Cureus Journal of Computer Science

Open Access Original Article

Secure and Intelligent Electronic Health Records: A Cloud-Based AI-Blockchain Framework

Ritu Singhal [1] , Ananya Singhal [2] , Ishita Singhal [3] , Vikas Bansal [4]

1. Department of Computer Science, Indraprastha College for Women, Delhi, IND 2. Department of Electronics and Communications, Maharaja Surajmal Institute of Technology, Delhi, IND 3. Department of Information Technology, Maharaja Surajmal Institute of Technology, Delhi, IND 4. IT, Xebia IT Architects India Private Limited, Delhi, IND

Corresponding author: Ritu Singhal, toritu7@gmail.com

Received 08/04/2025
Review began 08/20/2025
Review ended 11/03/2025
Published 11/10/2025

DOI:
https://doi.org/10.7759/s44389-025-09459-1

Abstract

In the evolving landscape of digital healthcare, the integration of artificial intelligence (AI) with secure data management technologies has become critical for enabling personalized, efficient, and reliable patient care. This study proposes a novel, multilayered electronic health record (EHR) framework that synergistically combines AI, blockchain, and cloud-edge computing to support predictive analytics, ensure data integrity, enhance scalability, and enforce secure access control. The architecture is composed of distinct layers, including stakeholder access, edge-level data acquisition, cloud-based AI-driven processing, integrated data management, and decentralized blockchain validation. To evaluate the system's predictive capabilities, several machine learning models, Logistic Regression, Random Forest, and XGBoost were trained and fine-tuned using a healthcare dataset. Among these, the Logistic Regression model demonstrated superior performance, achieving the highest receiver operator characteristic-area under the curve score. Additionally, blockchain was employed to validate the integrity of EHR documents through the comparison of cryptographic hashes between original and tampered records. The results underscore the proposed framework's robustness and intelligence, indicating strong potential for secure, real-time EHR management within digitally interconnected healthcare environments.

Categories: AI/ML-based decision support systems, Health Informatics, Safe and trustworthy AI in healthcare
Keywords: electronic health records (ehrs), blockchain, artificial intelligence, cloud computing, healthcare, security

Introduction

The global shift toward digitized healthcare has highlighted the immense potential of electronic health records (EHRs) to enhance clinical workflows, enable personalized treatment, and improve patient outcomes. However, this transformation also introduces critical challenges related to data privacy, integrity, access control, and real-time decision-making. Traditional centralized EHR systems often fall short in delivering secure, scalable, and intelligent solutions that meet the demands of modern healthcare. It is difficult to categorize and then run analytics on what is available from lab reports, prescription drugs, and diagnoses. Furthermore, the static nature of keeping data makes it difficult for healthcare providers to derive useful insights [1-3].

EHRs are digital systems maintained by healthcare professionals that store comprehensive patient information, including medical history, lab results, prescriptions, and administrative data. They support clinical tasks such as quality tracking, reporting, and data-driven decision-making. By integrating tools like telehealth platforms, e-prescribing systems, analytics dashboards, cloud computing, and patient portals, EHRs create an interconnected ecosystem that improves the efficiency, accuracy, and accessibility of healthcare delivery [4].

Recent advancements in artificial intelligence (AI) have enabled the extraction of actionable insights from vast amounts of patient data, supporting early diagnosis and predictive healthcare. Yet, without robust data governance and security mechanisms, these AI-driven outcomes remain vulnerable to manipulation or unauthorized access [5,6].

Blockchain technology addresses these concerns through immutable record-keeping, cryptographic hashing, and decentralized trust mechanisms [7].

Integrating AI and blockchain into EHRs promises enhanced security, efficiency, and personalization in digital healthcare. However, achieving real-time access and scalability requires the complementary support of cloud computing. When combined with edge computing, these technologies enable real-time analytics at the point-of-care while ensuring secure, traceable data exchange across healthcare networks.

This paper proposes a secure and intelligent framework that combines AI for personalized health analytics, Blockchain for immutable and verifiable access control, and a Cloud-Edge architecture for scalable, real-time processing. The AI component employs machine learning models for disease prediction and patient risk profiling. Blockchain ensures data integrity, auditability, and tamper resistance for EHR transactions. Edge computing supports low-latency inference at the point of care, while cloud computing handles long-term storage, large-scale computation, and cost-effective resource allocation. Cloud environments are simulated to validate real-time data retrieval and processing. Collectively, these technologies enhance decision-making, enable tailored treatments, and optimize healthcare operations.

The proposed model, an integrated AI-Driven, Blockchain-Secured EHR Framework, bridges these emerging technologies to overcome the limitations of traditional systems. It consists of multiple coordinated layers: a Stakeholder Layer for role-based interaction, an Edge Layer for real-time data collection and preprocessing, a Cloud Layer for scalable AI-based analysis, and a Blockchain Layer for validating data authenticity and preventing tampering.

To demonstrate the framework's viability, we developed and tested optimized machine learning models for clinical prediction, alongside a blockchain-based document verification system. The results confirm the framework's capability to deliver accurate healthcare analytics while ensuring robust data integrity. This integrated approach paves the way for a secure, intelligent, and patient-centered EHR system adaptable to diverse healthcare environments.

Problem statement

The exponential growth of digital health records and the increasing reliance on data-driven decision-making in healthcare have exposed serious gaps in existing EHR systems. Traditional EHR frameworks often operate in centralized environments, making them vulnerable to data breaches, unauthorized access, and lack of scalability. Furthermore, these systems lack intelligent capabilities to provide real-time clinical insights and personalized care recommendations.

In parallel, although AI holds promise for predictive analytics and decision support, integrating AI into real-world EHR systems is hindered by concerns about data privacy, explainability, and operational reliability. Cloud computing offers scalability but raises security concerns, while edge computing can improve real-time responsiveness but struggles with resource constraints.

Most critically, there remains an urgent need for a secure, verifiable, and intelligent EHR framework that not only supports accurate medical predictions using AI but also ensures data integrity, traceability, and interoperability across distributed healthcare environments. Thus, the core problem this research addresses is:

"How can we design a unified, intelligent EHR framework that leverages AI for healthcare predictions, ensures data integrity and trust using blockchain, and achieves real-time scalability through cloud-edge computing integration?"

This study seeks to fill that gap by proposing and demonstrating a novel AI-driven, blockchain-secured, cloud-edge enabled EHR framework that overcomes current limitations and provides a robust, scalable solution for modern digital healthcare. EHRs enable healthcare providers to standardize care, secure patient data, and enhance clinical outcomes. Quick and reliable access to EHRs improves decision-making efficiency for medical professionals and simplifies administrative tasks such as billing, medication refills, and appointment scheduling. Furthermore, multimedia data, including diagnostic imaging, can be seamlessly shared across healthcare organizations, ensuring continuity of care [8-10].

Integrating AI into EHR systems enhances the value and reliability of patient data. Machine learning algorithms can automate data-entry workflows, improve diagnostic precision, and reduce the administrative burden on clinicians [11]. By leveraging machine learning algorithms and natural language processing, AI can analyze massive volumes of EHR data, uncover anomalies, and support data-driven clinical decisions. By processing extensive datasets such as medical histories, laboratory reports, and imaging results, AI improves diagnostic accuracy by identifying patterns and correlations that might otherwise go unnoticed by human practitioners [12]. AI possesses the potential to enhance diabetes care by providing patients and medical providers with individualized, accurate, and data-driven support. AI can change diabetes care and raise the standard of living for millions of people worldwide by addressing issues and utilizing opportunities [13,14]. Additionally, AI-driven interface analysis supports the development of user-friendly designs, improving adoption and reducing usability challenges [15]. However, despite its potential for improving diagnosis, clinical decision support, and personalized treatment [16,17], AI integration raises ethical, legal, and regulatory concerns, emphasizing the need for robust governance frameworks [18,19].

Blockchain technology, known for its decentralization, immutability, and transparency, has emerged as a promising solution for securing medical data and addressing interoperability challenges [20-22]. Several studies have proposed blockchain-based EHR frameworks, demonstrating benefits such as tamper-proof data sharing and enhanced trust among stakeholders [23,24]. Yet, most implementations focus solely on security and data management, with limited integration of AI for intelligent, real-time analytics-highlighting a critical research gap. AI-focused approaches have incorporated federated learning with blockchain to preserve data privacy while enabling collaborative model training on the Multiparameter Intelligent Monitoring in Intensive Care dataset [25]. However, these frameworks often lack edge integration for real-time analytics, limiting their clinical applicability. Furthermore, review-based studies highlight the potential of combining AI, blockchain, and cloud computing but do not provide experimentally validated end-to-end implementations [26].

Cloud computing enables users to utilize computing resources including servers, storage, software, and various services over the internet. It provides flexibility, scalability, and cost-efficiency by allowing organizations and individuals to acquire resources on demand with minimal upfront investment [27,28] and contributes to environmental sustainability by optimizing resource utilization [29]. Operating on a pay-per-use basis, cloud computing supports multiple pricing mechanisms, including auction-based models, to deliver cost-effective infrastructure across diverse sectors such as education including barrier-free resources, government, and commercial enterprises [30,31]. In addition, several algorithms prioritize legitimate service providers to ensure fairness, authenticity, and quality of service delivery [32-34]. Cloud-based storage and computing capabilities have significantly enhanced the efficiency and scalability of EHR systems. This approach allows stakeholders to access EHRs via standard web browsers without the need to maintain complex infrastructure [35,36]. Emerging technologies such as AI and Blockchain increasingly rely on cloud infrastructure for computation and scalable resources [37,38], offering round-the-clock access to data and services from virtually any location.

The epidemic has caused the healthcare industry to shift its attention from old physical procedures to online ways of operation and large volumes of medical information are thus being uploaded to third-party systems, the cloud, on-site, and other platforms. The worries regarding the confidentiality and safety of healthcare data have arisen due to the massive digital data flow. Effective methods of managing data and safeguarding against cybersecurity threats are referred to as healthcare data privacy. Only those who are authorized can access patient data and health records thanks to a set of rules and regulations that control data privacy in the healthcare sector. Table *1* summarizing the usage of blockchain in EHRs, seen as one of the secure solutions.

Blockchain use in EHRs	Purpose/Function	Benefits (Pros)	Limitations (Cons)	Application areas	References
Immutable Health Record Storage	Tamper-proof recording of patient health data	Ensures data integrity and auditability	Large data storage on-chain is inefficient	Longitudinal patient records	[39]
Decentralized Data Management	Peer-to-peer access without central authority	Removes single point of failure, enhances transparency	Complex governance, interoperability issues	National health data exchanges	[40]
Patient-Controlled Access (Smart Contracts)	Enables dynamic, self-managed access permissions via smart contracts	Empowers patients, ensures fine-grained data sharing	Limited regulatory frameworks for smart contracts	Patient consent systems, data sharing	[41]
Interoperability Between Providers	Shared ledger across institutions with standard formats	Seamless exchange of records, reduces duplication	Adoption barriers, inconsistent standards	Multiprovider hospitals, health networks	[42]
Secure Health Information Exchange (HIE)	Tracks access and data exchange events on a public or permissioned ledger	Improves trust, supports regulatory compliance	Scalability concerns in high-throughput environments	Health data networks, insurance companies	[43]
Audit Trails and Compliance Monitoring	Real-time traceability of access history	Enhances GDPR/HIPAA compliance, builds transparency	May increase system latency	Legal audit, privacy compliance systems	[44]
Decentralized Identity (DID) for patients	Links patients to health data across systems via blockchain IDs	Reduces data fragmentation, improves access	Standardization and privacy risks in identity verification	Cross-border or mobile patient profiles	[45]
Tokenization and Incentive Models	Enables incentivization and monetization of health data use	Encourages data sharing for research, enables traceable rewards	Ethical issues, unclear legal frameworks	Clinical trials, health research consents	[46]

TABLE 1: Applications of Blockchain in EHRs.

EHR, electronic health records; GDPR, general data protection regulation; HIPAA, Health Insurance Portability and Accountability Act.

Some of the researchers explored hybrid blockchain-cloud consent management systems to facilitate secure data sharing, though these solutions remain constrained by cloud dependency and synchronization overhead [47,48]. Very few studies leverage a unified architecture that integrates AI, Blockchain, Cloud, and Edge computing for both secure data management and intelligent decision-making. Therefore, there exists a critical research gap in developing a holistic AI-driven, blockchain-secured, cloud-edge-enabled EHR framework capable of real-time analytics, privacy-preserving data sharing, and scalable healthcare operations, validated using real-world clinical datasets. The proposed study aims to bridge this gap by combining these technologies into a single architecture while simultaneously evaluating both security and clinical performance metrics.

Significance of the work

The healthcare industry is at a pivotal juncture, where the need for secure, intelligent, and patient-centric EHR systems has become more critical than ever. Despite numerous advancements in digital health, existing EHR infrastructures still face major bottlenecks such as lack of real-time intelligence, limited interoperability, poor scalability, and vulnerabilities in data integrity and access control. This research addresses these challenges by proposing a novel, unified framework that integrates AI, blockchain technology, and cloud-edge computing into a single cohesive architecture.

Innovation in integration

While many existing studies focus on either AI-based prediction or blockchain-based security in healthcare, very few attempt to combine these technologies within a single, operational framework. The present work is distinctive as it simultaneously integrates AI models for predictive diagnosis, a cloud-edge infrastructure to enable real-time and scalable processing with 24×7 availability of computational resources, and blockchain for tamper-proof storage and verifiable document integrity. This multilayered fusion enables intelligent data utilization while also ensuring the core principles of security, traceability, and trust that are essential for handling sensitive medical records.

Moreover, unlike purely conceptual proposals, this study includes a functional demonstration of key components. Tuned machine learning algorithms - specifically Logistic Regression, Random Forest, and XGBoost, are trained on real patient data to evaluate predictive performance. In parallel, blockchain hashing is implemented to validate the authenticity of generated medical documents and to detect tampering. The proposed framework is designed in a modular fashion to mirror real-world deployment feasibility, making it suitable for both hospital information systems and remote or resource-constrained healthcare environments.

Significance for healthcare transformation

This framework offers a holistic, future-ready solution for digital healthcare that empowers clinicians with accurate, AI-driven insights, protects patient data using verifiable blockchain storage, optimizes data flow across devices using cloud-edge distribution and supports compliance with regulations like GDPR and HIPAA through immutable audit trails.

Contribution to research and practice

The proposed model contributes to digital health research at both technological and methodological levels. It provides a reproducible reference architecture that integrates AI with blockchain to deliver secure, intelligent, and auditable EHR management. Unlike prior studies that focus primarily on either data intelligence or security, our framework demonstrates a unified implementation that ensures both clinical decision support and tamper-proof data integrity. In doing so, it bridges theoretical advancements with practical application, offering a prototype system that also serves as a roadmap for future innovation. Key avenues include extending smart contracts for automated access control, incorporating federated learning for privacy-preserving model training, and enabling mobile health applications for scalable accessibility

Materials And Methods

Addressing critical healthcare challenges such as fragmented data, limited transparency, privacy risks, real-time accessibility, and delays in clinical decision-making, we propose a intelligent framework that serves as a blueprint for building a next-generation EHR ecosystem. It is particularly relevant in the post-pandemic era of digital healthcare, where trust, personalization, 24x7 access and security have become essential rather than optional.

Proposed EHR framework: AI-Blockchain-Cloud-Edge system architecture

The proposed model represents a cutting-edge architecture that blends AI, Blockchain, and Cloud Computing into an integrated EHR system. It introduces a multilayered structure that ensures seamless data flow, real-time intelligence, and high security, handling the biggest challenges in today's healthcare data management systems. The architecture of the proposed system is designed to redefine how healthcare data is captured, processed, stored, and accessed, ensuring intelligence, security, and efficiency across all layers. The framework is organized into the following interconnected layers as shown in Figure *1*:

(a) Stakeholders Layer

(b) Edge Computing Layer

(c) Cloud Layer

(d) AI Inference Layer

(e) Blockchain Layer

(f) Data Verification Layer

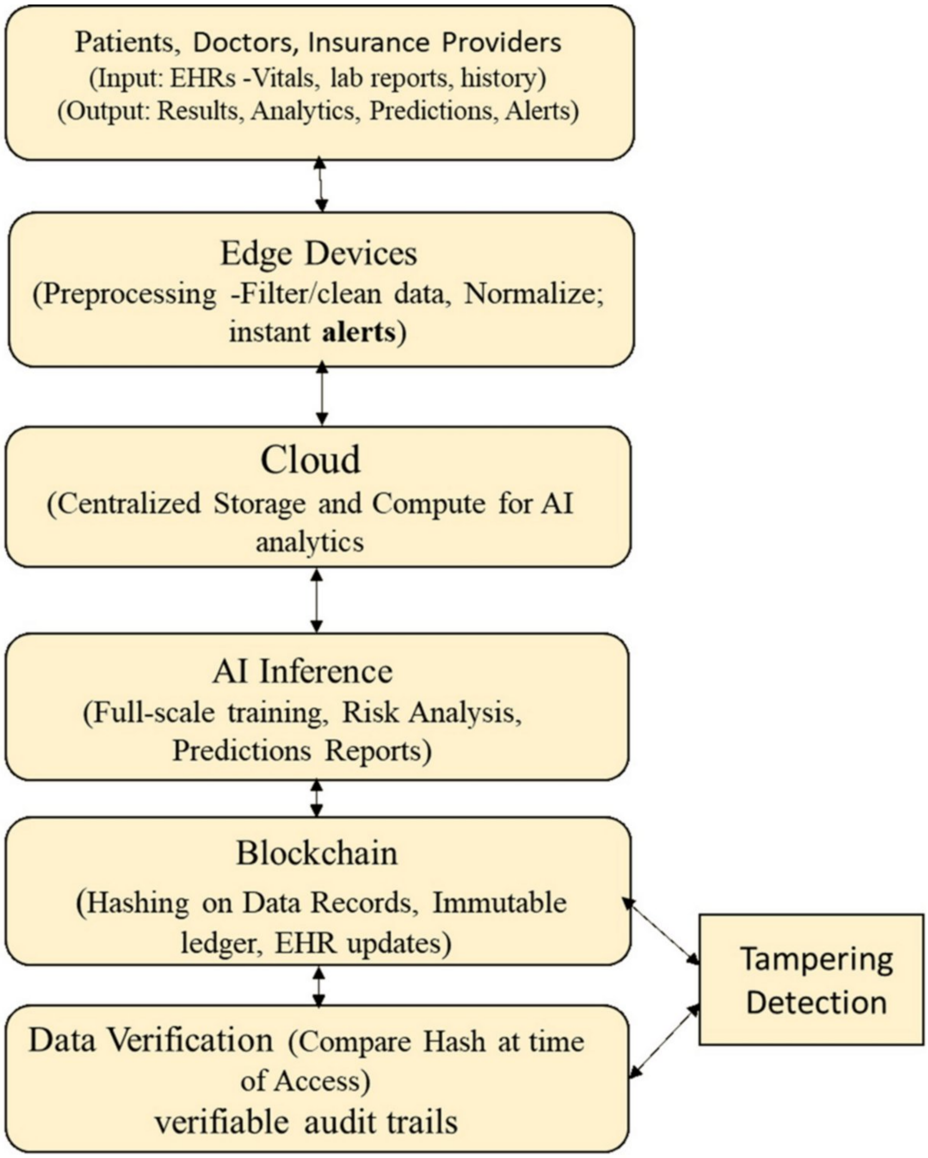


FIGURE 1: Proposed intelligent secure EHR framework.

AI, artificial intelligence; EHR, electronic health record.

The details of each layer are given below justifying novelty of proposed work.

(a) Stakeholders Layer (Top Layer)

At the top of the proposed architecture lies the Stakeholders Layer, encompassing the primary users of the EHR system including doctors, patients, hospital administrators, researchers, and regulatory authorities. This layer functions as both the entry and exit point for the entire system, forming the core interface through which stakeholders interact with health data.

Stakeholders interact with the system through various platforms including web portals, mobile applications, and connected smart devices, with access privileges assigned according to their specific roles. Doctors' access real-time dashboards for patient analytics, patients can view their medical history and reports, administrators manage compliance and records, and regulators audit data usage. Crucially, all these interactions are secured through blockchain-based authentication mechanisms that enforce consent-driven, role-specific access and maintain stringent privacy controls. The information flow at this layer is inherently bidirectional: stakeholders continually upload clinical data such as vital signs, prescriptions, or laboratory reports, while also receiving AI-generated results, alerts, diagnostic recommendations, and claims-related updates in return. The novelty of this layer lies in its capacity for context-aware, personalized access, ensuring that each user can interact with the system securely and appropriately, without jeopardizing data integrity. This dynamic and trust-based interaction significantly enhances the overall usability and reliability of digital EHR frameworks.

(b) Edge Computing Layer

Positioned directly below the stakeholders, the Edge Computing Layer serves as the real-time processing hub closest to the data source. It is deployed across hospitals, clinics, and patient environments including internet-of-things (IoT)-enabled medical devices, wearable tech, and local gateways [49]. This layer is responsible for the initial acquisition and rapid processing of medical data. Devices at the edge ingest high-frequency inputs from electrocardiogram (ECGs), glucose monitors, or pulse oximeters and perform preliminary tasks like data filtering, noise reduction, normalization, and validation. These steps ensure that only clean, usable data moves further into the system. More significantly, AI inference engines embedded at the edge execute immediate predictions and risk assessments like detecting cardiac anomalies or sudden glucose spikes. When such events are detected, instant alerts are generated, enabling timely responses at the point-of-care, without needing to wait for cloud-side processing. This design reduces latency, supports offline capabilities, and ensures real-time decision support. Compared to conventional EHR systems that rely solely on cloud infrastructure, this edge-intelligent setup offers a responsive, resilient, and localized approach, a critical advancement for time-sensitive healthcare delivery.

(c) Cloud Layer (Centralized Compute, Storage, and Data Management)

This layer serves as the backbone for centralized data processing, storage, and management. Once the edge devices preprocess the health data, it is securely transmitted to the cloud, where high-volume EHRs are stored and systematically organized. The cloud infrastructure ensures scalable storage for both structured and unstructured health data ranging from lab reports, imaging files, prescriptions, to real-time sensor data and provides the necessary compute power for high-volume analytics. The novelty here lies in the scalability and collaborative access enabled by the cloud, supporting distributed users like remote clinicians and health administrators.

In addition to storage, this layer performs comprehensive data management functions such as indexing, metadata tagging, compression, encryption, and maintaining data lineage. This ensures that the incoming health data is not only stored efficiently but is also searchable, interoperable, and ready for downstream AI analytics. It prepares curated datasets for the AI Inference Layer by filtering out noise, labeling patient records where required, and segmenting the data for model consumption. By integrating both data storage and management capabilities, the cloud layer minimizes local data storage and guarantees continuous data availability and readiness for secure processing, learning, and sharing, while adhering to healthcare compliance standards [50].

This layer ensures that data are always available and can be access from anywhere, scalable, redundant across zones, and ready to be fed into complex AI models for training and inference using compute resources. This layer harnesses the scalability of cloud platforms to support resource-intensive AI models such as disease classification, predictive diagnostics, patient clustering, or treatment recommendation systems. It also bridges multiple institutions into one unified EHR ecosystem.

(d) AI Inference Layer (Decision-Making & Risk Analysis)

AI Inference makes the EHR system intelligent. Leveraging machine learning algorithms, this layer performs deep risk analysis, anomaly detection, diagnosis support, and predictive analytics on the patient data [51,52]. AI models trained on thousands of cases offer insights that help doctors make faster, more accurate decisions. AI models are embedded across both edge and cloud layers. At the edge, lightweight machine learning models perform on-device inference. In the cloud, heavier models (e.g., XGBoost or deep learning architectures) are trained and updated with aggregated data. These models analyze structured and unstructured patient data to provide risk scores, diagnostics, treatment suggestions, or health trend predictions. The system supports feedback loops where model outputs can be reviewed by clinicians and refined over time. The uniqueness of the AI inference layer is its ability to provide personalized predictions tailored to a specific patient's profile rather than relying on generalized templates. Using real-time health inputs, this layer identifies early indicators of illnesses such as cardiac abnormalities or diabetic complications, thereby transforming the nature of preventive care. To determine its importance, in the implementation section, multiple machine learning algorithms including Logistic Regression, Random Forest, and XGBoost are trained and evaluated on the curated EHR dataset, and the results (as shown in the receiver operator curve (ROC) curve) demonstrate strong predictive performance.

This layer is responsible not only for centralized model training and continual updates, but also for supporting federated integration of EHR data across multiple healthcare centers and generating individualized prediction outcomes from both historical and real-time data streams. The outcome of these processes is communicated back to stakeholders in the form of visual dashboards, alerts, and treatment guidance, ensuring that end users receive actionable and data-driven clinical insights.

(e) Blockchain Layer (Tamper-Proof Security)

This layer serves as the foundational security mechanism of the proposed framework, enforcing data integrity, auditability, and trust across all system operations. As medical data traverses through the different layers of the architecture, it is hashed, timestamped, and immutably written into a distributed ledger so that each action - including patient uploads, physician modifications, or report generation - is securely logged using cryptographic mechanisms such as SHA-256 [53]. This process ensures that all records remain tamper-proof and traceable in compliance with standards such as HIPAA. In addition, smart contracts embedded within this layer dynamically regulate access control and patient consent, allowing only authorized personnel to retrieve or update health data. Such programmable contracts also automate authorizations and policy enforcement without manual intervention, thereby strengthening regulatory compliance and operational efficiency. The effectiveness of this approach is supported by our implementation results, which shows that every medical file or AI-generated report can be reliably validated by matching its hash with the ledger entry. This immutable audit trail not only prevents data manipulation but also enables full forensic inspection when required, ultimately reinforcing stakeholder confidence in the system.

(f) Data Verification Layer (Tampering Detection and Access Audits)

The final layer handles hash verification during data retrieval. Whenever a stakeholder accesses a record, the system regenerates its hash and compares it with the one recorded in the blockchain. If they do not match, tampering is immediately detected and flagged (demo shown in implementation section).

This layer not only maintains verifiable audit trails but also provides real-time integrity checks, making sure that data trustworthiness is preserved end-to-end. It brings a zero-tolerance mechanism against insider threats or breaches. Table *2* illustrates layered architecture of the proposed AI-powered secure scalable EHR framework workflow.

	Layer	Labels in Figure 1	Description/Function	Key contributions
1	Stakeholders Layer	Patients, Doctors, Insurance Providers	Interface for uploading health records (EHRs) and accessing predictions, alerts, reports.	Bidirectional interaction with role-based access control using blockchain.
2	Edge Computing Layer	Edge Devices	Real-time data preprocessing (cleaning, normalization) and instant alerts via AI deployed on local IoT devices.	Enables low-latency, localized decisions; triggers early alerts (e.g., anomaly detection) close to the source.
3	Cloud Layer	Cloud	Centralized compute and storage layer; scalable AI workloads run here after edge preprocessing.	Supports deep learning pipelines and large-scale analytics across hospitals or regions.
4	AI Inference Layer	AI Inference	Performs risk analysis, full model training, predictions, and generates interpretive reports.	Empowers healthcare professionals with real-time diagnostic support and predictive risk modeling.
5	Blockchain Layer	Blockchain	Provides data integrity through hashing, immutable ledger for transactions, and stores EHR updates securely.	Tamper-proof records and cryptographically secure updates.
6	Data Verification Layer	Data Verification (Compare Hash)	Compares hash values to verify data integrity upon access. Enables detection of unauthorized changes or breaches.	Adds transparency with verifiable audit trails, crucial for regulatory compliance and patient trust.
	Tampering Detection	Tampering Detection	Triggered if mismatch is detected during hash verification.	Enhances security monitoring with automated alerts for data tampering or unauthorized modifications.

TABLE 2: Layered architecture of the proposed AI-powered secure scalable EHR framework.

AI, artificial intelligence; EHR, electronic health record; IoT, internet of things.

Workflow of the AI-Blockchain-Cloud-Edge EHR system

The proposed system begins with the collection of patient data at the POC including vital signs, lab test results, ECG readings, or even inputs from wearable IoT devices. These inputs are immediately processed at the edge layer by lightweight AI models capable of detecting anomalies in real time; for instance, a patient arriving at an emergency unit with chest pain can have elevated cardiac risk detected instantly through ECG and blood pressure data. At the same time, the same data are transferred securely to the cloud layer, where more computationally intensive AI models perform deeper predictive analytics based on both real-time and historical datasets. In the cloud, advanced AI models trained on historical data of thousands of cardiac patients evaluate the patient's risk level, cross-reference prior medical history (if available), and suggest a personalized diagnosis and treatment plan. Throughout this process, every transaction from sensor data capture to AI inference and user access is cryptographically hashed and recorded immutably onto a private blockchain ledger, where smart contracts are used to enforce access permissions and patient consent policies.

To ensure data security, transparency, and tamper-proof access, every data transaction, starting from the initial sensor data capture to the AI-generated diagnosis, it is hashed and logged on a private blockchain network. Smart contracts govern who can access the EHR data and under what conditions. For example, if a cardiologist accesses the record, a blockchain transaction is triggered, verifying the doctor’s credentials and logging the activity immutably. When the patient is transferred to a different hospital or referred to a specialist, the receiving institution can verify the integrity of the EHR using the blockchain ledger. If any unauthorized change had occurred, it would be immediately detected via hash mismatch. This feature greatly reduces the risk of fraudulent or altered medical records.

Consider a real-time instance: A patient suffering from hypertension visits a clinic. The patient’s wearable continuously logs blood pressure and ECG data, sending it to edge devices for instant monitoring. One evening, an abnormal reading is flagged, and an alert is sent to the cloud. The AI model, trained on millions of cases, evaluates the trend and detects early signs of atrial fibrillation. A notification is sent to the patient's doctor via the stakeholder interface. Meanwhile, the entire activity like alert, AI inference, and physician access is logged immutably on the blockchain. Later, when the patient consents to share this data with a cardiologist, the smart contract allows it securely, while the hash verification layer ensures that the data has not been tampered with. This end-to-end scenario demonstrates how the system enables real-time, intelligent, secure, and patient-controlled healthcare proving its novelty and impact over conventional systems that operate in silos and lack automation, personalization, and tamper resistance.

This integrated pipeline demonstrates how the system delivers real-time, intelligent, and tamper-proof healthcare processing that beats traditional EHR systems by offering edge-based decision-making, secure cloud storage, blockchain audit trails, and seamless interoperability across institutions. The combination of speed, data integrity, personalization, and regulatory-grade security underscores the novelty and impact of the proposed framework in advancing trustworthy digital health systems.

Results And Discussion

This study adopts a two-phase methodology to demonstrate the power of AI algorithms for predictions on a healthcare dataset and for integrity verification of health records to emphasize the proposed framework’s robustness and intelligence, with a secure, real-time EHR management in a digital world: (i) AI model development and evaluation on an EHR dataset and (ii) blockchain-based integrity verification of EHR records.

Dataset description

The proposed framework was validated using the Pima Indians Diabetes Database, a benchmark dataset from Kaggle, originally sourced from the National Institute of Diabetes and Digestive and Kidney Diseases [54]. The dataset consists of 768 medical records of female Pima Indian patients aged 21 years and above, collected for diabetes prediction. Attributes include Pregnancies, Glucose level, Blood pressure, Skin thickness, Insulin level, Body Mass Index, Diabetes pedigree function, Age and Outcome (0 = No diabetes, 1 = Diabetes). This dataset is widely used in healthcare analytics for evaluating AI-driven diagnostic models due to its structured clinical attributes, suitability for classification tasks, and potential to demonstrate real-world applicability in an EHR-integrated environment [54]. The implementation is structured in two major phases: AI model performance on EHR dataset and blockchain-based integrity verification.

AI model performance on EHR dataset

Before evaluating the security layer, the machine learning models were first trained and validated using a curated EHR dataset. This section presents the setup and performance of the AI models, which form the intelligent core of the proposed framework.

Experimental setup for AI models evaluation

To assess the predictive capability of the proposed AI layer, a series of supervised machine learning algorithms including Logistic Regression, Random Forest, and XGBoost are implemented using Python (scikit-learn and XGBoost library) on a Pima Indians Diabetes dataset. The dataset was first cleaned by handling missing values and normalized using standard scaling techniques. The data were then split into training and test sets using a 75:25 ratio. Hyperparameter tuning was performed for each model using GridSearchCV with 5-fold cross-validation to select optimal parameter combinations.

The experiment is conducted in the Google Colab environment, which served as a cloud-based platform with 8GB RAM for executing the code using Python 3.11 and no GPU acceleration, indicating that the models are computationally feasible and reproducible even in limited-resource settings.

To evaluate how accurately machine learning algorithms can predict health conditions based on EHR data, we trained these three widely used models. The input dataset contained patient details such as age, blood pressure, glucose levels, and other clinical features. The goal is to predict the likelihood of a disease occurrence such as diabetes issues.

The trained models were then evaluated on the test set using five standard metrics: Accuracy, Precision, Recall, F1-Score, and ROC-AUC. Table *3* summarizes the key metric scores and observations for each model. Confusion matrix of each model is shown in Figures *2*-*4*. In addition, Figure *5* and Figure *6* show the ROC curves and Precision-Recall distributions, respectively, which visually confirm the numerical results in terms of classification quality and trade-off characteristics among the models. Random Forest performed best with an AUC of 0.83, whereas Logistic Regression followed with 0.82 and XGBoost had a slightly lower AUC of 0.80. These results confirm that the AI layer in our model is capable of robust classification and can support clinical decisions by predicting outcomes with high confidence.

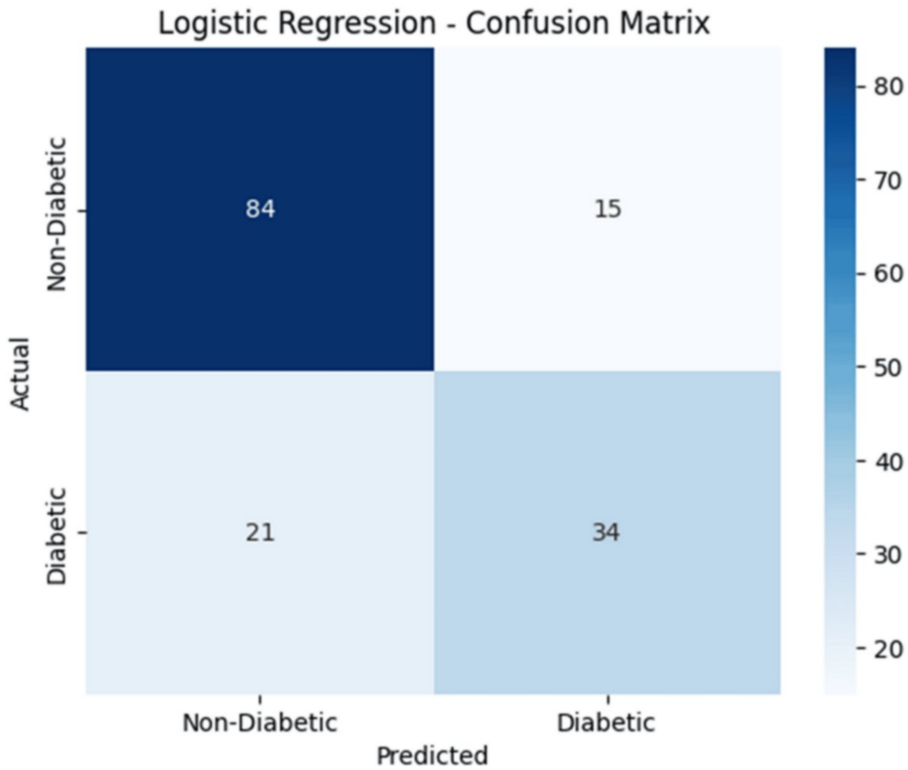


FIGURE 2: Confusion matrix for logistic regression.

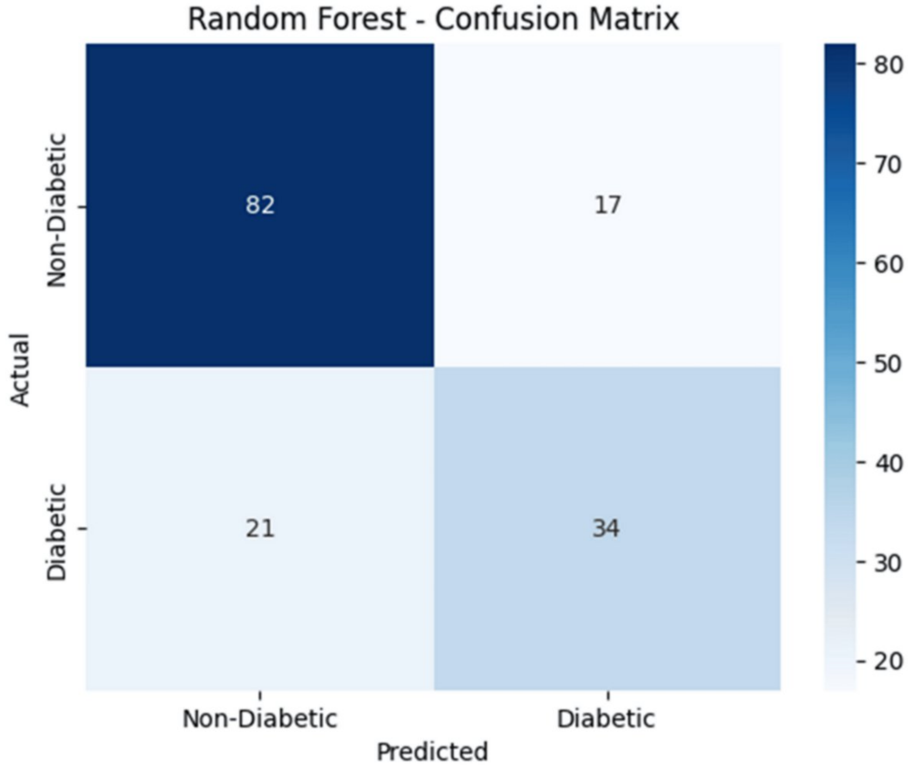


FIGURE 3: Confusion matrix for Random Forest.

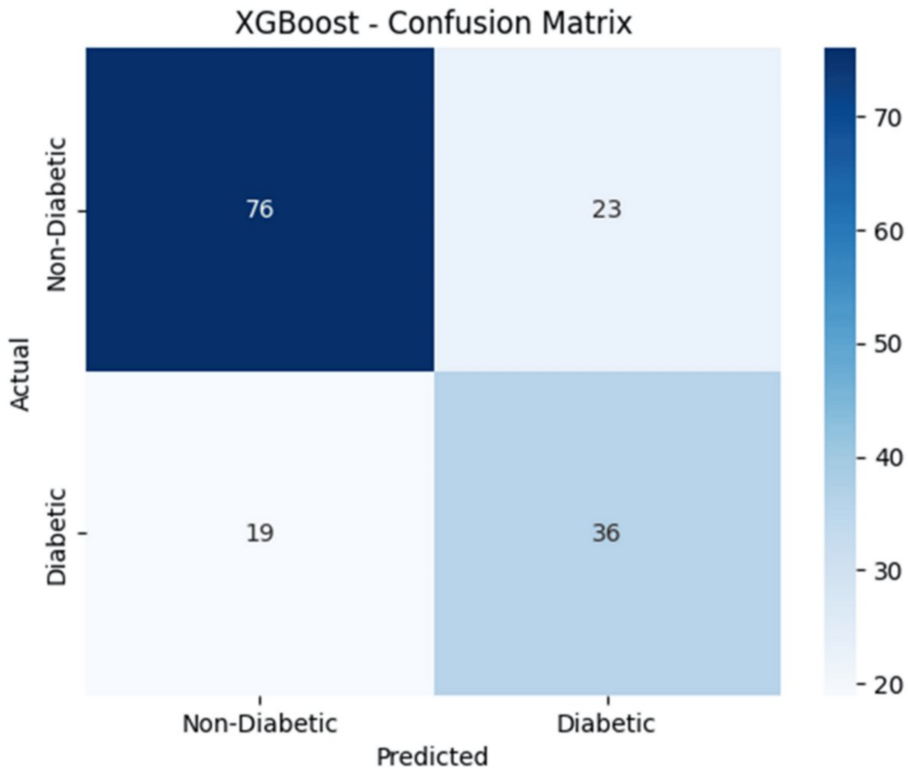


FIGURE 4: Confusion matrix for XGBoost.

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC	Key observations
Logistic Regression	0.77	0.69	0.62	0.65	0.823	Best precision, stable AUC
Random Forest	0.75	0.67	0.62	0.64	0.835	Best overall ROC-AUC
XGBoost	0.73	0.61	0.65	0.63	0.804	Highest recall, but lower AUC

TABLE 3: Performance metrics of ML models.

ML, machine learning; ROC, receiver operator curve; AUC, area under the curve.

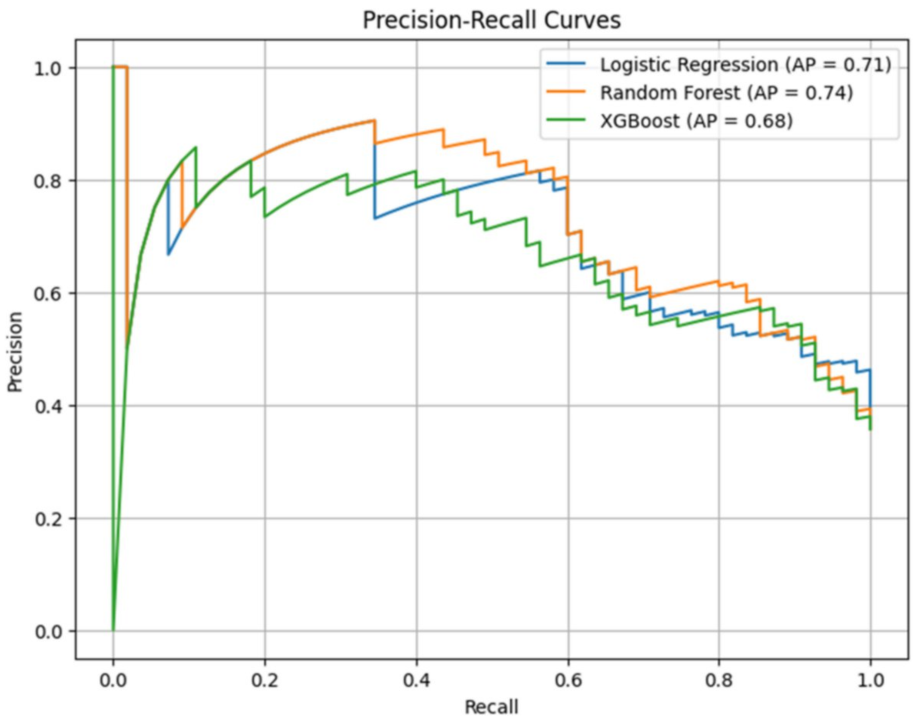


FIGURE 5: Precision recall curves of ML models.

ML, machine learning.

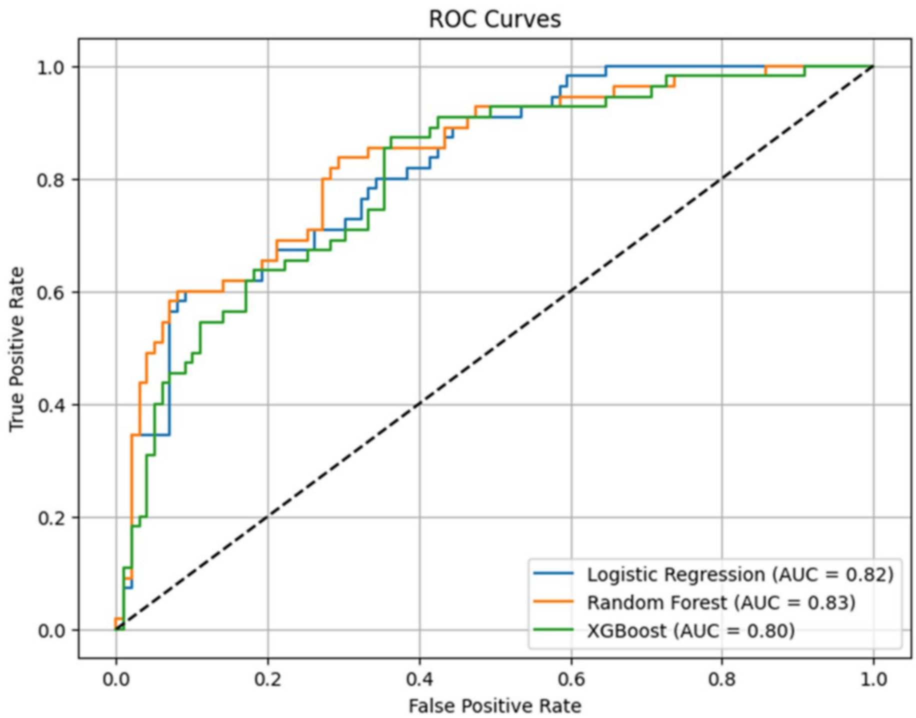


FIGURE 6: ROC curves of ML models.

ROC, receiver operating curve; ML, machine learning.

Blockchain hashing and integrity verification of health records

After accurate diagnosis using AI tools, it is essential that medical records remain unaltered, verifiable and prevent unauthorized tampering. To address this, we integrate a SHA-256 hashing mechanism [55] by a blockchain ledger to verify every uploaded EHR document. Following steps are taken for implementation and evaluation:

PDF Generation: Each patient's processed record was saved as a PDF document.

Cryptographic Hashing (SHA-256): Every medical record, transaction, or update is hashed and immutably stored on the distributed ledger, ensuring tamper-proof provenance. The SHA-256 hash was generated for each PDF file.

Timestamping and Immutable Ledgering: Each transaction (e.g., report upload, prescription update) is time-stamped and appended to the blockchain, providing a permanent and verifiable trail. The hash, along with metadata (e.g., timestamp, user ID), was stored in a simulated blockchain ledger.

Access Traceability and Tamper Detection: Any future access to the document involved re-hashing the file and verifying the hash against the one stored on the blockchain. The blockchain logs "who accessed what data and when," enabling forensic audits and regulatory compliance. If the file was modified, the hash would differ, instantly flagging potential tampering.

Experimental setup for blockchain hashing Implementation

To validate the integrity of EHR documents, a prototype hashing and verification algorithm is developed using Python (version 3.11). The experiment is conducted in the Google Colab environment, which served as a cloud-based platform for executing the code and uploading PDF files representing patient reports. For hashing, Python's built-in hashlib library was utilized to generate cryptographic SHA-256 hash values of the EHR files. Two types of files are uploaded manually in each test case - the original EHR PDF file (e.g., EHR_Report_Logistic.pdf) and a manually altered version of the same file (e.g., EHR_Report_Logistic_TAMPERED.pdf) for tampering detection.

During each run, the original file is hashed and the resulting SHA-256 value is stored inside a comma-separated value (CSV)-based simulated ledger (representing the blockchain). The file is then intentionally modified and re-uploaded to simulate an attack or unauthorized modification. A second hash is computed and compared to the stored value. If both hash values matched, the system logged the result as "Verified," indicating no tampering. If the hash differed, the system flagged it as "Tampered Detected." This hashing code is executed with support for file uploads and ledger logging using the key Python components hashlib for cryptographic hashing, pandas for storing and updating the ledger entries and Google Colab's files.upload() application programming interface for browsing and selecting files to test. All hashing outputs are recorded and saved in a CSV ledger file (ehr_blockchain_ledger.csv) along with the timestamp and verification status. The experimental outputs are visualized directly in the Colab notebook as shown in Appendix (Supplementary section), which include successful hash matches for authentic files and hash mismatches for tampered files and ehr_blockchain_ledger.csv. Hash Verification Results in both the cases as per Ledger are given in Table 4 as shown below.

Case	Patient ID	Test file	Original hash match	Tampering detected
Case 1	Patient001	EHR_Report_Logistic.pdf	Yes	No
Case 2	Patient001	EHR_Report_Logistic_TAMPERED.pdf	No	Yes

TABLE 4: Hash verification result in both the cases.

EHR, electronic health record.

Result analysis

This section evaluates the effectiveness of the proposed AI-Blockchain integrated framework for secure and intelligent EHR management. The results are reported in terms of both AI-based prediction performance and blockchain-based hash verification integrity. The performance of three machine learning classifiers Logistic Regression, Random Forest, and XGBoost is evaluated on the structured EHR dataset for diabetes prediction. Logistic Regression achieved the highest precision (0.69) and overall accuracy (77%), indicating strong performance in identifying positive cases with fewer false positives. Random Forest performed slightly better in terms of ROC-AUC (0.835), reflecting a superior ability to discriminate between classes across thresholds. XGBoost, while achieving the highest recall (0.65), had slightly lower precision and AUC, indicating a trade-off favoring the identification of more true positives at the expense of increased false positives.

These results suggest that different models excel in different metrics. Logistic Regression provides a reliable baseline with high interpretability, Random Forest offers robust discrimination, and XGBoost prioritizes sensitivity which is critical in early diagnosis scenarios. These findings support the integration of AI into the proposed EHR framework, offering data-driven personalization and clinical decision support within a secure blockchain infrastructure. AI models performance comparison is shown in Figure 7.

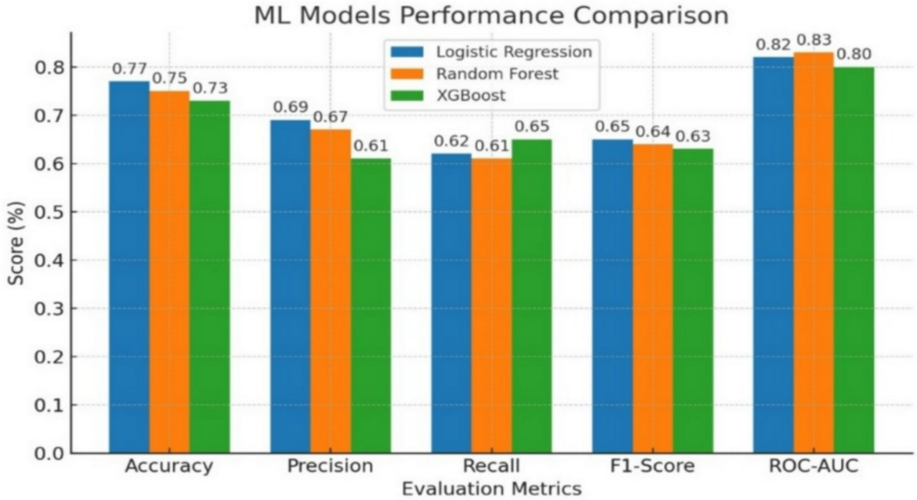


FIGURE 7: Comparative performance metric of ML models.

ML, machine learning; ROC, receiver operating curve; AUC, area under the curve.

Hash Verification Result for secure EHR management clearly demonstrates preservation of data integrity, and system resilience to insider and outsider threats. It can also be integrated with a permissioned blockchain network (e.g., Hyperledger or Ethereum private chain) for real-world deployment. To ensure the trustworthiness of AI predictions, each result was hashed at the time of model output and stored. During later access, hash values were recomputed and compared. No mismatch was detected, confirming verifiable audit trails and zero tampering. This validates the tamper-resistance offered by the Blockchain and Data Verification Layer. To ensure data integrity in experimentation, 120 records of EHRs are hashed and various combinations of files are uploaded for verification. Upon retrieval, hash values are recomputed and compared to detect tampering. Table *5* shows the verification results.

Parameters	Value
Records verified	120
Records with hash match	100
Tampered records simulated	20
Tampered records detected	20
Blockchain integrity maintained	Yes

TABLE 5: Hash verification results for 120 records.

This demonstrates that the system reliably flags any unauthorized modifications in EHR data, thus offering verifiable audit trails and real-time tamper detection.

The AI component not only aids in early prediction and patient risk stratification but also works in tandem with edge alerts. Simultaneously, blockchain ensures that any access or updates are securely logged, verifiable, and immutable. This holistic architecture ensures accuracy in healthcare prediction, data immutability through blockchain, and transparent access control all of which are essential for next-generation digital health systems. A simulation using EHR dataset demonstrates the proposed framework's feasibility. Results show improved classification performance and secure data handling.

Conclusions

This study proposes a secure, intelligent, and scalable EHR framework that combines AI, blockchain, and cloud-edge computing under role-based stakeholder access. The AI component utilizes three tuned machine learning models Logistic Regression, Random Forest, and XGBoost, to predict clinical outcomes from healthcare data. Random Forest achieved the highest ROC-AUC of 0.83, followed by Logistic Regression (0.8228) and XGBoost (0.8044), demonstrating reliable predictive capability. To ensure trust and data integrity, a blockchain-based hashing mechanism is implemented to detect tampering in uploaded EHR documents. The hash verification process successfully validated original files and flagged modified ones, highlighting the blockchain layer's effectiveness in safeguarding sensitive medical data.

Overall, the proposed multilayered framework including Stakeholder Interface, Edge Processing, Cloud with integrated data management, AI Analysis, and Blockchain Security proved effective for real-time processing, secure data storage, and personalized healthcare delivery. By blending intelligent prediction with tamper-proof verification, the framework provides a resilient EHR ecosystem capable of supporting modern and trustworthy digital healthcare.

Appendices

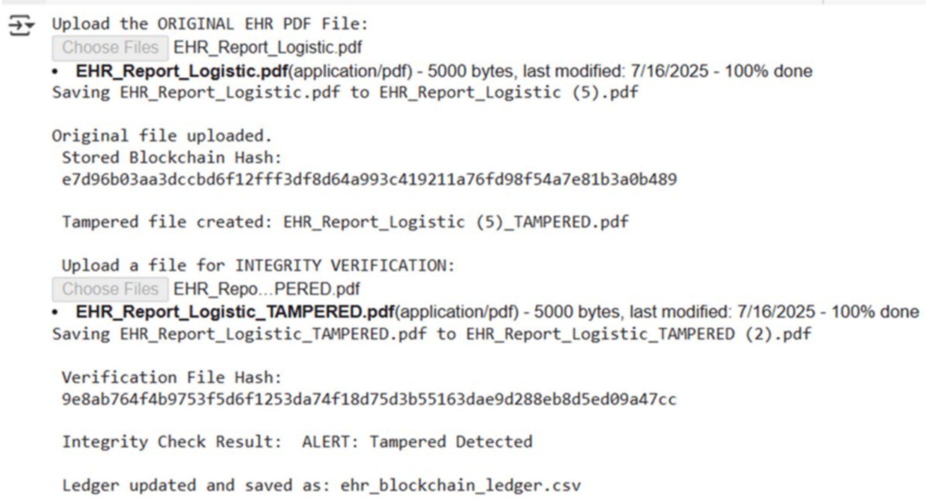
Appendix

(Supplementary Section)

```
Upload the ORIGINAL EHR PDF File:
Choose Files EHR_Report_Logistic.pdf
• EHR_Report_Logistic.pdf(application/pdf) - 5000 bytes, last modified: 7/16/2025 - 100% done
Saving EHR_Report_Logistic.pdf to EHR_Report_Logistic (2).pdf

Original file uploaded.
 Stored Blockchain Hash:
 e7d96b03aa3dccbd6f12fff3df8d64a993c419211a76fd98f54a7e81b3a0b489

 Tampered file created: EHR_Report_Logistic (2)_TAMPERED.pdf

 Upload a file for INTEGRITY VERIFICATION:
Choose Files EHR_Report_Logistic.pdf
• EHR_Report_Logistic.pdf(application/pdf) - 5000 bytes, last modified: 7/16/2025 - 100% done
Saving EHR_Report_Logistic.pdf to EHR_Report_Logistic (3).pdf

 Verification File Hash:
 e7d96b03aa3dccbd6f12fff3df8d64a993c419211a76fd98f54a7e81b3a0b489

 Integrity Check Result:  Verified: No Tampering

 Ledger updated and saved as: ehr_blockchain_ledger.csv
```

FIGURE 8: Case 1- Python code outcome for hashing.

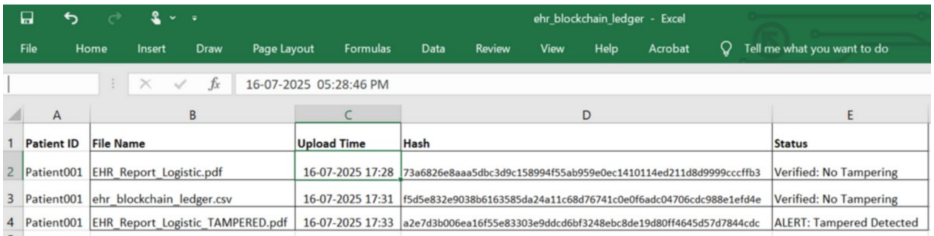
EHR, electronic health record.



```
Upload the ORIGINAL EHR PDF File:
Choose Files EHR_Report_Logistic.pdf
• EHR_Report_Logistic.pdf(application/pdf) - 5000 bytes, last modified: 7/16/2025 - 100% done
Saving EHR_Report_Logistic.pdf to EHR_Report_Logistic (5).pdf

Original file uploaded.
 Stored Blockchain Hash:
 e7d96b03aa3dccbd6f12fff3df8d64a993c419211a76fd98f54a7e81b3a0b489

 Tampered file created: EHR_Report_Logistic (5)_TAMPERED.pdf

 Upload a file for INTEGRITY VERIFICATION:
Choose Files EHR_Repo...PERED.pdf
• EHR_Report_Logistic_TAMPERED.pdf(application/pdf) - 5000 bytes, last modified: 7/16/2025 - 100% done
Saving EHR_Report_Logistic_TAMPERED.pdf to EHR_Report_Logistic_TAMPERED (2).pdf

 Verification File Hash:
 9e8ab764f4b9753f5d6f1253da74f18d75d3b55163dae9d288eb8d5ed09a47cc

 Integrity Check Result:  ALERT: Tampered Detected

 Ledger updated and saved as: ehr_blockchain_ledger.csv
```

FIGURE 9: Case 2 - Python code outcome for hashing (Tampered data).

EHR, electronic health record.



Patient ID	File Name	Upload Time	Hash	Status
Patient001	EHR_Report_Logistic.pdf	16-07-2025 17:28	73a6826e8aaa5dbc3d9c158994f55ab959e0ec1410114ed211d8d9999cccffb3	Verified: No Tampering
Patient001	ehr_blockchain_ledger.csv	16-07-2025 17:31	f5d5e832e9038b6163585da24a11c68d76741c0e0f6adc04706cdc988e1efd4e	Verified: No Tampering
Patient001	EHR_Report_Logistic_TAMPERED.pdf	16-07-2025 17:33	a2e7d3b006ea16f55e83303e9ddcd6bf3248ebc8de19d80ff4645d57d7844cdc	ALERT: Tampered Detected

FIGURE 10: ehr_blockchain_ledger.csv File for patient001 records.

EHR, electronic health record.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Ritu Singhal, Ishita Singhal

Acquisition, analysis, or interpretation of data: Ritu Singhal, Ananya Singhal, Vikas Bansal

Critical review of the manuscript for important intellectual content: Ritu Singhal, Ishita Singhal, Vikas Bansal

Supervision: Ritu Singhal, Vikas Bansal

Drafting of the manuscript: Ananya Singhal

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

Acknowledgements

Acknowledgments This article was previously presented at the ICETTEM Conference at Amity France on May 19, 2025.

References

1. Baltrusaitis K, Brownstein JS, Scarpino SV, et al.: Comparison of crowd-sourced, electronic health records based, and traditional health-care based influenza-tracking systems at multiple spatial resolutions in the United States of America. BMC Infectious Diseases. 2018, 18:1-8. 10.1186/s12879-018-3322-3
2. Tsai CH, Eghdam A, Davoody N, Wright G, Flowerday S, Sabine K: Effects of electronic health record implementation and barriers to adoption and use: a scoping review and qualitative analysis of the content. Life. 2020, 10:327. 10.3390/life10120327
3. Upadhyay S, Hu HF: A qualitative analysis of the impact of electronic health records (EHR) on healthcare quality and safety: clinicians' lived experiences. Health Services Insights. 2022, 15:1178632921107072. 10.1177/11786329211070722
4. Baumann LA, Baker J, Elshaug AG: The impact of electronic health record systems on clinical documentation times: a systematic review. Health Policy. 2018, 122:827-836. 10.1016/j.healthpol.2018.05.014
5. Bekbolatova M, Mayer J, Ong CW, Toma M: Transformative potential of AI in healthcare: definitions, applications, and navigating the ethical landscape and public perspectives. Healthcare. 2024, 12:125. 10.3390/healthcare12020125
6. Alowais SA, Alghamdi SS, Alsuhebany N, et al.: Revolutionizing healthcare: the role of artificial intelligence in clinical practice. BMC Medical Education. 2023, 23:1-15. 10.1186/s12909-023-04698-z
7. Panda SK, Jena AK, Swain SK, Satapathy SC: Blockchain Technology: Applications and Challenges. Springer, Switzerland; 2021. 10.1007/978-3-030-69395-4
8. Evans RS: Electronic health records: then, now, and in the future. Yearbook of Medical Informatics. 2016, 25:S48-S61. 10.15265/iys-2016-s006
9. Menachemi N, Collum TH: Benefits and drawbacks of electronic health record systems. Risk Management and Healthcare Policy. 2011, 4:47-55. 10.2147/rmhp.s12985
10. Murthi S, Martini N, Falconer N, Scahill S: Evaluating EHR-integrated digital technologies for medication-related outcomes and health equity in hospitalised adults: a scoping review. Journal of Medical Systems. 2024, 48:1-19. 10.1007/s10916-024-02097-5
11. Ehrenstein V, Kharrazi H, Lehmann H, Taylor CO: Obtaining data from electronic health records. . Tools and Technologies for Registry Interoperability, Registries for Evaluating Patient Outcomes: A User's Guide, 3rd edition, Addendum 2 [Internet]. Gliklich RE, Leavy MB, Dreyer NA (ed): Agency for Healthcare Research and Quality, Rockville, MD; 2019. 52-79. 10.23970/AHRQEPCREGISTRIES3ADDENDUM2
12. Kaur P, Kaushik A, Jyotsna, Singhal I, Pandey A, Singhal R: Advancing brain MRI segmentation using segment anything model. Procedia Computer Science. 2025, 260:110-117. 10.1016/j.procs.2025.03.183
13. Nomura A, Noguchi M, Kometani M, Furukawa K, Yoneda T: Artificial intelligence in current diabetes management and prediction. Current Diabetes Reports. 2021, 21:1-6. 10.1007/s11892-021-01423-2
14. Guan Z, Li H, Liu R, et al.: Artificial intelligence in diabetes management: advancements, opportunities, and challenges. Cell Reports Medicine. 2023, 4:101213. 10.1016/j.xcrm.2023.101213
15. Karaferis D, Balaska D, Pollalis, Y: Design and development of data-driven AI to reduce the discrepancies in healthcare EHR utilization. Journal of Clinical Medicine Research. 2025, 5:1-10. https://www.cmjpublishers.com/wp-content/uploads/2025/01/design-and-development-of-data-driven-ai-to-reduce-the-discrepancies-in-healthcare-her-utilization.pdf
16. Tsai ML, Chen KF, Chen PC: Harnessing electronic health records and artificial intelligence for enhanced cardiovascular risk prediction: a comprehensive review. Journal of the American Heart Association. 2025, 14:e036946. 10.1161/jaha.124.036946
17. Li YH, Li YL, Wei MY, Li GY: Innovation and challenges of artificial intelligence technology in personalized healthcare. Scientific Reports. 2024, 14:1-9. 10.1038/s41598-024-70073-7
18. Mennella C, Maniscalco U, De Pietro G, Esposito M: Ethical and regulatory challenges of AI technologies in healthcare: a narrative review. Heliyon. 2024, 10:e26297. 10.1016/j.heliyon.2024.e26297
19. Apell P, Eriksson H: Artificial intelligence (AI) healthcare technology innovations: the current state and challenges from a life science industry perspective. Technology Analysis and Strategic Management. 2021, 35:179-193. 10.1080/09537325.2021.1971188
20. Zhang P, Schmidt DC, White J, Lenz G: Blockchain technology use cases in healthcare. Advances in Computers. Raj P, Deka GC (ed): Elsevier, New York; 2018. 111:1-41. 10.1016/bs.adcom.2018.03.006
21. Usharani S, Bala P, Rajmohan R, Kumar TA, Pavithra M: Blockchain technology use cases in healthcare management: state-of-the-art framework and performance evaluation. Blockchain, Artificial Intelligence, and the Internet of Things. Raj P, Dubey AK, Kumar A, Rathore PS (ed): Springer International Publishing, Cham; 2021. 117-140. 10.1007/978-3-030-77637-4_7
22. Agbo CC, Mahmoud QH, Eklund JM: Blockchain technology in healthcare: a systematic review. Healthcare. 2019, 7:56. 10.3390/healthcare7020056
23. Attaran M: Blockchain technology in healthcare: challenges and opportunities. International Journal of Healthcare Management. 2020, 15:70-83. 10.1080/20479700.2020.1843887
24. Haleem A, Javaid M, Singh RP, Suman R, Rab S: Blockchain technology applications in healthcare: an overview. International Journal of Intelligent Networks. 2021, 2:130-139. 10.1016/j.ijin.2021.09.005
25. Ali AA, Gunavathie MA, Srinivasan V, Aruna M, Chennappan R, Matheena M: Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare. Clinical eHealth. 2025, 8:125-133. 10.1016/j.ceh.2025.04.002
26. Bathula A, Gupta SK, Merugu S, et al.: Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. Artificial Intelligence Review. 2024, 57:1-123. 10.1007/s10462-024-10873-5
27. Singhal R: Introduction to cloud computing (AWS). Authors Press, Delhi; 2025.
28. Singhal R, Sonia, Singhal A: Rising future of agile software development using cloud computing: a study using

cloud computing in different phases of an agile method-SCRUM. International Journal of Computer Technology & Applications. 2016, 7:240-246.
29. Singhal R, Singhal A, Sharma V, Saachi: E-cloud: a solution towards e-waste management for educational institutions. International Journal of Recent Technology and Engineering. 2019, 8:964-972. 10.35940/ijrte.b1184.0782s619
30. Singhal R, Singhal A, Sonia: Towards a generic e-cloud architecture for universities. International Journal of Web Applications. 2016, 8:36-43.
31. Singhal R, Singhal A, Bhatnagar M, Malhotra N: Design of an audio repository for blind and visually impaired: a case study. Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing. Mandal J, Bhattacharyya D, Auluck N (ed): Springer, Singapore; 2019. 702:77-85. 10.1007/978-981-13-0680-8_8
32. Singhal R, Singhal A: A combinatorial economical double auction resource allocation model (CEDARA). International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon). 2019, 497-502. 10.1109/COMITCon.2019.8862456
33. Singhal R, Singhal A: A combinatorial fair economical double auction resource allocation model. Advances in Computing and Data Sciences. ICACDS 2019. Communications in Computer and Information Science. Singh M, Gupta P, Tyagi V, Flusser J, Ören T, Kashyap R (ed): Springer, Singapore; 2019. 1046:272-281. 10.1007/978-981-13-9942-8_26
34. Singhal R, Singhal A: A feedback-based combinatorial fair economical double auction resource allocation model for cloud computing. Future Generation Computer Systems. 2021, 115:780-797. 10.1016/j.future.2020.09.022
35. Aswini J, Yamini B, Jatothu R, Nayaki KS, Nalini M.: An efficient cloud-based healthcare services paradigm for chronic kidney disease prediction application using boosted support vector machine. Concurrency and Computation: Practice and Experience. 2021, 34:6722. 10.1002/cpe.6722
36. Rai V, Bagoria K, Mehta K, et al.: Cloud computing in healthcare industries: opportunities and challenges. Recent Innovations in Computing. Lecture Notes in Electrical Engineering. Singh PK, Singh Y, Chhabra JK, Illés Z, Verma C (ed): Springer, Singapore; 10.1007/978-981-16-8892-8_53. 855:695-707. 10.1007/978-981-16-8892-8_53
37. Singhal R, Sharma V, Singhal I, Bansal V: Blockchain-enabled auction for cloud resource provisioning: a survey on trust and economy. International Journal of System Assurance Engineering and Management. 2024, 15:2787-2807. 10.1007/s13198-024-02314-x
38. Singhal R, Singhal I, Sharma V, et al.: Artificial intelligence: revolutionizing industrial decisions . Data-centric Approaches to Industrial Decisions. Asset Analytics. Kapur PK, Alhazmi O, Singhal S (ed): Springer, Singapore; 2025. 317-327. 10.1007/978-981-96-7556-2_25
39. Guimarães T, Duarte R, Cunha J, Silva P, Santos MF: The role of blockchain technology in ensuring security and immutability of open data in healthcare. Blockchain and Applications, 5th International Congress. BLOCKCHAIN 2023. Lecture Notes in Networks and Systems. Machado JM (ed): Springer Nature, Cham; 2023. 778:317-327. 10.1007/978-3-031-45155-3_32
40. Shuaib K, Abdella J, Sallabi F, Serhani MA: Secure decentralized electronic health records sharing system based on blockchains. Journal of King Saud University Computer and Information Sciences. 2022, 34:5045-5058. 10.1016/j.jksuci.2021.05.002
41. Dutta J, Barman S: Smart contract and blockchain-based secured approach for storing and sharing electronic health records. Multimedia Tools and Applications. 2025, 84:16883-16907. 10.1007/s11042-024-19714-7
42. Reegu FA, Abas H, Gulzar Y, et al.: Blockchain-based framework for interoperable electronic health records for an improved healthcare system. Sustainability. 2023, 15:6337. 10.3390/su15086337
43. Lax G, Nardone R, Russo A: Enabling secure health information sharing among healthcare organizations by public blockchain. Multimedia Tools and Applications. 2024, 83:64795-64811. 10.1007/s11042-024-18181-4
44. Ahmed A, Shahzad A, Naseem A, Ali S, Ahmad I: Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: a quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology. PLOS One. 2025, 20:e0324285. 10.1371/journal.pone.0324285
45. Javed IT, Alharbi F, Bellaj B, Margaria T, Crespi N, Qureshi KN: Health-ID: a blockchain-based decentralized identity management for remote healthcare. Healthcare. 2021, 9:712. 10.3390/healthcare9060712
46. Kassab M, Nassabi S: Blockchain-driven incentive models for healthcare data sharing: challenges and opportunities. 2025 IEEE/ACM 7th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). 2025, 34-41. 10.1109/WETSEB66605.2025.00011
47. Mandarino V, Pappalardo G, Tramontana E: A blockchain-based electronic health record (EHR) system for edge computing enhancing security and cost efficiency. Computers. 2024, 13:132. 10.3390/computers13060132
48. Grover B, Kushwaha DK: Authorization and privacy preservation in cloud-based distributed ehr system using blockchain technology and anonymous digital ring signature. Health Services and Outcomes Research Methodology,. 2023, 23:227-240. 10.1007/s10742-022-00281-z
49. Singh A, Chatterjee K: Securing smart healthcare system with edge computing. Computers & Security. 2021, 108:102353. 10.1016/j.cose.2021.102353
50. Yadav S, Kaushik A, Sharma S: Simplify the difficult: artificial intelligence and cloud computing in healthcare. IoT and Cloud Computing for Societal Good. EAI/Springer Innovations in Communication and Computing. Verma JK, Saxena D, González-Prida V (ed): Springer, Cham; 2021. 855:101-124. 10.1007/978-3-030-73885-3_7
51. Wubineh BZ, Deriba FG, Woldeyohannis MM: Exploring the opportunities and challenges of implementing artificial intelligence in healthcare: a systematic literature review. Urologic Oncology: Seminars and Original Investigations. 2024, 42:48-56. 10.1016/j.urolonc.2023.11.019
52. Olawade DB, David-Olawade AC, Wada OZ, Asaolu AJ, Adereni T, Ling J: Artificial intelligence in healthcare delivery: prospects and pitfalls. Journal of Medicine, Surgery, and Public Health. 2024, 3:100108. 10.1016/j.glmedi.2024.100108
53. Jena SK, Barik RC, Priyadarshini R: A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare. Internet of Things. 2024, 25:101111. 10.1016/j.iot.2024.101111
54. Pima Indians Diabetes Database. Kaggle [Online]. Accessed: April 30, 2025:

https://www.kaggle.com/datasets/uciml/pima-indians-diabetes-database.

55. Fotohi R, Aliee FS: Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. Computer Networks. 2021, 197:108331. 10.1016/j.comnet.2021.108331