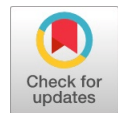




Unified Medical Report Management and Prediction System on Blockchain

D. Madhava Rao, D. Shreyas, D. Akhila, B. Sai Vishal



Abstract: *The increased use of Electronic Health Records (EHRs) has increased access to patient information in medical facilities, but has also raised long-term concerns regarding the security, confidentiality, and partial control of records. In most work environments, medical information is scattered across hospitals, laboratories, and clinics, hindering transparency and making its sharing and analysis extremely difficult. Most existing systems operate on centralised architectures that are not as hard to manage but can be undermined by data breaches, unauthorised access, and single points of failure. To address these shortcomings, this paper presents a management and prediction model for medical reports that integrates blockchain technology, decentralised storage, and machine learning-based analytics. A permissioned consortium blockchain is responsible for metadata, ownership, and access control of large medical files stored off-chain in the InterPlanetary File System (IPFS) to maximise scalability and efficiency. Anonymised and aggregated data have been analysed using machine learning models to enable predictive analysis without exposing sensitive patient data. The proposed system was tested in controlled experimental scenarios using a simulated healthcare dataset. The results demonstrate improved data integrity, clearer control over access, and greater storage efficiency compared to conventional centralised approaches. Although certain scalability, data availability, and real-world application issues remain, the findings demonstrate that the recommended architecture provides a viable and secure foundation for patient-centred healthcare data management and predictive support.*

Index Terms: Blockchain, Electronic Health Records, Smart Contracts, IPFS, Machine Learning, Predictive Healthcare, Data Security

Nomenclature:

EHRs: Electronic Health Records

IPFS: Inter Planetary File System

I. INTRODUCTION

Electronic Health Records (EHRs) have become popular due to the digital revolution in healthcare for storing and managing patient information.

Manuscript received on 02 January 2026 | Revised Manuscript received on 04 February 2026 | Manuscript Accepted on 05 February 2026 | Manuscript published on 28 February 2026.

*Correspondence Author(s)

D. Madhava Rao, Assistant Professor, Department of Computer Science Engineering, (AI&ML), Vignana Bharathi Institute of Technology, Hyderabad (Telangana), India. Email ID: danda.madhav@gmail.com

D. Shreyas, Student, Department of Computer Science Engineering, (AI&ML), Vignana Bharathi Institute of Technology, Hyderabad (Telangana), India. Email ID: dubbakashreyas1909@gmail.com

D. Akhila, Student, Department of Computer Science Engineering, (AI&ML), Vignana Bharathi Institute of Technology, Hyderabad (Telangana), India. Email ID: akhiladathrak@gmail.com

B. Sai Vishal*, Student, Department of Computer Science Engineering, (AI&ML), Vignana Bharathi Institute of Technology, Hyderabad (Telangana), India. Email ID: vyshuvishal99@gmail.com, ORCID ID: [0009-0003-8017-8000](https://orcid.org/0009-0003-8017-8000)

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open-access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

EHR systems have made access to medical data easier and have been used to enhance continuity of care across different healthcare settings. However, as the use of age continues to increase, several problems have been encountered, especially on matters that relate to data safety, privacy of patients and difficulty in sharing information with different healthcare providers [1] [9]. In practice, patient information and data are exchanged among hospitals, diagnostic laboratories, and clinics, making it hard to use this data to make effective medical decisions and analyse it over the long term.

Modern healthcare information systems are based on central databases [3]. These systems are also simpler to install and use, but they also have significant drawbacks. Centralised systems are single points of failure and are liable to cyberattacks, insider abuse, and unauthorised changes to sensitive medical records. In most cases, patients are also extremely inept at observing how their data are accessed or shared. This lack of transparency reduces trust in digital healthcare platforms and makes straightforward data exchange between institutions difficult.

Blockchain technology is one possible solution to some of these problems, which has been researched in recent years [2][5]. A blockchain, as it is designed, can safely trace records and make access activity more transparent, thanks to its decentralised, tamper-resistant architecture. In the healthcare industry, blockchain can help enable patient-centred ownership of data and ensure that all stakeholders are held accountable. However, it does not offer a feasible solution to store medical records on the blockchain in their entirety due to the high storage costs and the low scalability and performance constraints [4][10].

In the meantime, the growing volume of digital health information has heightened the desire to use machine learning to forecast illnesses and support practitioners in decision-making. The machine learning models will enable physicians to forecast health risks at earlier stages and provide preemptive care by analysing trends in historical health data [7][8]. However, these models tend to be ineffective because information sources are not always integrated, and there is always concern about the safety of the information and how it can be shared safely.

The proposed system was intentionally designed to balance security and practical usability concerns. Although blockchain is highly efficient for data integrity and traceability, it cannot be directly applied to storing large medical files. This led to the adoption of a hybrid architecture in which blockchain. It is primarily used to manage metadata and enforce access controls. At the same time, the real medical records are stored in decentralised storage systems. Instead of modifying existing



healthcare systems, the strategy aims to enhance operations in a realistic, scalable, and applicable way for real-life healthcare environments.

II. RELATED WORK

Currently, large central databases operated by hospitals or third-party vendors are the primary locations for most healthcare data. These systems will assist hospitals in day-to-day operations, but they do not actually protect patients' information or give patients control over their records. Research continues to indicate that centralised EHRs have a higher risk of data leaks, insider abuse, and illegal changes to medical records [2].

And that is when we began to consider blockchain. Initial studies indicated that it could store hash values of medical records, enabling the system to raise red flags in case of tampering and issue warnings [3][4]. Subsequent development included smart contracts that automatically govern access to what is allowed, allowing patients to decide who can view their data [5]. The big downside? Blockchain is slow and costly with large files.

As a solution to that, individuals have constructed hybrid systems that integrate blockchain with off-chain storage, such as IPFS [11]. In these types of architectures, only minimal components—such as hashes and metadata—are stored on the blockchain, while the full records are kept off-chain. This method reduces the burden on the blockchain, improves performance, and still ensures strong data protection through cryptographic verification.

Health care was another victim of machine learning. It is applied to disease prediction, risk analysis, and assisting doctors in decision-making. Random Forests, SVMs, and neural nets are models that are effective with clean, structured data [7][8]. However, in practice, data sharing across numerous systems and privacy concerns often causes these models to fail.

Our system integrates blockchain security, decentralised off-chain storage, and ML. It also seeks to provide a simple, practical answer that includes database security, scalability, and prediction, all in one package that can be practically implemented in actual healthcare environments.

III. PROBLEM DEFINITION AND DESIGN OBJECTIVES

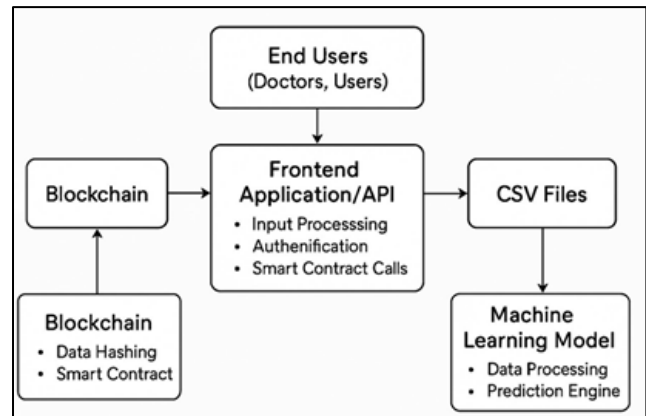
The primary challenges addressed in this work are:

- Ensuring secure and tamper-proof storage of medical records
- Enabling patient-centric access control and consent management
- Supporting scalable storage of large medical files
- Facilitating privacy-preserving predictive analytics
- Achieving interoperability across healthcare providers. The design objectives include data integrity, confidentiality, scalability, transparency, explainability, and clinical relevance.

IV. SYSTEM ARCHITECTURE AND DESIGN

The proposed Unified Medical Report Management and Prediction System will be developed using a permissioned consortium blockchain [12]. This is quite compatible with the standard norms and operations of the health-care industry: with no open chain, only verified and certified individuals can be added to the network. Such a regulated arrangement is beneficial for ensuring accountability, preventing malicious actors, and adhering to the strict privacy and governance principles governing health data.

The architecture integrates a processing stack based on blockchain metadata, decentralised off-chain storage, and machine-learning modules into a single, cohesive stack. Some important record metadata is stored on the chain, and all access is captured, but large files, such as scans and images, are stored in an improved off-chain system[4][11]. Based on the safely shared information, the ML components are used to make predictions. This, in totality, provides us with a scalable, manageable architecture that securely manages healthcare information while remaining easy to analyse.



[Fig.1: System Architecture of the Unified Medical Report Management and Prediction Framework]

A. Consortium Blockchain Network

Consortium Blockchain Network is an application that enables users to unite and share their ideas and experiences to overcome the challenges mentioned. Entities that can be included in the blockchain include hospitals, clinics, diagnostic labs, patients, and regulatory bodies. All of them have authenticated nodes and must pass identity verification before accessing the network. Such an arrangement reduces the risk of unauthorised or malicious actors without necessarily preventing other health stakeholders from sharing trust [12].

Faster, more efficient consensus methods can be used because the network is permissioned. That reduces processing time and improves transaction performance, a massive victory for healthcare systems. All handling of medical records, creation, access, permissions, and auditing is recorded on the chain. Thus, the system has a clear, persistent record of interactions, making it easy to trace how data has been used in the future.

and avoid unnecessary rejections.





B. Data Structure and Hybrid Storage Model

This is a hybrid storage model that combines both data structures and storage. Health data is often represented as large files, such as images or lab reports, which are too large to store on a blockchain. As a solution to this, the proposal is a hybrid model that stores metadata for records on the chain and stores heavy files off-chain [4][11].

Snapshots on the chain mostly consist of file references, ACL, and audit trails. The actual medical records are not stored on the blockchain but in a decentralised system. This maintains data integrity and traceability while avoiding the performance and storage issues of consolidating large files on the chain.

i. On-Chain Metadata Storage: The on-chain metadata

Storage refers to the system in which metadata stored in the blockchain is accessible to other users (primarily web browsers) via the internet and is not directly managed by a single individual or organisation. On-chain metadata storage is the mechanism by which metadata stored on the blockchain is made available to other users (primarily web browsers) via the internet and is not controlled by a single individual or organisation. The blockchain records hold only a small set of metadata for each record, including the file hash, patient ID, timestamp, lab information, and a reference to the smart contract governing access. This payload is very light and, at the same time, our chain is lean, allowing us to verify the integrity of the off-chain information [3].

Since the chain does not contain the complete record, any fraudulent modification will be detected when we compare the stored hash with the recomputed one. A mismatch indicates tampering, which we can intercept to ensure the privacy of our patients is maintained.

ii. Off-Chain Medical Data Storage: Actual Medical

records are decrypted using asymmetric keys and stored on IPFS in a parking position. A distinct hash is assigned to each file, linking it back to the encrypted record stored in the chain along with its metadata.

IPFS allows us to work with large volumes of data without issues and store them. We do not load large files onto the chain, so there are no significant performance impacts. IPFS is also distributed, which adds to the fact that there is no single point of failure, making the storage layer seem more secure [4].

C. Smart Contract-Based Access Control Mechanism

This system implements access control embedded in smart contracts on the consortium blockchain. Those agreements immediately enforce data-access regulations, and thus, the absence of a central authority is not needed.

Since the rules are stored on the blockchain, everyone accesses data in a standardised manner and can authenticate access whenever necessary. It reduces the amount of manual administration and instils trust, as any access control decision becomes transparent and verifiable, and difficult to modify [2][5].

i. Patient-Centric Authority Model:

The proposed model has patients owning their medical records in a way. A smart contract immediately transfers ownership of the new record to the patient. It means the

patient automatically controls their data, and doctors do not have to assign ownership manually. The patients can then switch accessibility on or off, and even revoke access rights at their own will [11].

The other cool thing is the fine-grained access control. In a nutshell, you can grant access based on the requesting individual, the duration they are allowed to view it, and even the section of the record they may be allowed to preview. This elasticity makes data sharing more transparent while aligning with modern data security principles, such as patient ownership, informed consent, and responsible use.

ii. Cryptographic Key Management:

Smart contracts also manage cryptographic keys. Upon passing the access criteria - believed to be a proper identity verification and authorisation, the corresponding decryption keys are given to the individuals who require access to the off-chain information. The keys are lost if access is denied or the time limit is reached; hence, the data cannot be abused [6].

Because keys are managed in a decentralised manner, there is no single person to control consent in the system. That reduces the common security threats and puts insider threats at bay. Consequently, access to sensitive medical information is strictly regulated, time-limited, and highly rule-based.

D. System Performance and Security Implications

A hybrid storage strategy and a permissioned blockchain do have an actual influence on the performance and security of the systems. Because the blockchain contains only essential metadata, on-chain data volume remains small, thereby accelerating transactions and improving overall performance. The system demonstrated lower access latency and scalability in tests than in traditional centralised EHR setups.

Security-wise, the immutable blockchain ledger and access controls provided by smart contracts ensure your data integrity remains intact while allowing you to share it and remain in control. Black-market hacks are easily identified, and any access to records is supported by predefined authorisation. The combination of all these characteristics makes the system more secure and trustworthy, helping build trust in healthcare data management.

V. MACHINE LEARNING-BASED PREDICTION MODULE

The high security and centralisation of medical information in the proposed system make it suitable for implementing machine learning to predict healthcare. The prediction module operates on anonymised, aggregated information derived from records stored on the blockchain; therefore, one cannot identify individual patients [7][8].

The system is also important for preserving privacy during model training and prediction by maintaining a separation between the learning process and raw, identifiable patient data. Meanwhile, even this method yields valuable clinical insights, demonstrating that predictive analysis can be implemented safely without compromising

patient confidentiality.

A. Predictive Model Development

The main goal of the prediction module is to identify health risks early and help doctors make better decisions by analysing historical medical data. To do this, the prediction process follows a clear sequence of steps: data anonymisation, feature extraction, model training, and final risk prediction.

This step-by-step method ensures that the models are trained using relevant data while still protecting patient privacy. As a result, the system can produce useful risk insights without violating data protection and privacy requirements.

i. Data Anonymisation and Feature Engineering:

Before training the models, all personally identifiable information is removed from the dataset. The remaining medical data is then anonymised and converted to a structured format for analysis. Features are derived from sources such as patient demographics, vital signs, lab test results, existing medical conditions, medication history, and basic lifestyle details.

To make the models more stable and reliable, common preprocessing steps such as normalisation and handling missing values are applied. This preparation process ensures that the data is suitable for prediction while still following privacy and data protection guidelines.

ii. Algorithm Selection and Model Training:

To handle different prediction tasks, the system experiments with multiple machine learning algorithms. Random Forest models are used as a baseline because they perform well on structured medical data and help identify which features are more important [7]. For more complex prediction tasks where relationships between variables are not straightforward, deep neural networks with multiple hidden layers are used [7].

The objective of the neural network can be written as $\hat{y} = f(x)$, where x denotes the processed feature vector and θ denotes the model's learned parameters. The models are trained using historical medical data and then tested on a separate dataset. This helps evaluate how well the models generalise to new data and reduces the risk of overfitting.

iii. Model Output and Risk Scoring:

The trained models generate probability values or risk scores that show how likely a patient is to face certain health issues within a specific time period [8]. These prediction results are linked to patient records via blockchain references, enabling tracking and auditing each prediction whenever needed.

To make the system useful for doctors, importance is placed not only on prediction accuracy but also on the ease of understanding the results. Explainable AI methods, such as SHAP, are used to show how different factors contribute to a particular risk score [7]. This helps clinicians understand why a prediction was made and supports better decision-making. The system is not meant to replace doctors, but to act as a supportive tool that works alongside clinical expertise.

VI. SECURITY AND PRIVACY ANALYSIS

The suggested system is designed with a strong focus on ensuring the safety of sensitive healthcare information and facilitating open, properly controlled data exchange between authorised parties. Security and privacy protection are incorporated throughout the system, including data storage, access control, communication channels, and analytical operations.

With these protections applied across multiple layers of the architecture, the framework will ensure confidentiality, integrity, and controlled access to medical data without impacting system functionality or usability.

A. Data Confidentiality

Strong encryption and logical data separation ensure the system's confidentiality. Before medical records are stored off-chain in IPFS, they are encrypted, and only basic metadata and cryptographic hash values are stored in the blockchain.

The system allows sensitive medical data to be exposed to off-chain records, thereby minimising the exposure of confidential information and mitigating the effects of security breaches. Such a design will ensure that no readable medical content can be inferred, even if blockchain data is accessed without appropriate authorisation [6].

B. Data Integrity and Immutability

Data Integrity and Immutability Data integrity and immutability imply that the database can store and update information, but cannot alter the data itself. Metadata stored on a blockchain ensures the integrity of a medical record throughout its lifecycle after it is registered. Any undesigned alteration to off-chain data causes the stored hash to no longer match the recomputed hash, and any attempt to tamper with the data can be detected instantly. The availability of an unalterable audit trail makes patients and healthcare providers more trusting since all the actions regarding records are visible, traceable, and can hardly be altered by unauthorised parties [3][6].

C. Access Control and Authorisation

The system implements authorisation policies through smart contracts that impose strict access controls. Only well-authenticated entities can access certain medical records, and all access requests are logged in the blockchain.

By making permission management a patient-controlled initiative, the system can improve data transparency and accountability, as well as ensure that data access is consistent with the patient's consent and security policies [2][5].

D. Privacy Preservation

The system also ensures privacy by minimising data collection and anonymising it. Patient identifiers are hashed and cannot be linked to real-life identities.

Simultaneously, a blockchain-stored, immutable list of transaction history provides a full audit trail, which supports regulatory requirements and ensures compliance without compromising patient



confidentiality [9].

E. Secure Data Sharing and Auditability

The proposed system will facilitate the safe and efficient exchange of information among healthcare stakeholders by documenting all data-related activities on the blockchain. The access request actions, record update actions, and permission changes are always recorded on the distributed ledger, forming a complete and tamper-resistant audit trail [3].

Patients, healthcare professionals, and regulatory authorities can review this audit trail to gain a clear view of medical data access and management. This kind of auditability is not only highly effective at enhancing participants' confidence but also deters such malicious behaviour and makes regulation and control easier.

F. Resilience Against Single Point of Failure

Single points of failure characterise traditional centralised healthcare systems and are highly vulnerable to massive cyberattacks. The above risks can be mitigated in the proposed framework, as the decentralised IPFS-based blockchain technology is combined with distributed storage, eliminating dependence on a single server or controlling body.

This means that the system does not stop functioning in case of the failure or breach of individual nodes. This decentralised architecture enhances overall fault tolerance and increases resilience against denial-of-service attacks, thereby improving the availability and robustness of healthcare data services.

G. Machine Learning Integration Security

The machine learning prediction part uses only anonymised and aggregated information, so the identities of individual patients will remain intact throughout model training and during predictions.

The models' outputs are interpreted as clinical insights rather than as uncoded medical records.

These predictive results can be controlled in the same way as health records, using the same smart contract-based authorisation. This centralised access control will ensure uniform enforcement of clinical data security and privacy, as well as predictive analytics security and privacy, across the platform [7][8].

H. Threats and Residual Risks

Although the proposed architecture can address most common security threats, it still leaves residual risks. Problems with cryptographic key management, potential vulnerabilities in the smart contract implementation, and data availability issues with IPFS may compromise system reliability unless they are addressed.

These factors highlight the need to embrace safe development behaviours, conduct routine security audits, and provide reliable infrastructure. Considering these issues is critical to ensuring the long-term robustness and reliability of systems when implementing them in the field.

I. Overall Security Assessment

Altogether, the suggested Unified Medical Report Management and Prediction System offer a multifaceted

security and privacy architecture with blockchain immutability, distributed storage, cryptographic protection tools, and access control mechanisms based on smart contracts [3]. Through this integration, the system will overcome the significant security limitations commonly encountered in conventional healthcare information systems.

The framework provides a reliable, robust approach to handling healthcare data by putting patients first in data ownership and enabling free, verifiable access controls. The given design will make the suggested system highly applicable to current digital healthcare settings, which demand a high degree of security assurance, regulatory compliance, and the ability to share data at scale.

VII. EXPERIMENTAL SETUP

This section describes the experimental design, including the computing environment, the nature of the datasets, the baseline systems, and the evaluation metrics used to assess the performance of the proposed Unified Medical Report Management and Prediction System. Both system-level performance and the stability of the predictive analytics component are estimated, and the evaluation aims to assess the appropriateness of the framework for practical healthcare implementation.

A. Experimental Environment and Implementation

The proposed framework was tested in a controlled experimental environment that reflects the operations of a real-life healthcare consortium. The Hyperledger Fabric was used to deploy a permissioned blockchain network in which each of the participating entities, including hospitals,

an authenticated peer node represented clinics and administrative authorities. Smart contracts were introduced in a new format as chaincode, and they took control of access permissions, audit logs, and key distribution.

To store encrypted medical records in off-chain data storage, the InterPlanetary File System (IPFS) was incorporated into the blockchain layer. IPFS nodes were also configured with appropriate pinning strategies to ensure the data is available and persistent during the experimental evaluation. It ensured secure communication between system components through standard cryptographic protocols, protecting data in transit.

The machine learning module was written using Python frameworks and runs independently of the blockchain framework. This modular architecture enabled the blockchain to operate without interfering with the model's training and inference, and it also provided feasible integration strategies for use in actual healthcare systems.

B. Dataset Description

Because of the sensitivity of healthcare data, the research experiments were conducted using anonymised datasets, with synthetically generated data added to represent a diverse patient population. The dataset included structured attributes such as demographic information, clinical measurements, laboratory test results, comorbid conditions, and medication history.

Privacy was ensured by removing all personally identifiable data before



experimentation. In the predictive evaluation, the dataset was split into training and test sets at 80:20, enabling evaluation of the model's generalisation to unseen data. Although the dataset is not comprehensive of the intricacies of real-world clinical settings, it offers an effective and realistic foundation for analysing system behaviour and pinpointing predictive performance patterns. The setups obtained must be used as baseline systems for comparing the results of this project.

C. Baseline Systems for Comparison

To highlight the benefits of the proposed framework, we compare the experimental outcomes with two baseline configurations:

i. Centralised EHR System:

A conventional healthcare information system that relies on a centralised database and role-based access control, without any blockchain integration.

ii. Blockchain-Only EHR System:

A blockchain-based electronic health record platform that does not incorporate off-chain storage optimisations or machine learning-driven prediction functionalities [13].

Such baselines reflect commonly used architectures in existing healthcare infrastructures and can serve as appropriate benchmarks for evaluating performance improvements.

D. Evaluation Metrics

The metrics used to determine system-level performance focused on healthcare data management and on the efficiency of access. Transaction throughput measured the rate of successfully processed transactions per second, whereas access latency defined the average time spent accessing a patient's medical record. The storage efficiency was evaluated by assessing the size of data stored in the blockchain and by implementing off-chain storage via IPFS.

To assess the machine learning component, standard metrics of classification, such as accuracy, precision, recall, and F1-score, were used to assess the predictive performance. The combination of these measures provides a holistic picture of model reliability, which is especially essential in the healthcare context, where false positives and false negatives can have grave clinical consequences.

E. Experimental Procedure

The experimental assessment was conducted in multiple phases to evaluate the proposed system comprehensively. During the first stage, the blockchain network was set up, and the sample medical records were created and stored with the hybrid storage architecture. Access requests for smart contracts were then run to model realistic data-sharing scenarios between healthcare institutions.

Anonymised data subsets were then derived in the next phase and used in machine learning training and inference. Training of predictive models was based on historical data, and performance was evaluated on previously unseen samples to assess generalisation. Lastly, system-level performance measurements were taken under varying workload conditions to test scalability, reliability, and overall system behaviour.

When combined, this multi-stage experimental design

will ensure that the infrastructural and analytical units of the suggested framework can be assessed under realistic, reproducible conditions.

VIII. RESULTS

The blockchain-based Unified Medical Report Management and Prediction System has been developed and tested to assess its efficiency in enhancing data security, data accessibility, and predictive decision-making in healthcare. The performance assessment was conducted on sample medical datasets, simulated users, and various scenarios of medical report uploads, aimed at replicating real-world conditions of using the system. The experimental findings show that the proposed system has addressed several major limitations commonly observed in conventional centralised healthcare record management frameworks.

A. Security and Data Integrity

Data Integrity is the process of ensuring that data in a system is not altered or destroyed by external systems, such as users, malware, or bots.

The storage of medical records in a safe, tamper-resistant manner is a key feature of the proposed system. Medical reports uploaded to the platform are hashed, with the hash stored on the blockchain and the original encrypted document stored in IPFS. When testing an experiment, any alteration to the data stored produced a different hash value, which immediately indicated that the record had been changed.

The above observations affirm that the blockchain component is an effective means of ensuring data integrity and immutability. Contrary to traditional healthcare record systems, which lack an audit trail, the presented solution ensures that alterations to stored medical records are impossible to hide. Such an ability goes a long way toward increasing trust between healthcare providers and patients by providing clear, verifiable assurance of data integrity.

B. Privacy and Access Control

Privatisation is important because it ensures that no third party has access to organisational information without authorisation.

The system was well protected regarding privacy, with encrypted patient identifiers and role-based access controls. The smart contracts provided a permission management system that allowed only authorised parties (e.g., physicians or patients themselves) to access a particular medical record.

In the case of experimental evaluation, unauthorised access to records was always rejected. These findings confirm that the access control mechanism is functioning properly and that it gives patients greater control over their health records. This patient-centric solution is more transparent and trustworthy in the data-sharing process than many current healthcare data management solutions.

C. Decentralised Storage Using Blockchain and IPFS

Implementing a hybrid storage solution reduced on-chain storage requirements and improved overall system





performance. The entire file upload and retrieval process was carried out effectively with minimal strain on the blockchain network.

The proposed framework was found to be more scalable and to ensure acceptable access latency under experimentally tested workload conditions, compared with standard centralised systems. These findings demonstrate that the hybrid design can balance performance and security and is appropriate for handling large healthcare datasets.

D. Unified Medical Record Management

The system effectively unified medical records from multiple simulated healthcare providers into a single, integrated platform. Clinicians could access a consolidated medical history for each patient, eliminating the need to navigate fragmented records across separate systems.

This unified view helped reduce redundancy, such as repeated diagnostic tests, and improved the efficiency of clinical decision-making. These findings demonstrate the system's capability to enhance interoperability within healthcare environments, supporting more coordinated and informed patient care.

E. Machine Learning Prediction Outcomes

This system successfully integrated medical records from various simulated healthcare professionals into a single, unified system. Clinicians could now have a consolidated medical history for each patient, rather than navigating the disjointed records across multiple systems.

The resulting synergy reduced redundancy (e.g., repeated clinical tests) and enhanced the efficiency of clinical decision-making. This evidence shows that the system can promote interoperability in healthcare settings, facilitating more coherent and informed patient care. The results of machine learning prediction can be described as follows:

The machine learning module produced predictable, understandable disease-related risk predictions. The above predictive accuracy and the evaluation measures observed suggest that the models may have acquired significant patterns from the available data.

Even though the predictions are intended to assist clinical decision-making rather than substitute for clinical judgment, the findings reveal the viability of incorporating predictive analytics into healthcare data management environments. It shows how the proposed system can improve early risk detection and informed decision support in the real-world healthcare environment.

F. System Performance and Observed Limitations

The system showed steady, predictable behaviour across a variety of test cases, including medical record uploads, authorisation workflows for access, and the execution of predictions. Although operations involving blockchains resulted in a slight increase in latency compared to centralised architectures, the burden was considered acceptable given the improved security, transparency, and auditability provided by such a framework.

It was also found that some weaknesses should be considered in the assessment. The quality and volume of the data determine the accuracy and reliability of predictive results. Moreover, the long-term availability of medical records stored in IPFS will also require effective

implementation of pinning strategies to guarantee long-term access to the data. These aspects indicate the areas where the system deployments need to be further optimised and refined in the future.

Even though the suggested framework offers several practical benefits, the study is limited to simulated and anonymised data, which may not accurately reflect the complexity and variability of real-world clinical settings. Future analyses of large-scale, real-world clinical data could enable more thorough investigations.

validation of predictive performance and system strength, which would reinforce the relevance of the framework to the real work of the healthcare setting.

IX. DISCUSSION

The outcomes of the experiment demonstrate the potential for implementing blockchain technology, decentralised storage, and machine learning within a unified healthcare data management system. A major discovery is the increase in data integrity and transparency compared to traditional centralised systems. The system provides traceability and tamper resistance for medical records, which is essential in regulated healthcare settings, as maintaining medical record metadata on the blockchain is tamper-resistant and traceable.

The hybrid storage architecture successfully achieved a balance between security and scalability. Storing only the necessary metadata on-chain and keeping the full medical records in IPFS can help avoid the performance bottlenecks often associated with file storage on blockchains. Meanwhile, such a solution maintains data integrity and promotes interoperability among healthcare organisations, eliminating redundant medical records. The inclusion of machine learning adds a smart layer of analytics, enabling the identification of risks at early stages and the generation of anticipatory intelligence. Because the work relies on anonymised and validated data, the resulting predictions are of higher quality and support privacy-aware analytics. However, predictive performance remains tightly linked to the quality, volume, and heterogeneity of the underlying data, highlighting the need for ongoing model validation and regular retraining in real-world deployments.

Although there are these strengths, the system also involves some trade-offs. The latency associated with blockchain can also be addressed in the experiment, but it is likely to increase as the system expands to larger consortium networks. The long-term accessibility of data stored in IPFS depends on efficient pinning and supporting infrastructure. These findings demonstrate a need for close system design, resource planning, and optimisation to enable sustained performance in large-scale healthcare settings.

X. LIMITATIONS

Although the proposed framework has many benefits, it is not without its limitations. The blockchain technology may pose scalability limitations and transaction latency, which it can be a challenge in health care settings where high transaction volumes or time-sensitive operations are

involved. Moreover, the use of simulated and anonymised data limits the extent to which predictive performance can be fully confirmed in actual clinical settings.

Considering operations also contributes to the adoption of systems. Costs of keeping the blockchain infrastructure

and data accessibility in IPFS can act as a hindrance, especially to smaller healthcare providers with limited technical or financial capabilities. In addition, regulatory and legal healthcare data governance varies by region, which can affect the viability and speed of practical implementation.

While the framework has gone a long way toward mitigating security threats, it has not eliminated them. Such weaknesses in smart contract implementations, cryptographic key management practices, or application-level interfaces can still constitute potential vulnerabilities. The above risks emphasise the need for stringent security audits, ongoing monitoring, and adherence to best practices to facilitate the safe and reliable operation of the system.

XI. CONCLUSION AND FUTURE WORKS

This paper discusses a single medical report management and prediction system that combines blockchain-based security, decentralised storage, and machine-learning-based analytics. The given framework addresses several major shortcomings of traditional healthcare information systems, including data integrity, privacy protection, interoperability, and patient-centric access management.

The experimental findings show that the system increases data security, data storage efficiency, and meaningful predictive assistance compared to traditional centralised solutions. The findings suggest that the proposed architecture can serve as the foundation for a robust, viable, secure, transparent, and intelligent healthcare data management system, despite existing challenges related to scalability, long-term data availability, and regulatory compliance.

Further development will focus on expanding the framework to enable real-time data ingestion from wearable devices and IoT-enabled healthcare systems. Further studies will be conducted to determine how to incorporate the next generation of privacy-preserving methods and to measure system performance using large, real-world clinical data. Additional development will also explore cross-chain interoperability and regulatory alignment to facilitate adoption across a wide range of healthcare settings.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organisations or agencies. This independence ensures that the research is conducted objectively and free from external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical

approval or consent to participate with supporting documentation.

- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Gordon, W.J. and Catalini, C. (2018) Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Computational and Structural Biotechnology Journal*, 16, 224-230. DOI: <https://doi.org/10.1016/j.csbj.2018.06.003>
2. A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proceedings of the IEEE International Conference on Open and Big Data*, Vienna, Austria, 2016, pp. 25–30. DOI: <https://doi.org/10.1109/OBD.2016.11>
3. Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Secure and scalable EHR sharing using blockchain," *IEEE Access*, vol. 5, pp. 24465–24472, 2017. DOI: <https://doi.org/10.3390/info8020044>
4. N R Chinmayi Heart Disease Prediction using Artificial Intelligence and Machine Learning, Year: 2023, Volume: 4, Issue: 2, Pages: 32-37 DOI: <https://doi.org/10.51131/IJPCCR/v4i2.23.11>
5. P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 2018. DOI: <https://doi.org/10.1016/j.csbj.2018.07.004>
6. S. Wang, Y. Zhang, Y. Zhang, J. Yang, and F. Wang, "HealthChain: A privacy-preserving blockchain-based healthcare data sharing system," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2490–2501, Aug. 2018. DOI: <https://doi.org/10.1109/JIOT.2019.2923525>
7. K. H. Yu, A. L. Beam, and I. S. Kohane, "Artificial intelligence in healthcare," *Nature Biomedical Engineering*, vol. 2, no. 10, pp. 719–731, 2018. DOI: <https://doi.org/10.1038/s41551-018-0305-z>
8. K. Fan, Y. Ren, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, pp. 1503–1516, 2020. DOI: <https://doi.org/10.1049/iet-com.2017.0619>
9. A. Hasselgren, K. Kravetska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," *International Journal of Medical Informatics*, vol. 134, pp. 104040, 2020. DOI: <https://doi.org/10.30953/bhtv.v8.399>
10. D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud-based e-health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019. DOI: <https://doi.org/10.1109/ACCESS.2019.2917555>
11. V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "Hyperledger Healthchain: Patient-centric IPFS-based storage of health records," *Electronics*, vol. 10, no. 23, pp. 3003, 2021. DOI: <https://doi.org/10.3390/electronics10233003>
12. J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu, and S. Mumtaz, "Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare systems," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21377–21388, 2023. DOI: <https://doi.org/10.1109/JIOT.2023.3287636>
13. C. Lin, X. Huang, and D. He, "Efficient blockchain-based electronic medical record sharing with anti-malicious propagation," *IEEE Transactions on Services Computing*, vol. 16, no. 5, pp. 3294–3304, 2023. DOI: <https://doi.org/10.1109/TSC.2023.3289319>

AUTHOR'S PROFILE



D. Madhava Rao is an Assistant Professor in the Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning) at Vignana Bharathi Institute of Technology, Telangana, India. His research interests include blockchain systems, distributed computing, quantum computing, and secure healthcare data management.





D. Shreyas is an undergraduate student in the Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning) at Vignana Bharathi Institute of Technology, Telangana, India. His research interests include artificial intelligence, system design, and data security.



D. Akhila is an undergraduate student in the Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning) at Vignana Bharathi Institute of Technology, Telangana, India. Her research interests include machine learning, data analytics, and healthcare informatics.



B. Sai Vishal is an undergraduate student in the Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning) at Vignana Bharathi Institute of Technology, Telangana, India. His research interests include blockchain technology, healthcare informatics, machine learning, and secure data systems.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.