iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74048

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Secure Federated Cloud Storage Protection Strategy using Hybrid Heuristic Attribute-Based Encryption with Permissioned Blockchain

SheelaRani C M[1], Prapthi Shenava[2], Rakshitha M S[3], Sinchana N[4], Thanvi B V[5]
[1]*Assistant Professor, Dept. of CSE, Sapthagiri College of Engineering*
[2, 3, 4, 5]*Dept. of CSE, Sapthagiri College of Engineering*

Abstract: ***Healthcare in the country is grappling with medical data exchange fragmentation, doctor-to-doctor referral process, secure information transfer between hospitals, and patient-convenient portals to personal records being termed as critical points of vulnerability. Concerns are the isolation of health records within hospitals, risks of information abuse of revealed information, and the absence of adequate security protocols. To address these, the Electronic Health Record (EHR) Architecture based on Blockchain was created in collaboration with the hospital, physician, payer, and patient ecosystem. This paper evaluates the feasibility of applying the architecture to store clinical data in a manner that preserves privacy, provides controlled availability and reconciles competing demands for sharing and confidentiality, and promotes compatibility among disparate clinical and administrative system domains. Privacy, in this context, means detailsis accessible only to particular parties and is inviolate in any way—visible, modified, transmitted, or deleted—while being kept, transported, or processed without authorization by a patient. Availability requires that, despite unforeseen sabotage, malfunction, equipment obsolescence, or malicious behavior, patients and legitimate caregivers have access to required information without impeding workflows. Both practice and literature point out that the creation of this double horizon of privacy and resilience require the active participation of all stakeholders, corporate or individual. Interoperability in legacy practice valleys has centered mainly on plugs between information systems. The patient-care community has been busy in now with enabling patients to enter their healthdetails, with the passing being at their discretion. Our system offers privacy and data integrity through the acquisition of medical data first and then encrypting the data through Attribute-Based Encryption, where the best to sharpen the key is the DES algorithm.***
After encryption, the information is kept in a permissioned blockchain, provides layered access control and protection against compromised information. To further support the patient, we have integrated a predictive analytics module in our patient interface that utilizes machine-learning classifiers i.e. Random Forest, Logistic Regression, and Decision Tree to make near disease detection

I. INTRODUCTION

Blockchain is an open, distributed, and digital ledger system to keep a record of activity across several machines in a manner that no identical record will be modified in the past without modifying all subsequent blocks. The concept was released as a white paper by Satoshi Nakamoto in the year 2008. Protected Health Information of all patients is the most precious asset of any healthcare system.

Blockchain technology offers a remarkable and revolutionary way to maintain references to the dispersed patient information. An Electronic Health Record (EHR) is a broad aggregation of patients' personal information and medical histories maintained electronically in digital form. EHRs are patient-driven legitimate documents containing the information accessible to authorized stakeholders immediately in a safe format. An EHR holds patients' personal and medical history. The EHR system is planned to go above usual clinical data collection to be more complete of a broader view of patient outcomes. Assume each reported EHR injects updates into an open-source, community-owned trusted ledger about medications, issues, and allergy lists, so changes in the medical records are evidently clear and auditable across those organizations. In place of merely displaying data from a given database, the EHR could present data from any database that is cross-referenced within the ledger. The outcome would be ethereally balanced community-based information, with assured credibility from the date of data origin to the date of need, irrespective of manual human intervention. Healthcare systems all over the world are undergoing a digital transformation, with special focus on safe handling of data, patient-centered care, and inter-institutional interoperability. Patient medical records are the most sensitive categories of data, and their security is crucial for maintaining trust and compliance with privacy regulation.

Traditional data storage habits in medicine, which rely on centralized databases or external servers, are open to issues such as unauthorized access, data leaks, single points of failure, and interoperability problems between hospitals or clinics. Blockchain has been proposed as a potential solution to all these problems. Blockchain is a decentralized, transparent, and immutable ledger system which makes one trusted authority unnecessary. Through the distribution of data across a network of nodes, it makes it impossible for medical records to be altered and traceable always. In medicine, this would translate to the fact that patient records would be shared securely between doctors, labs, and patients without compromising strict privacy controls.

To enhance security, Attribute-Based Encryption (ABE) is incorporated with blockchain. ABE protects medical records by encrypting them based on attributes like doctor specialization, patient permission, or lab responsibilities, so that only the right parties can access particular parts of the data. This high-level access control prevents the misuse of sensitive information and provides patients with more control over their own health records. In addition, the implementation of Machine Learning (ML) makes the system more feasible by allowing predictive healthcare. Algorithms such as Random Forest, Decision Trees, and Logistic Regression are used to analyze patient information—based on symptoms and medical history—to forecast possible diseases. This offers doctors useful decision-support tools, enhances diagnostic precision, and improves treatment. The integrated application of Blockchain, ABE, and ML establishes an interoperable, safe, and smart Electronic Health Record (EHR) platform. It maintains privacy, accessibility, and trustworthiness of medical data, and also empowers healthcare workers with smart predictive analytics. Finally, this combined method not only meets the limitations of dispersed healthcare information but also serves as a base for a patientoriented, safe, and futureproof healthcare system.

II. BACKGROUND AND MOTIVATION

The Healthcare Sector facingmajor challenges in managing and sharing the Electronic Health Records (EHR) efficiently, safely and transparently. Traditional ecosystems are plagued by fragmented records stored in many organizations, often staying on the unsafe third-party database. This fragmentation leads to many major risks and disabilities

1) Data Fundament :Patients are spread in record hospitals and clinics, making it difficult to achieve an integrated, accurate medical history.
2) Data security and privacy concerns:Violations, unauthorized access, or susceptible to abuse when stored or transferred sensitive health data without strong safety measures.
3) Limited Interoperability : Different hospital systems often lack general standards, the exchange of medical records is complicated.
4) Access and Availability: Systems or hardware failures may cause data loss or delay in access to important medical information, possibly affecting the patient's care.

Blockchain technology combined with Attribute-Based Encryption (ABE) is helping to address many long-standing challenges in healthcare data management. Blockchain’s decentralized ledger clarify that medical records are transparent, tamper-proof, and verifiable manner. While ABE enables fine-grained access control, ensuring that only authorized users can view specific parts of sensitive health information. In addition, Machine Learning is playing a vital role in healthcare by supporting predictive analytics, disease detection, and patient experience evaluation. The integration of these technologies has the potential to enhance clinical decision-making, enable more personalized treatment plans, and reduce errors or misuse of patient data.

III. LITERATURE SURVEY

A. *Big Data Analytics Framework For Opinion Mining Of Patient Health Care Experience*

Authors: G. Sabarmathi and R. Chinnaiyan

Year: 2020

Link: https://ieeexplore.ieee.org/document/9076477

WAC (Web-based Life, Analysis, and Cloud) is the data system that enables seamless information sharing faster than what we see with Big Data. The large amounts of data derived from this vast collection, often referred to as Big Data, need a better way of handling it, especially in healthcare. We can explore this data pool to support a framework that aims to understand partner needs by gathering insights on various important topics. Value management can help identify key decisions where new research can lead to different directions.There is a significant need to analyze and assess the findings presented in the existing body of literature. Conducting such a review allows researchers to identify prevailing trends, highlight key developments, and findparticular areas for future investigation. In this context, the present article offers ainclusive exploration of prior studies focused on opinion mining within the healthcare domain.

B. Public Auditability And Data Dynamics For Storage Security In Cloud Computing
Authors: Q. Wang, C. Wang, J. Li, K. Ren, W. Lou
Year: 2011
Link: https://doi.org/10.1109/INFOCOM.2010.5462173
In this paper, the authors presented a public auditability framework for cloud storage systems, allowing third-party secure auditing of outsourced data. The paper also facilitated data dynamics, enabling clients to update their data stored in the cloud and maintain integrity verification. The proposed protocol employed homomorphic authenticators and random masking methods to ensure auditing cannot violate data privacy. This groundwork gave way to blockchain-based auditing systems by developing the principle of secure, open verification without compromising sensitive information.

C. Blockvault: A Blockchain-Enabled Federated Cloud Framework For Data Security
Authors: O. Malomo, T. Zuva, S. Ngwira
Year: 2020
Link: https://doi.org/10.1109/ICACCS48705.2020.9074183
Malomo et al. came up with BlockVault, a blockchain-enabled federated cloud architecture that will safeguard vital enterprise data. This method tackled weaknesses with centralized cloud storage by using a distributed ledger for trust management. Decentralized auditing, fault tolerance, and control were achieved through blockchain's immutable ledger, removing a failure. BlockVault showed the practical application of using blockchain with cloud storage systems for end-to-end security and audibility.

IV. METHODOLOGY

"Secure Federated Cloud Storage Protection Strategy Using Hybrid Heuristic Attribute-Based Encryption with Permissioned Blockchain" aims to address key issues in health data management. This includes privacy, security, interoperability, and smart analytics. The approach combines modern encryption techniques, blockchain technology, and machine learning as follows:

1) System Architecture and Modules - The project has four main modules: - Patient - Doctor - Lab Technician - Blockchain Server Each module has clear roles in data flow, security, and system operations.

2) Data Collection and Access Management - Patient data is collected and entered into the system through secure user interfaces. - Stakeholder identities, including doctors, labs, and patients, are confirmed through safe registration and login processes. - Access permissions are managed carefully. Stakeholders request access to patient records, which the permissioned blockchain then processes.

3) Attribute-Based Encryption (ABE) and Data Security - Patient health information is encrypted using Attribute-Based Encryption (ABE) with a key produced by the DES algorithm. - ABE offers distributed and detailed access control based on user attributes, such as roles and clearance levels. - Only authorized users with the right attributes can decrypt and access specific data. This ensures strong privacy and decreases the risk of unauthorized data exposure.

4) Secure Record Storage Using Permissioned Blockchain

- Encrypted electronic health records and medical transactions are stored on a permissioned blockchain network.
- Blockchain ensures:

- Immutability: No record can be changed or deleted without agreement, which creates a strong audit trail. - Transparency and
- Traceability: All data accesses and changes are logged and can be audited by stakeholders.
- Decentralization and Availability: Data will remain safe from hardware failures and is always accessible to authorized users without relying on a single centralized server. Stakeholders, such as doctors, lab technicians, and patients, must request permission through the blockchain to access or change any patient data. Every action is recorded in the ledger, which allows for complete traceability.

5) Data Sharing and Interoperability

- The blockchain-based EHR system allows secure sharing of medical reports and lab results between patients, doctors, and laboratories at different health institutions.
- Interoperability is maintained through a common blockchain protocol and secure APIs, removing barriers between previously isolated medical records.

6) Disease Prediction with Machine Learning

- The system includes a disease prediction module that implements machine learning algorithms like Random Forest, Logistic Regression, and Decision Trees.
- Patient symptoms and historical health data serve as inputs, and the models train on real-world datasets from sources like Kaggle.
- The prediction results help doctors with diagnoses and support patient-centered decision-making, adding smart analytics to the platform.

7) Workflow Overview

• Patient/Doctor/Lab Registration and Login: Secure sign-up and authentication.
• Data Input: Patients record symptoms and schedule appointments; doctors and lab technicians create and upload reports.
• Encryption: Medical data is encrypted with ABE and DES-generated keys before storage.
• Blockchain Storage: Encrypted data is present in the permissioned blockchain ledger.
• Permission Management: Access requests are managed through the blockchain's access control. This confirms that only respected users with the right attributes can view or decrypt relevant records.
• Machine Learning Analytics: The disease prediction module processes patient data and sends predictions to clinicians.
• Audit and Traceability: All actions are logged for transparency, security, and future audits.

Technology Stack:
Frontend: Java Swings / Python Tkinter
Backend: MySQL Server 5.0 and blockchain technology
Development Tools: JDK 1.8 & NetBeans 8.2, Visual Studio Code
Security: Hybrid Heuristic Attribute-Based Encryption with DES keys
Machine Learning: Random Forest, Logistic Regression, Decision Tree (using Python, trained on Kaggle datasets)
Platform: Windows OS
This multi-layered approach ensures confidentiality, accessibility, interoperability, and intelligence, aiming to create a trustworthy, secure, and smart medical data system that uses the latest technologies.

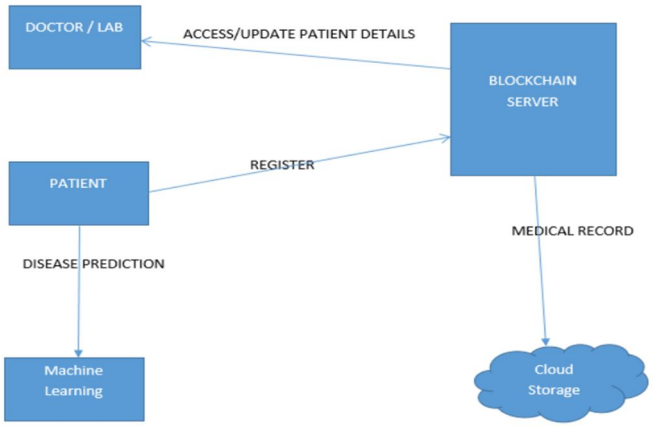


Fig.1: System Architecture

V. CONCLUSION

This project demonstrates a robust and innovative approach to securing electronic health records (EHRs) using a hybrid strategy that integrates Attribute-Based Encryption (ABE) with Permissioned Blockchain technology. By doing so, the solution effectively addresses core challenges in the healthcare sector related to fragmented patient records, insecure storage, and unauthorized data access. The proposed framework enables reliable, privacy-preserving sharing of medical data among patients, doctors, and lab technicians, ensuring that each stakeholder accesses only the information they are permitted to view.Leveraging blockchain ensures a single, tamper-proof version of the truth for each medical record, substantially reducing the chance of data breaches. and unauthorized modifications.

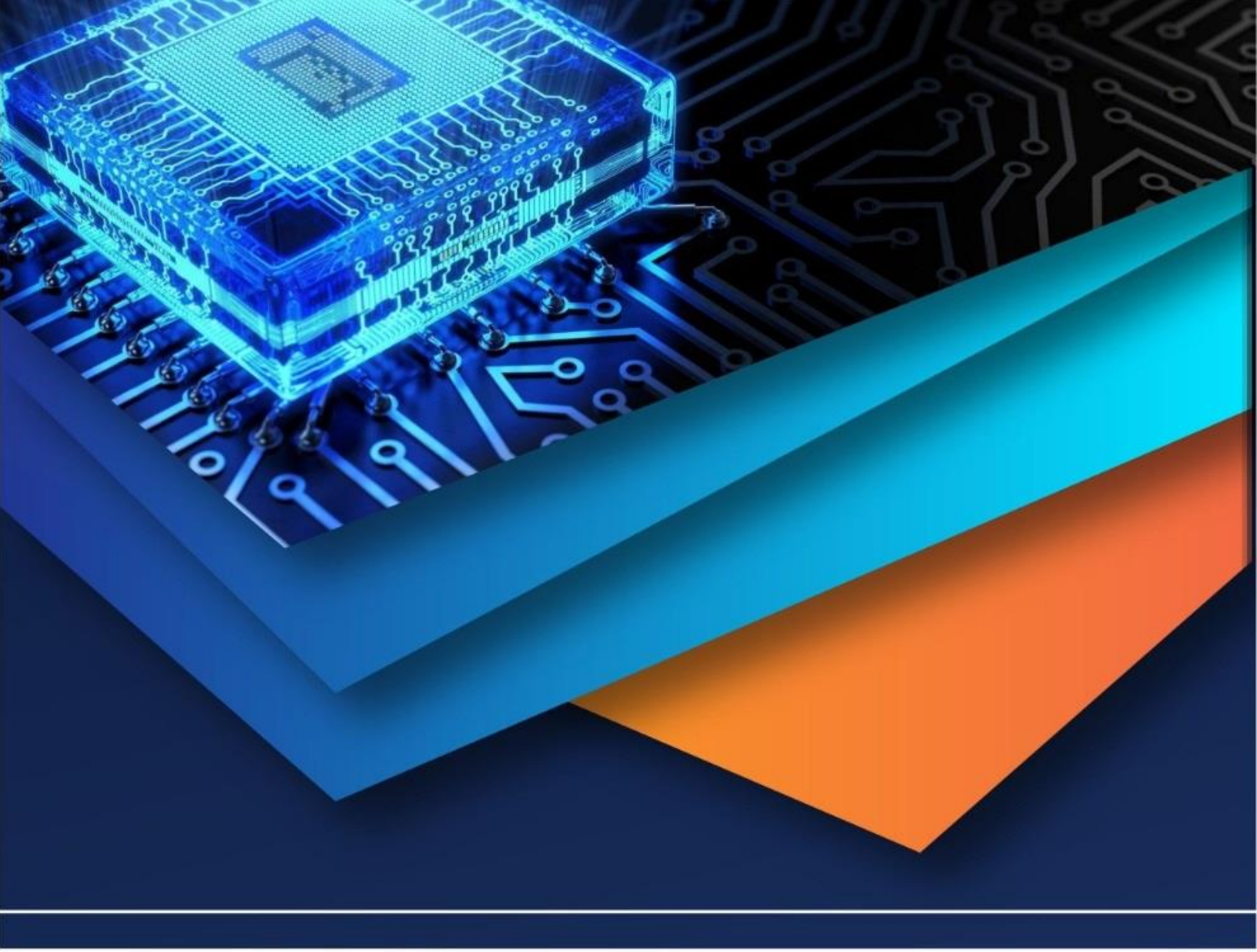
The use of optimal encryption keys generated by the DES algorithm further enhances data confidentiality, while permissioned access on the blockchain maintains strong integrity and access control.Furthermore, the project incorporates machine learning algorithms—such as Random Forest, Logistic Regression, and Decision Tree—for disease prediction within the patient module. This empowers personalized, data-driven healthcare and can help clinicians make quicker, more precise decisions. based on historical and real-time patient data.By combining state-of-the-art encryption, blockchain, andpredictive analytics, the system not only secures patient information but also promotes data interoperability, patient-centric sharing, and improved accessibility in healthcare environments—laying the groundwork for a smarter, safer, and more efficient digital health ecosystem.

REFERENCES

[1] A. B. Kathole et al., "Secure federated cloud storage protection strategy using hybrid heuristic attribute-based encryption with permissioned blockchain," IEEE Access, vol. 12, pp. 117154–117170, Aug. 2024, doi: 10.1109/ACCESS.2024.3447829.
[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[3] Y. Zhang, J. Ni, K. Yang, and X. S. Shen, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, June 2018.
[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data, 2017, pp. 557–564.
[5] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," IEEE Access, vol. 7, pp. 73295–73305, June 2019.
[6] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018.
[7] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in Proc. IEEE Int. Conf. Wireless and Mobile Computing, Networking and Communications, 2017, pp. 1–6.
[8] R. K. Ko, P. Jagadpramana, and B. S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," Proc. IEEE World Congr. Services, 2011, pp. 584–588.
[9] M. Alhussein, K. Aurangzeb, and S. I. Haider, "Blockchain-based secure healthcare system for electronic medical records," IEEE Access, vol. 9, pp. 19230–19244, Jan. 2021.
[10] S. R. Moosavi, T. N. Gia, A. Rahmani, E. Nigussie, S. Virtanen, and H. Tenhunen, "End-to-end security scheme for mobility enabled healthcare Internet of Things," Future Generation Computer Systems, vol. 64, pp. 108–124, Nov. 2016.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY