emphasize encryption at rest and in transit, blockchain-based audit trails, and robust access control. These specifications establish the technical blueprint that ensures the system meets its core objective: to securely manage sensitive healthcare data using Blockchain and Hierarchical Attribute-Based Encryption (HE-ABE), while enabling authorized, role-based access. Furthermore, the design accounts for regulatory compliance with healthcare data protection laws such as HIPAA and GDPR.

II. LITERATURE SURVEY

[1] proposed a cloud-based health data management system that focused on integrating electronic medical records (EMRs) into a centralized web platform. The solution offered functionalities such as patient registration, doctor-patient communication, and digital prescription handling. However, the system relied on traditional encryption methods and lacked fine-grained access control, which limited its security effectiveness in protecting sensitive patient information.[2] introduced a blockchain-enabled health record sharing platform that emphasized tamper-proof data storage and audit trails. Their decentralized architecture helped eliminate single points of failure, enhancing system resilience. Despite strong data integrity guarantees, the system did not implement user-specific access control mechanisms, making it difficult to tailor data visibility to individual roles within a healthcare institution.[3] developed an Attribute- Based Encryption (ABE) scheme for secure sharing of patient data across hospitals. Their model allowed access based on user attributes like designation and department. While the ABE model offered better access control, it did not scale efficiently with dynamic user roles and lacked integration with decentralized technologies like blockchain for auditability and traceability.[4] designed a smart healthcare management portal that leveraged machine learning to predict patient outcomes based on medical history and real-time sensor data. The platform supported real-time monitoring through wearable devices, offering valuable predictive insights. However, the system did not address the secure transmission and storage of sensitive physiological data collected from sensors, posing privacy risks.[5] explored a hybrid cloud architecture for EMR management, emphasizing cost-efficiency and scalability. Their study showed that hybrid models helped hospitals with

limited on- premise infrastructure to adopt digital systems. Yet, the proposed system did not incorporate strong encryption standards or traceable access logs, leaving data vulnerable to unauthorized access.[6] implemented a privacy-preserving IoT healthcare system using lightweight cryptographic algorithms for wearable devices. The system focused on minimizing energy consumption while maintaining data confidentiality. Although suitable for resource-constrained environments, the approach was not robust enough for enterprise-grade healthcare systems that require multi-layered access control and data integrity assurances.

III. PROBLEM STATEMENT

Electronic Health Records (EHRs) have transformed healthcare by digitizing patient records, enabling efficient data management, and improving clinical decision-making. However, despite their advantages, several critical challenges hinder their effectiveness, security, and interoperability. One of the primary concerns in EMR systems is data security and privacy risks. As patient records contain highly sensitive medical and personal information, they are prime targets for cyber threats, unauthorized access, and data breaches. Many existing EMR systems lack robust encryption mechanisms, making them vulnerable to hacking, ransomware attacks, and unauthorized data leaks. Another major challenge is the lack of interoperability between different EMR platforms. Healthcare institutions often use disparate systems that are not standardized, making it difficult to share and integrate patient records seamlessly across hospitals, clinics, and pharmacies. This limitation affects the continuity of care, delays medical decisions, and creates inefficiencies in patient treatment. Additionally, unauthorized access and insufficient role based restrictions pose a significant risk in EMR management. Traditional EMR systems often do not enforce strict access controls, allowing non-medical personnel or unauthorized users to view or manipulate patient data. Maintaining data integrity and trust is another pressing issue in EMRs.

IV. PROPOSED SYSTEM ARCHITECTURE

The proposed system enhances the security, accessibility, and integrity of Electronic Health Records (EHRs) and health data using Hierarchical Key – Attribute-Based Encryption (HE-ABE) and Blockchain Technology. This system ensures fine-grained access control, secure storage, and transparent auditing while integrating a Medicine Availability System to track real-time medicine stock in pharmacies. The system employs Hierarchical Key – Attribute-Based Encryption (HE-ABE) to ensure that only authorized users, such as doctors, patients, and pharmacists, can access sensitive medical data. Unlike conventional encryption methods, HE-ABE allows fine- grained access control by assigning different access rights based on user attributes (e.g., medical role, department, or clearance level). This ensures that confidential medical data remains protected from unauthorized users while allowing legitimate access to healthcare professionals as needed.

HBAC, while useful in many systems, lacks flexibility in dynamic healthcare environments. It relies on predefined hierarchical structures, which may not be able to accommodate rapidly changing roles or new user requirements. This rigid framework could potentially restrict access management, making it difficult to adapt to evolving needs, such as accommodating temporary roles or cross-functional teams that don't fit neatly into a hierarchy. Blockchain technology is integrated to maintain a decentralized and tamper-proof ledger for recording all medical data transactions. Every access, update, or modification to the EMR system is securely logged onto the blockchain, ensuring data integrity and transparency. Since blockchain records cannot be altered or deleted, it helps prevent unauthorized data modifications, data breaches, and fraudulent activities, providing a trustworthy and auditable healthcare system. The system integrates pharmacy databases to track the real-time availability of prescribed medicines across government and private pharmacies. When a doctor prescribes a medicine, the system cross- references pharmacy inventories to determine availability, ensuring faster medicine procurement and uninterrupted patient care. In cases where a prescribed medicine is unavailable, the system provides alternative pharmacies where the medicine is in stock, improving accessibility and reducing treatment delays.

V. ADVANTAGES OF PROPOSED SYSTEM

- **Fine-Grained Access Control**: Implements **Hierarchical Attribute- Based Encryption (HE-ABE)** to restrict data access based on user roles and attributes (e.g., doctor, nurse, researcher).
- **Blockchain Integration for Auditability**: Ensures **tamper-proof logs** of data access and modifications through a decentralized, immutable ledger.
- **Enhanced Data Security**: Protects sensitive Electronic Medical Records (EMRs) and wearable sensor data using **end-to-end encryption** and blockchain-based integrity verification.
- **Real-Time Access Control**: Supports **dynamic permission assignment**, allowing data sharing policies to be updated in real time without compromising system security.

- **Privacy-Preserving Architecture**: Prevents unauthorized access and **minimizes exposure of patient data**, even in cloud environments.
- **Interoperability Support**: Designed to integrate with **heterogeneous healthcare systems**, enabling secure data exchange across hospitals, clinics, and labs.
- **Accountability and Transparency**: Every action on patient data is **logged and verifiable**, providing traceability and meeting compliance standards (e.g., HIPAA, GDPR).

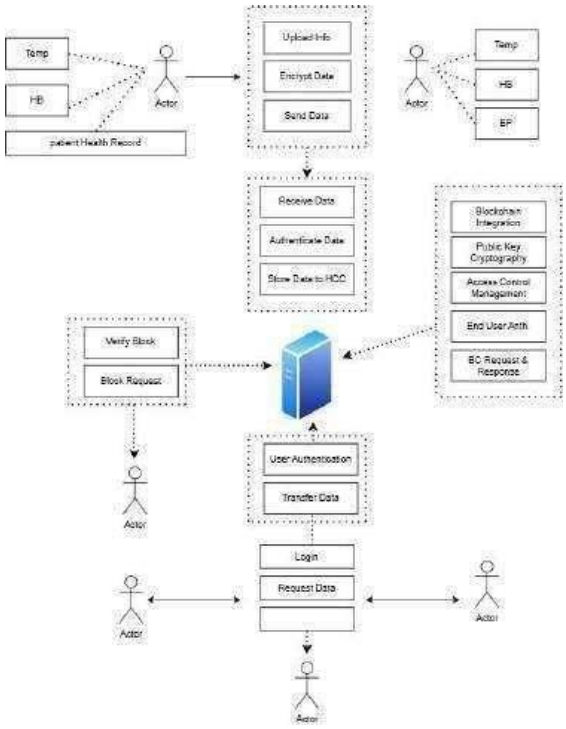

Fig. 1: System Architecture

The activity flow of the AI DataLock system begins when users—including doctors, nurses, patients, researchers, and administrators— access the secure web portal and either register or log in. Upon successful authentication, the system identifies their role and grants specific access permissions using Hierarchical Attribute-Based Encryption (HE-ABE). Based on their role, different activities are initiated. Healthcare providers can request access to patient records or sensor data, which the system verifies against their attributes before decrypting and displaying. They may then update or add medical information, which is re- encrypted and stored. Patients, on the other hand, can upload real-time health data from wearable devices, manage their profiles, and control access permissions by granting or revoking data-sharing rights. Researchers may request access to anonymized datasets for analysis, subject to policy validation and approvals. System administrators oversee role management, policy configurations, and monitor audit trails. Every interaction—such as data access, sharing, or modification—is recorded on a blockchain ledger, ensuring tamper-proof logs for full accountability. Throughout the process, the system performs policy checks at each decision point to allow or deny access based on real-time attributes. Users are continuously updated via automated notifications regarding system events, access decisions, or anomalies. This secure, role- based, and traceable workflow ensures healthcare data is managed with maximum privacy, transparency, and efficiency.

VI. RESULT AND DISCUSSION

The AI DataLock system delivers a secure, high-performance, and scalable solution for managing sensitive healthcare data by combining Blockchain technology and Hierarchical Attribute-Based Encryption (HE- ABE). The frontend is built using HTML5, CSS3, JavaScript, and Bootstrap, offering a clean and responsive user interface tailored for roles such as Patients, Healthcare Providers, Researchers, and Administrators. Each user role is provided with intuitive access to functionalities like viewing medical records, uploading real-time sensor data, granting/restricting data access, and monitoring system activity logs. The backend is developed using Python and Flask, which facilitates secure user authentication, seamless data flow, and interaction between the frontend and the blockchain-integrated database. MySQL serves as the primary storage system, efficiently managing EMRs, user profiles, and access records through normalization, indexing, and optimized queries. The system's reliability is strengthened through rigorous unit testing, integration testing, and security verification to ensure robust protection of patient data. AI DataLock also incorporates containerization via Docker, allowing for smooth deployment and environment consistency. The application is hosted on an Apache server with a containerized database for scalability. To ensure long-term performance and reliability, routine database backups, continuous performance monitoring, and modular design principles are implemented, leaving room for future feature expansions and policy updates in response to evolving healthcare requirements.

VII. CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, this project successfully addresses the growing need for secure, efficient, and reliable management of sensitive health data in the healthcare sector. By integrating advanced technologies like Hierarchical Key – Attribute-Based Encryption (HE-ABE), Blockchain for data integrity, and real-time medicine availability tracking, the system ensures that patient data is protected from unauthorized access, tampering, and other security risks. The Hierarchy-based access control (HBAC) mechanism ensures that

healthcare professionals, patients, and administrators have access only to the data they are authorized to view or modify, thus maintaining confidentiality and privacy. Furthermore, the Health Data Integrity Verification system guarantees that any changes to sensitive health information are recorded and verifiable, preventing data corruption. The medicine availability and recommendation system improves patient care by providing real- time information about drug availability and suggesting alternative medications, ensuring that treatment plans are not delayed due to stock shortages. Through secure access, integrity verification, and timely medication recommendations, this project enhances the healthcare experience for both patients and healthcare providers. The system is scalable, allowing for future improvements and expansions as the healthcare landscape continues to evolve. This project not only meets the current demands for secure healthcare data management but also sets a foundation for future advancements in secure and efficient health data systems. This project serves as a significant step forward in ensuring the privacy, integrity, and availability of health data in a rapidly evolving healthcare environment.

REFERENCES

[1] Adams, E. R., Peterson, J. T., & Ramirez, M. A. (2022). Transforming Student Careers: A Case Study of Effective Training and Placement Cell Strategies. Journal of Educational Management, 18(2), 145-162.

[2] J. Yu and W. Shen, "Secure cloud storage auditing with deduplication and efficient data transfer", *Cluster Comput.*, vol. 27, no. 2, pp. 2203-2215, Apr. 2024.

[3] B. Grover and D. K. Kushwaha, "Authorization and privacy preservation in cloud-based distributed ehr system using blockchain technology and anonymous digital ring signature", *Health Services Outcomes Res. Methodol.*, vol. 23, no. 2, pp. 227- 240, Jun. 2023.

[4] R. Tertulino, N. Antunes and H. Morais, "Privacy in electronic health records: A systematic mapping study", *J. Public Health*, vol. 32, no. 3, pp. 435-454, Jan. 2023.

[5] Z. Bao, D. He, H. Wang, M. Luo and C. Peng, "A group signature scheme with selective linkability and traceability for blockchain-based data sharing systems in E-health services", *IEEE Internet Things J.*, pp. 1, 2023.

[6] C. Lai, Z. Ma, R. Guo and D. Zheng, "Secure medical data sharing scheme based on traceable ring signature and blockchain", *Peer-Peer Netw. Appl.*, vol. 15, no. 3, pp. 1562-1576, May 2022.

[7] A. Ali, M. A. Almaiah, F. Hajjej, M. F. Pasha, O. H. Fang, R. Khan, et al., "An industrial IoT-based blockchain- enabled secure searchable encryption approach for healthcare systems using neural network", *Sensors*, vol. 22, no. 2, pp. 572, Jan. 2022.

[8] A. Ali, M. F. Pasha, J. Ali, O. H. Fang, M. Masud, A. D. Jurcut, et al., "Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography", *Sensors*, vol. 22, no. 2, pp. 528, Jan. 2022.

[9] A. Lu, W. Li, Y. Yao and N. Yu, "TCABRS: An efficient traceable constant-size attribute-based ring signature scheme for electronic health record system", Proc. IEEE 6th Int. Conf. Data Sci. Cyberspace (DSC), pp. 106-113, Oct. 2021.

[10] B. S. Egala, A. K. Pradhan, V. Badarla and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control", *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717-11731, Jul. 2021.

[11] S. Xu, J. Ning, J. Ma, X. Huang and R. H. Deng, "K -time modifiable and epoch-based redactable blockchain ", *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4507-4520, 2021.aker, C. L., Turner, A. B., & Hughes, L. R. (2021). Industry-Academia Collaboration for Enhanced Employability: Insights from Training and Placement Cells. International Journal of Training and Development, 14(4), 311-328.