



Artificial Intelligence-enhanced Blockchain Telehealth Systems: Pioneering Secure and Intelligent Remote Healthcare Delivery

Waseem Ahmad¹, Sana Shahab², Tauseef Ahmad³, Mohd Anjum^{4,*}, Mohd Sadim⁵, Habib Figa Guye⁶

- ¹ Department of Computer Science and Engineering, Vishveshwarya Group of Institutions, Gautam Buddha Nagar 201314, Uttar Pradesh, India
² College of Business Administration, Princess Nourah Bint Abdulrahman University, PO Box 84428, Riyadh 11671, Saudi Arabia
³ Department of Information Technology, Rajkiya Engineering College, Azamgarh 276201, India
⁴ Department of Computer Engineering, Aligarh Muslim University, Aligarh 202002, India
⁵ Computer Science & Engineering Department, KCC Institute of Technology and Management, Greater Noida, Uttar Pradesh 201306, India
⁶ Department of Information Science, College of Informatics, Bule Hora University, Oromia 144, Ethiopia

ARTICLE INFO

Article history:

Received 15 July 2026
Received in revised form 10 October 2026
Accepted 21 October 2026
Available online 24 October 2026

Keywords:

Predictive Analytics; Blockchain; Telehealth System Research; Data Security; Gradient Boosting Machine

ABSTRACT

The artificial intelligence (AI)-enhanced Blockchain telehealth framework proposes a new architecture that addresses remote healthcare delivery challenges through AI and Blockchain technologies, making services secure, intelligent, and transparent. Traditional telehealth delivery models face significant data security, privacy, and trust concerns. This study addresses these issues by applying AI predictive analytics to assess service delivery risk among patient populations through patterns of telehealth utilization and accessibility across demographic, ethnic, and geographic cohorts. After collecting and preprocessing patient information from the Telehealth Services for Medicaid and CHIP Population dataset, a Gradient Boosting Machine model was developed, achieving 99.96 percent accuracy, 99.89 percent precision, 99.98 percent recall, and a 99.93 percent F1-score. The experimental evaluation showed promising performance, with very low gas consumption of about 22,500 units per transaction, a latency of 0.013 seconds, and a strong encryption throughput of 57.75 MB/s. These results confirm that the framework is scalable and highly efficient. Overall, the proposed framework would improve security, reliability, and interoperability in the telehealth ecosystem, supporting more robust, resilient, and patient-centered sustainable digital health initiatives.

*Corresponding author.

E-mail address: mohdanjum@zhcet.ac.in

<https://doi.org/10.65069/ara31202738>

© The Author(s) 2026 | [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

1. Introduction

The rapid advancement of artificial intelligence (AI), the Internet of Things (IoT), and blockchain has been transforming healthcare worldwide and opening new possibilities for intelligent, secure, and personalized telehealth solutions [1]. Remote consultations, combined with wearable monitoring and e-prescriptions, have opened up possibilities for greater data privacy, interoperability, and trust [2]. Conventional telehealth systems suffer from fragmentation and susceptibility to data leakage, thereby compromising patient trust [3]. Used together, AI and blockchain can thoroughly address the fundamental trust and privacy issues by providing an intelligent, transparent, and tamper-proof health service delivery system [4]. The purpose of this telehealth framework is to apply AI within blockchain technology in a meaningful way by enhancing the intelligence behind medical and related decisions, using resources more effectively, and protecting patient data [5]. The proposed framework will combine predictive analytics with decentralized data management, thereby establishing reliable and effective remote healthcare delivery [6]. Furthermore, in the long run, this combined approach will benefit the ongoing monitoring of patient health, support automated diagnostic systems, and create transparency in record maintenance [7]. In essence, the AI-Enhanced Blockchain Telehealth Framework is a digital healthcare ecosystem that promises greater safety, fairness, and a data-driven culture [8].

Modern approaches to telehealth security and intelligence include IoT-based healthcare monitoring systems, cloud-based storage of electronic health records, AI-driven predictive diagnosis, and stand-alone blockchain-based medical record systems. IoT systems provide real-time patient data and contextual health analytics, but most offer only simple encryption and can be hacked at any time [9]. While cloud-based approaches to healthcare delivery increase patient accessibility, they still raise concerns about patient privacy and single points of failure [10]. AI-driven diagnostic solutions (such as classifiers based on CNN, SVM, and various deep learning techniques) can deliver accurate results, but they currently operate in silos because secure data-sharing protocols are lacking [11]. Similarly, blockchain-based technologies such as Hyperledger Fabric can be used for the secure storage and transfer of medical records and provide immutability, but they face scalability issues and limited computational efficiency [12]. While each of these systems has a specific purpose, none provides a single interoperable solution that achieves intelligence, privacy, and efficiency at the same time [13]. As a result, they are not equipped to meet the demands of the rapidly evolving telehealth field, which requires both responsible data governance and predictive accuracy [14].

The AI-Enhanced Blockchain Telehealth Framework addresses the above problems through predictive modeling using a Gradient Boosting Machine (GBM) and data authentication using blockchain layers, minimizing dependence on human assessment while improving trustworthiness through automated smart contracts. Unlike past approaches, this framework provides end-to-end data security without compromising diagnostic intelligence. The blockchain layer serves as an immutable store for health records, prescriptions, and transactions, while enabling AI algorithms to perform health risk assessment and provide decision support with very high accuracy. Smart contracts automate actions, including the approval of prescriptions, the initiation of emergency services, and the settlement of claims, greatly reducing the potential for human error and fraud. The innovative aspect of this framework lies in its dual-layer design: AI provides analytical intelligence, while blockchain provides transparency and trust. This combination creates a connected telehealth ecosystem that is intelligent, secure, and scalable. Together, these features represent a new standard of care and monitoring in remote care delivery:

- construct an AI-backed, blockchain-based telehealth system to guarantee secure, intelligent, and transparent remote healthcare services, while leveraging seamless integration of AI, blockchain technology, and telecommunications;

- employ the Telehealth Services for Medicaid and CHIP Population dataset to gather, organize, and analyze patient demographic, medical, and telehealth interaction data for model training and validation;
- to ensure proactive and equitable healthcare delivery, set up an AI-driven GBM model to analyze preprocessed telehealth data and generate accurate predictions of telehealth service risks; and
- create a blockchain-based infrastructure that uses smart contracts to secure data transactions, authenticate digital prescribers, facilitate emergency response, and automate insurance claims and payments.

This paper is organized into five primary sections. Section 1 introduces the integration of AI and blockchain for secure and intelligent telehealth delivery, discussing the background, motivation, and goals in detail. Section 2 reviews the literature on AI, IoT, and blockchain in healthcare and highlights the corresponding privacy, interoperability, and scalability challenges. Section 3 outlines the methodology, covering data collection from the Telehealth Services for Medicaid and CHIP Population dataset, preprocessing, AI-based GBM health risk prediction, and integration with blockchain for data protection and automation. Section 4 presents the experimental results and discussion, showing an exceptional model accuracy of 99.96%, together with high efficiency and a low blockchain latency of 0.013 s. Finally, Section 5 concludes the paper with the major contributions of this study and outlines future research directions toward telehealth systems that are highly secure, patient-centric, and scalable through interoperable and federated learning technologies.

2. Related Work

The rapid pace of technological innovation, including AI, IoT, blockchain, and big data, has transformed global health systems into highly intelligent, robust, and patient-focused ones. Various studies conducted between 2020 and 2025 have investigated how these innovations have altered diagnostics, logistics, patient engagement, data security, and management in healthcare, as well as the ethical, infrastructural, and policy issues that accompany this transformation. Dash [15] first highlighted the worldwide growth of IoT in healthcare, fueled by the COVID-19 pandemic. This study underscored how digital connectivity transformed healthcare delivery while highlighting technology development, data privacy, and uneven adoption by healthcare workers as areas of concern. Building on this, Chen *et al.* [16] developed an intelligent regional health security monitoring and emergency medical response system based on IoT, big data, and AI to improve medical resource scheduling, ICU management, and infectious disease early warning—especially in less developed areas such as Ganzhou, Jiangxi, China. In the same way, Lakhwani *et al.* [17] developed an IoT-drone healthcare logistics system that achieved impressive efficiency improvements, including a 78% decrease in delivery times and a 65% reduction in carbon emissions, demonstrating the potential of AI and IoT to overcome environmental and logistical challenges in the remote delivery of medical supplies.

As healthcare infrastructures become more reliant on networked devices and data streams, security and trust have become the primary concerns. Alharbi *et al.* [18] proposed a blockchain-based system that incorporates smart contracts to protect IoT-enabled remote healthcare monitoring systems, making the data tamper-proof, transparent, and automated. Building on this premise, Shinde *et al.* [19] conducted a systematic review to investigate the possibility of using blockchain to protect AI-powered healthcare systems. The review detected critical deficiencies in data protection associated with training and using certain AI models, and therefore recommended blockchain solutions to enhance privacy and security in NLP, computer vision, and acoustic AI applications. Similarly, Saxena *et al.* [20] developed a framework using Hyperledger Fabric for chronic disease management (CDM),

addressing persistent challenges in data interoperability and access control. Their AI-based solution achieved 96% accuracy and an F1-score of 0.92, demonstrating the potential of blockchain and AI in secure and scalable healthcare systems.

AI is transforming healthcare in many areas. Deep learning and machine learning perform remarkably well in detecting and diagnosing diseases across various imaging modalities, from X-rays to CT scans, MRIs, and ultrasound. These applications also emphasize the importance of AI specialists and clinicians working together ethically and effectively to put these technologies into practice [21]. Rashid *et al.* [22] observed that AI is broadening horizons in diagnosis, surgery, and patient monitoring, while also carrying risks such as algorithmic bias and privacy breaches, and they called for cross-sector collaboration and continued funding for ethical AI research.

The integration of AI into both operational and patient-facing systems is revolutionary in its own right. Saini *et al.* [23] built an AI-based queue management model that reduced emergency patients' waiting times by 40% and improved resource allocation through reinforcement learning techniques, an approach that may scale to telemedicine for effective direct care. Khamaj [24] developed a chatbot designed primarily for older adults that offers various options for voice interaction, adjustable text, and personalized dialogue to enhance engagement and usability. Testing confirmed that older patients felt more engaged and that their satisfaction with healthcare providers increased, suggesting that AI could foster inclusiveness.

Wearable technology has become a frontier of innovation in AI-driven healthcare. Real-time physiological and biochemical data have enabled personalized, proactive care through wearable bioelectronics. Although these systems support the management of chronic conditions, interoperability, privacy, and ethical considerations remain concerns [25]. Other AI-based techniques include federated learning for preserving privacy and deep learning for noise reduction, which improve the accuracy and interoperability of wearable devices with electronic health records [26]. This study highlighted the potential of blockchain-based interoperability and of collaboration among stakeholders in developing a secure and scalable environment for digital health.

The widespread application of AI in health networks and hospitals has been highly beneficial. AIDhaen [27] measured the effect of AI on patient safety at hospitals within the Gulf Cooperation Council and reported a diagnostic accuracy of 95.2% and a significantly reduced incidence of medication errors and delayed treatment. The study demonstrated that AI helps improve operational efficiency while reinforcing the importance of digital literacy and training.

The digital revolution in healthcare would not have occurred without the emergence of AI, IoT, blockchain, and data intelligence, which together tie the studies reviewed above into a single narrative. The convergence of these technologies is establishing new standards for healthcare delivery, monitoring, and management, ranging from secure data handling and telemedicine provision to patient-centric care and smart logistics. However, as noted in the preceding discussion, ethical governance, open systems that enable interoperability, and alignment among stakeholders, namely policymakers, technologists, and clinicians, are still required. These technological changes foreshadow a digital healthcare environment that will be more accessible, secure, and equitable in the near future.

2.1 Problem Statement

Pre-existing safety and efficacy limitations, mostly tied to home telehealth models, have proven problematic for securing and retaining private information [28]. This study investigates the applicability of AI and blockchain technologies in addressing the gaps in telehealth systems to improve performance, security, and scalability [29]. The research aims to study the combined use of AI and blockchain to provide a secure and transparent route for accessing patient-controlled records while improving data authorization procedures in telehealth settings [30]. Moreover, the research seeks to

determine whether this integration could help mitigate cyberattack threats that appear to have been exacerbated by digital transformation in healthcare [31]. Building on this foundation, the research will further explore how the combination of computing technologies, namely AI, blockchain, and cloud computing, can address pressing needs for data privacy, real-time analytics, and system interoperability, ultimately fostering a healthcare delivery ecosystem that is secure, connected, and patient-centric.

3. Proposed Methodology for Secure and Intelligent Remote Healthcare Delivery

The data collection process is the first step in the workflow, in which Medicaid telehealth data are collected and subsequently stored on the blockchain for secure and tamper-proof storage. Then, in the preprocessing stage, which consists of data cleaning, feature engineering, and normalization and prepares the data for further analysis, the AI-driven data analysis and prediction process, as shown in Figure 1, uses the GBM to analyze the data and generate health risk assessments, which are also securely stored on the blockchain. The prescription and drug delivery step involves verifying digital prescriptions, with blockchain support to validate them and prevent fraud. The remote consultation process is supported by AI, which assists in making diagnoses, while the blockchain stores the consultation data to guarantee its integrity. The emergency service activation function reduces the time responders take to arrive and ensures that the emergency services are confirmed and logged. The pharmacovigilance stage monitors side effects and safety data, with the blockchain recording adverse drug reactions and safety information.

3.1 Data collection

A telehealth system with AI-augmented blockchain can collect data from patients in different ways, including electronic health records, telehealth service logs, and data from wearable devices. The primary source of such data is the Telehealth Services for Medicaid and CHIP Population dataset, which contains elements such as patient demographics, complete medical history, details of telehealth sessions conducted with patients, and real-time health metrics such as heart rate, blood pressure, and oxygen levels. Storing all data on the blockchain secures it, rendering it tamper-proof, transparent, and time-stamped for audit purposes. Blockchain technology not only provides a secure access system in which authorized users can view sensitive information, but also maintains the confidentiality and reliability of data. In addition, data obtained from telehealth interactions, such as consultations between doctors and patients, can be encrypted and recorded on the blockchain for greater visibility. This creates a robust data collection system that supports accurate AI analysis and health risk prediction. Ultimately, the collected data are used for continuous monitoring and healthcare improvement, enabling proactive care before patients become ill:

- Dataset Link - <https://data.medicaid.gov/dataset/651fa253-4dd4-4867-8725-2b5ae1dd5ce9>

3.2 Preprocessing

Data collection is followed by preprocessing, which ensures that the data are clean, consistent, and ready for analysis. The process handles missing data through imputation, using the mean for numerical data and the mode for categorical data. In addition, outliers are identified and removed using the Z-score method to maintain data quality. Finally, features are scaled or normalized so that all variables have an equal impact on the machine learning models, which improves performance.

Data cleaning involves handling missing or erroneous values to ensure high-quality data. For miss-

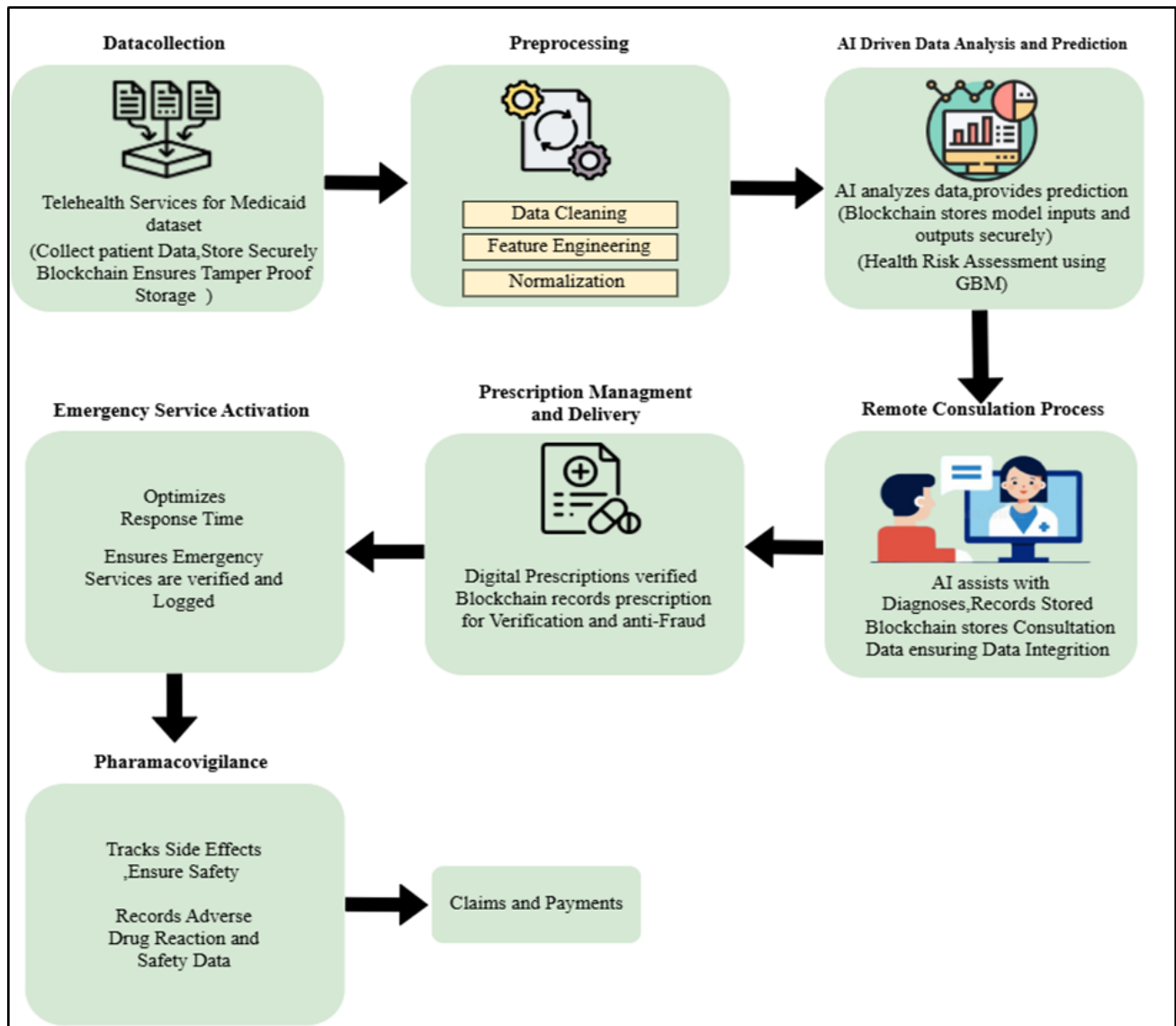


Fig. 1. AI-enhanced Blockchain telehealth system workflow

ing numerical values, imputation using the mean is applied, as shown in Eq. (1).

$$X_{\text{imputed}} = \frac{\sum_{i=1}^n X_i}{n} \quad (1)$$

For categorical data, mode imputation is used, and outliers are detected using the Z-score, where values $|Z| > 3$ are considered outliers. This ensures that the data are accurate and ready for analysis.

Feature engineering creates new features or transforms existing ones to improve model performance. For example, interaction features can be generated by multiplying two features, as shown in Eq. (2).

$$X_{\text{interaction}} = \text{Feature}_1 \times \text{Feature}_2 \quad (2)$$

For categorical variables, one-hot encoding is used to create binary columns, as shown in Eq. (3).

$$\text{Gender} = \begin{cases} 1 & \text{if Male} \\ 0 & \text{if Female} \end{cases} \quad (3)$$

To capture non-linear relationships, polynomial features can be created, as shown in Eq. (4).

$$X_{\text{poly}} = X^2 \quad (4)$$

Normalization and scaling are crucial for ensuring that all features are on the same scale, which improves the performance of machine learning models. Min-max scaling rescales data to a range of $[0, 1]$, using the formula shown in Eq. (5).

$$X_{\text{scaled}} = \frac{X - \min(X)}{\max(X) - \min(X)} \quad (5)$$

This ensures that all features contribute equally to the model, making it more efficient and accurate. In addition, other techniques like standardization and robust scaling can be used depending on the data characteristics, but min-max scaling is commonly applied in practice.

3.2.1 On-chain and off-chain data architecture

Figure 2 shows the interaction between on-chain and off-chain components in the AI-Enhanced Blockchain Telehealth System. On-chain, the blockchain manages hashes of records, prescription IDs, claim IDs, and timestamps to ensure integrity. The complete patient data, records, and diagnostic images remain securely stored off-chain in an encrypted database (or IPFS/cloud). A smart contract links on-chain hashes to off-chain encrypted data, ensuring auditability, security, and scalability while keeping sensitive patient data off the blockchain.

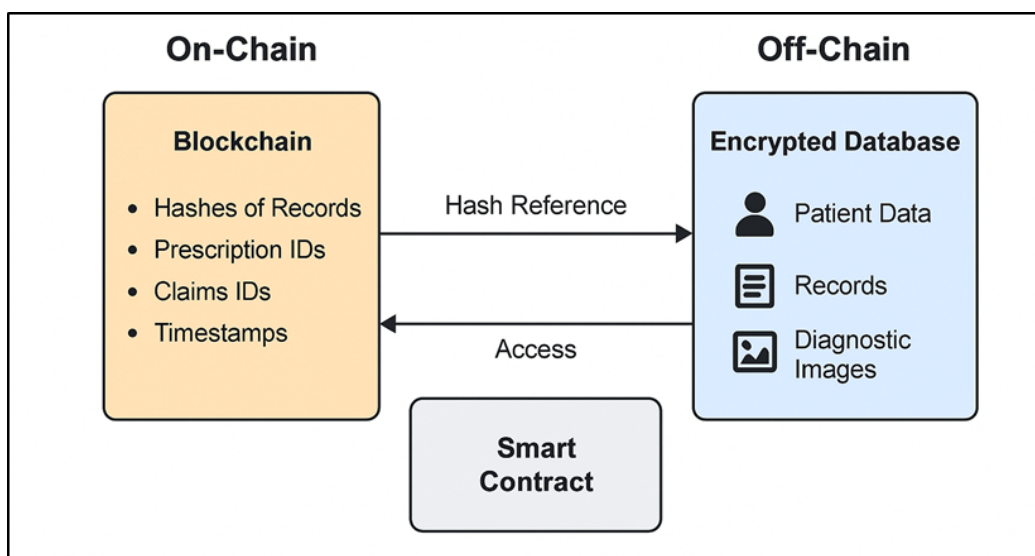


Fig. 2. On-chain and off-chain interaction

3.2.2 Data privacy and protection before Blockchain storage

The system applies rigorous protection and anonymization measures to the data before any data enters the blockchain, thereby ensuring compliance with privacy standards such as HIPAA and GDPR. All health information that can identify individuals, including names, medical history, and diagnostic reports, is encrypted and stored off-chain in secure cloud or IPFS repositories. Only hashed metadata, transaction logs, timestamps, and record identifiers are kept on-chain, which ensures immutability without exposing sensitive content. Each hash is a cryptographic fingerprint that provides proof of authenticity and integrity of the encrypted data while concealing any patient information. This two-layer design preserves privacy while providing the telehealth network with transparency and auditability.

3.3 AI-driven Data Analysis and Predictions using Gradient Boosting Machines

AI-driven data analysis and prediction apply AI models (e.g., GBM) to medical data to predict health risks. After collecting and preparing the data, which comprise patient demographic information, medical background, and real-time health measurements, the AI model evaluates it and assigns health risk classifications, including the probability that a patient will develop a chronic illness or be admitted to the hospital. These predictions, along with the original input data, are then stored on the blockchain for security. The blockchain makes it practically impossible to alter either the input data or the predictions, thereby providing a transparent and immutable record of the analysis. This means that the whole procedure, from data collection to prediction, is securely logged, giving healthcare practitioners confidence in the outcomes and the ability to trace any decision back to its original data source. In addition, the blockchain's transparency feature supports auditable records that can be scrutinized over time to verify the reliability and consistency of the health risk evaluations, thereby contributing to better healthcare decision-making and enabling "always on" monitoring of patient health. Figure 3

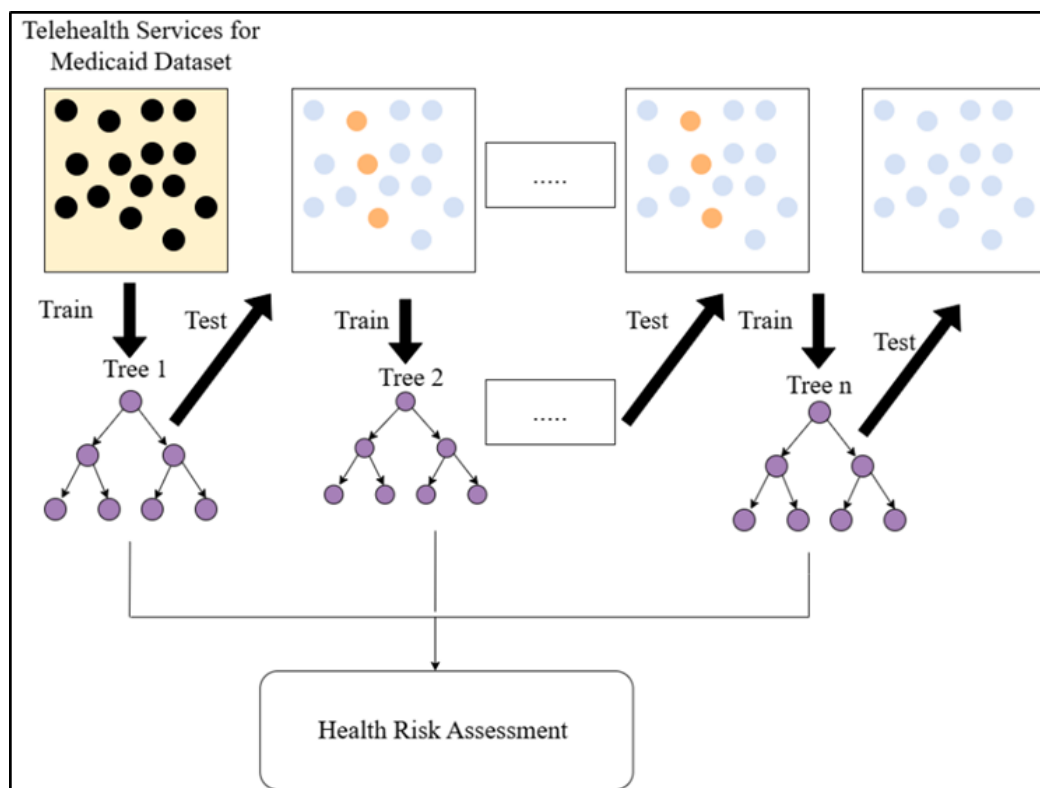


Fig. 3. Architecture of gradient boosting machines for health risk prediction

illustrates the full process of health risk prediction using GBM on the Telehealth Services for Medicaid and CHIP Population dataset. The first step is splitting the dataset into training and testing sets. Decision trees (Tree 1, Tree 2, ..., Tree n) are trained in parallel on the same training data, with each tree learning different aspects of the data. Afterward, the individual trees are evaluated on the test set and their performance is measured. The predictions of all the trees are then combined (boosted) to produce a final, more accurate model. Through this ensemble learning technique, health risk predictions, for instance, those for chronic diseases, are significantly improved as the individual tree predictions are summed, making the model more robust and trustworthy for medical personnel's decision-making.

In GBM, multiple decision trees are trained iteratively. Each tree focuses on correcting the errors (residuals) of the previous tree. The first tree is trained on the full training data. After the first tree, subsequent trees are trained on the residuals (errors) left by the previous trees. This process improves

the model iteratively. For tree t , the prediction is given by

$$f_t(x) = \sum_{i=1}^m w_i \cdot h_i(x) \quad (6)$$

where $f_t(x)$ is the prediction for the t -th tree, w_i are the weights assigned to each tree, and $h_i(x)$ is the prediction function (decision tree) for the i -th feature.

After training each tree, the model's performance is tested using the test set. This is done to assess how well the trained model generalizes to unseen data. The prediction errors (residuals) are calculated as shown in Eq. (7).

$$\text{Error} = \text{True Value} - \text{Predicted Value} \quad (7)$$

Each tree in the ensemble predicts the chronic disease risk based on what it has learned from the training set. The errors are accumulated and used to adjust the weights of the next tree.

In the boosting process, each tree is trained to reduce the residuals or errors of the previous tree. The predictions from all trees are then aggregated (usually via a weighted sum) to make the final prediction, as expressed in Eq. (8).

$$\hat{y}(x) = \sum_{t=1}^n \alpha_t \cdot f_t(x) \quad (8)$$

where $\hat{y}(x)$ is the final prediction of the health assessment for a given patient, α_t is the weight of the t -th tree, and $f_t(x)$ is the prediction made by the t -th tree. The boosting process ensures that the trees collectively focus on different parts of the data and reduce errors over iterations, leading to improved accuracy.

The final model, which pools the predictions of all the decision trees, is used to evaluate a patient's health risk. The resulting score indicates the risk level, which doctors can use to estimate the probability that the patient will develop health-related problems or illnesses, based on their health indicators and past records. This health risk assessment supports the selection of appropriate patient care and intervention strategies by enabling informed decisions.

3.4 Remote Consultation Process

AI is now widely used in telemedicine, where it helps physicians assess patients' conditions during video consultations. After analyzing patient data such as symptoms, medical history, and health metrics, it gives the doctor insight into possible diagnoses and thus assists in decision-making. The doctor then records their decisions and the AI suggestions in the patient's file for further consultation, ensuring continuity of care. All information concerning the consultation, including patient details, doctor notes, AI suggestions, and the final decision, is stored securely via blockchain technology. Blockchain technology ensures that this consultation data is permanent, immutable, and transparent, thereby preserving data integrity and allowing access only to authorized users. With this system, patient information is kept safe and can be accessed smoothly by doctors for follow-up care, audits, and decision-making, which in turn builds trust and improves the overall healthcare experience.

The workflow for a remote consultation system is illustrated in Figure 4. First, the patient submits a consultation request by providing the necessary documents and making the payment. The consultation experts from the tertiary hospital evaluate the request, and their opinion is shared with the physician at the primary hospital, who takes further action and treats the patient. After that, the Remote Consultation Management Center manages the consultation data. It consolidates the consultation data, provides advice, and supervises service delivery. The center ensures that the patient data

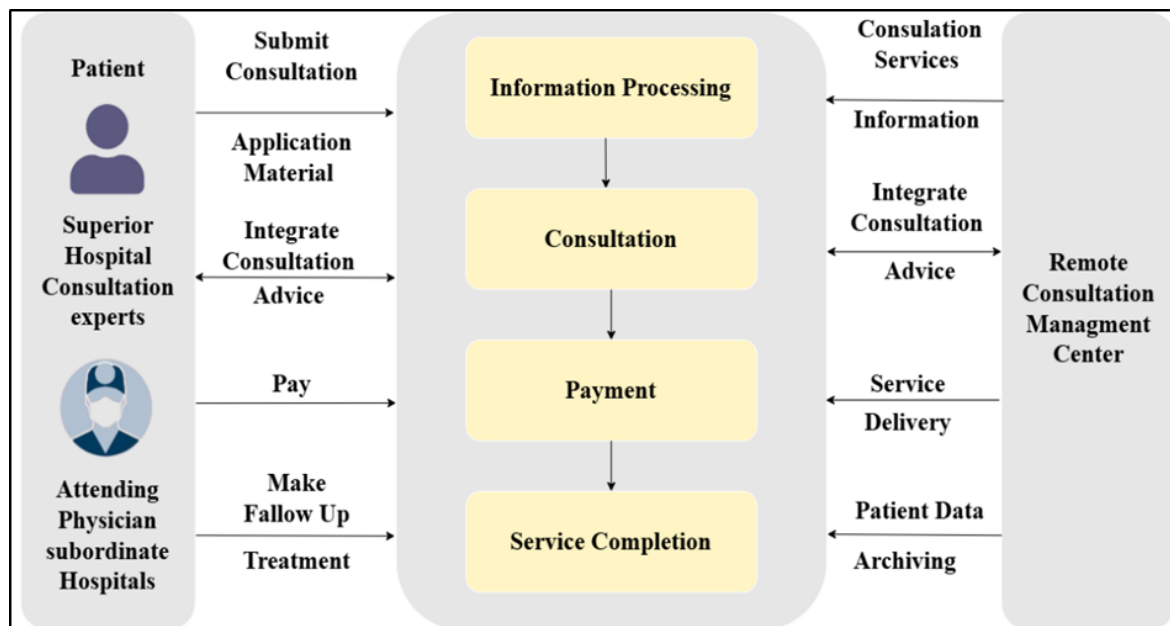


Fig. 4. Architecture of remote consultation services

are stored and managed properly. The service concludes with the consultation, payment, and final service delivery. Through this well-organized procedure, remote consultations are managed efficiently, ensuring that the needs of both patients and healthcare providers are met.

3.5 Prescription Management and Delivery process

The prescription management and delivery procedure ensures a secure process for the creation, verification, and distribution of digital prescriptions to pharmacies and patients. Once a doctor prescribes a medication, the prescription is generated and verified through the telehealth platform using AI algorithms to ensure that it is accurate, legal, and in line with medical standards. The verified prescription is then logged on the blockchain, where it is timestamped and stored immutably, so that it cannot be altered. The blockchain entry allows pharmacies and patients to independently verify a prescription's authenticity, giving both parties transparency and trust in the process. In addition, smart contracts operating on the blockchain can automate dispensing and delivery for duly licensed pharmacies, reducing the chance of human error and improving efficiency. The combined use of AI and blockchain technology helps prevent counterfeit prescriptions and makes prescription delivery within the telehealth ecosystem secure, trustworthy, and traceable. The entire procedure begins with the generation of a prescription, as illustrated in Figure 5, in which a digital prescription is created by the healthcare provider. The next step is the Verification Process, which checks the prescription for correctness and compliance. Once the prescription is verified, it is securely stored through Blockchain Recording, which ensures tamper-proof records and traceability. Authentication and Access allow only authorized pharmacists and patients to access the data. The prescription is then automatically dispensed, and the process is tracked and stored through Record Maintenance, so that the healthcare system benefits from the transparency and safety provided by the entire workflow.

3.6 Emergency Services Activation

The Emergency Services Activation function of the AI-Enhanced Blockchain Telehealth System manages urgent healthcare requests efficiently and securely. When a patient or healthcare provider sub-

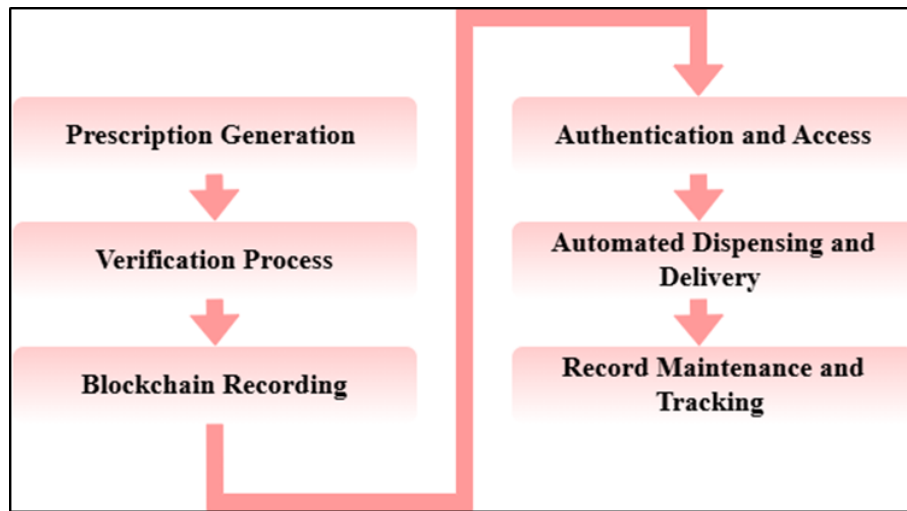


Fig. 5. Management and delivery process

mits an emergency request, the system first checks the availability and credibility of the emergency service providers, such as ambulances and hospitals, through the blockchain records. Next, AI algorithms evaluate the patient's health data, the severity of the patient's condition, the location, and the resources available to prioritize the request and determine the best response. After a provider is assigned to the case, the dispatch and all further actions, such as travel time, arrival, and treatment initiation, are logged on the blockchain, making the record tamper-proof, transparent, and auditable. This allows healthcare administrators to monitor response and service delivery times, thereby supporting continuous improvement in emergency services. Through this combination of AI for decision-making and blockchain for secure record-keeping, emergency care interventions become timely, accountable, and trustworthy.

Emergency request submission step allows the patient or healthcare provider to raise an alert when urgent medical care is needed. This alert is recorded in the system with a timestamp t , a patient identifier P , and a location L . The emergency request can therefore be mathematically expressed as shown in Eq. (9).

$$R = f(P, t, L) \quad (9)$$

here, R is the emergency request, P is the patient ID, t is the time of submission, and L is the location of the patient. This structured logging allows the exact recording of each emergency request for further verification, prioritization, and dispatch.

Verification of emergency service provider step ensures that only authorized and trustworthy providers respond to emergency requests. In response to an emergency request, the system verifies the provider's credentials and status as stored on the blockchain. This verification can be expressed mathematically as shown in Eq. (10).

$$V = \text{Verify}(E) \quad (10)$$

where V is the verification status and E is the emergency service provider's ID. Relying on blockchain records ensures that only verified providers, such as registered ambulances or hospitals, are dispatched, supporting safety, accountability, and reliability in emergency response.

AI-Rank uses AI algorithms to prioritize emergency requests by urgency and severity. The system assesses multiple variables to compute a priority score, including the severity of the patient's medical condition, the distance to the nearest emergency service, and the availability of resources. The resulting score guides resource allocation based on an aggregated assessment. The score can be expressed

as shown in Eq. (11).

$$S = \alpha \cdot H + \beta \cdot D + \gamma \cdot R_a \quad (11)$$

where S is the priority score, H is the patient's health severity, D is the distance to the nearest service, R_a is the available resources, and α, β, γ are weight factors that determine the relative importance of each parameter. This ensures that the most critical and time-sensitive cases are addressed first, thereby optimizing emergency response efficiency.

Dispatch-and-response logging entails sending emergency services to the patient according to the priority score S assigned by the AI system. Once the service is dispatched, all activities, including the start and end times of the response, the emergency request, and the provider's ID, are securely logged on the blockchain for accountability. This can be expressed as shown in Eq. (12).

$$B = \text{Blockchain_Log}(R, E, t_s, t_e) \quad (12)$$

where B is the blockchain log record, R is the emergency request, E is the ID of the emergency service provider, and t_s and t_e are the start and end times of the response. Logging on the blockchain makes the entire response process permanently traceable, so that it can be reviewed clearly during audit trails and serves as a credible record for review and optimization.

Review and optimization step aims to evaluate historical emergency response data and refine the response logic for future interventions. The response time of an emergency is computed as the difference between the end time and the start time of the service, as shown in Eq. (13).

$$T_{\text{response}} = t_e - t_s \quad (13)$$

where T_{response} is the response duration, t_s is the start time, and t_e is the end time. AI algorithms use T_{response} along with other logged metrics, such as location, resource usage, and case severity, to optimize routing, allocate resources effectively, and improve overall emergency service efficiency for future requests.

3.7 Pharmacovigilance in the AI-enhanced Blockchain Telehealth System

In the AI-enhanced Blockchain Telehealth System, pharmacovigilance is an ongoing process of monitoring and documenting adverse drug reactions (ADRs) and other safety data reported by healthcare providers and patients. The patient's side effect or concern is recorded together with metadata such as patient ID, drug details, severity, and timestamp. The information is then secured on the blockchain, so the reports cannot be altered or manipulated and can always be verified, which preserves data integrity. The AI analyzes the reports logged on the blockchain to detect safety signals and potential drug risks and to flag them as urgent for immediate intervention. Blockchain and AI together offer a transparent and effective pharmacovigilance system, which enables healthcare administrators and providers to act quickly on new drug safety issues, improve patient safety, and comply with regulations. Figure 6 illustrates the different kinds of adverse drug reactions (ADRs) that can be caused by medications. Vomiting, diarrhea, dizziness, skin changes, thyroid abnormalities, stomach inflammation, abdominal pain, and even depression are some of the side effects that drugs can produce. If a patient reports these reactions in the system, the telehealth platform not only captures the reports but also securely logs them on the blockchain. This process ensures data immutability and transparency, which prevents tampering. The AI system then analyzes the ADR data to identify patterns that point to new drug safety problems. Health professionals receive immediate alerts so that they can respond promptly when urgent action may be needed. Together, these steps improve pharmacovigilance, transparency, and the speed of action on drug safety issues.

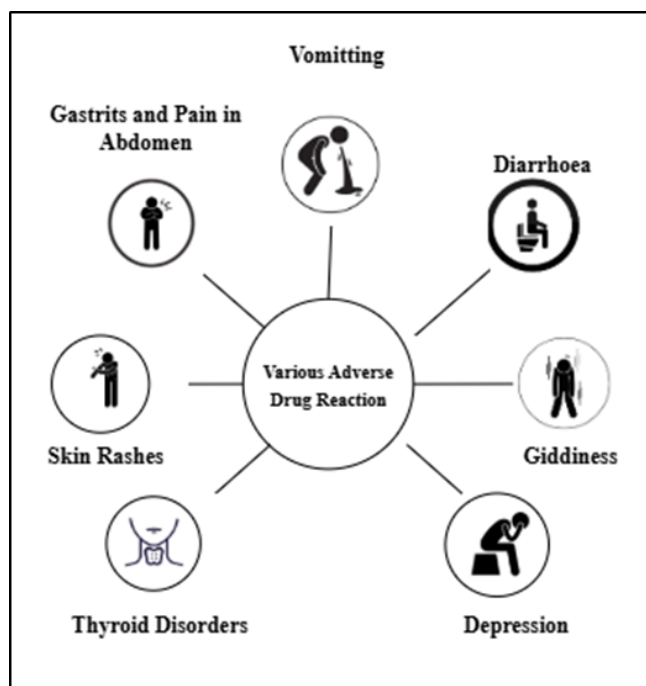


Fig. 6. Adverse drug reactions

3.8 Claims and Payments

The claims and payments process is linked to pharmacovigilance and safeguards the financial aspects of drug safety and treatment. This process ensures that patients who experience ADRs are compensated whenever an adverse drug effect is identified and reported. Once an ADR is recorded on the blockchain, it can trigger a claim for compensation or for treatment coverage. The blockchain stores the claim, allowing each participant, whether a patient, healthcare provider, or insurance company, to access immutable records, which strengthens transparency and deters fraud. AI helps verify the validity and genuineness of the claim, using patient data and ADR reports as evidence. The financial component relies on smart contracts on the blockchain, which enable fund transfers to either the healthcare provider or the patient, depending on the case. Integrating ADR reporting and claims processing through blockchain secures the entire process, maintains an audit trail, and makes it efficient, thereby improving the reliability of pharmacovigilance and insurance systems.

3.9 Blockchain Network Configuration

Before the blockchain network was deployed, the applicable guidelines and regulations were reviewed. Because health-data regulations have recently been tightened, the system was designed to comply with them. An agreement between the in-house project management team and the other stakeholders was established under the regulatory and negotiation framework of this pilot. The network configuration follows the requirements of an information security management system (ISMS) and ISO 27799:2008. An environment checklist was used to systematically ensure data security and privacy, covering system management, network services, host security, incident management, business continuity, and data restoration and recovery.

4. Result and Discussion

The experimental results of the proposed AI-Enhanced Blockchain Telehealth System demonstrate that it can deliver secure, accurate, and efficient remote healthcare services. The integration of AI and blockchain technology has not only strengthened data integrity and transparency but also enhanced the analytical accuracy and responsiveness of the system. The GBM model applied to the Telehealth Services for the Medicaid and CHIP Population dataset demonstrated remarkably good predictive power for classifying patient health risk into Low (L), Medium (M), and High (H) categories. The system achieved an impressive accuracy (99.96%), precision (99.89%), recall (99.98%), and F1-score (99.93%), indicating a good balance between precision and recall. Furthermore, ROC and Precision-Recall curves confirmed almost perfect discrimination by the model, with AUC values above 0.9999 for all classes. In addition, the smart contracts deployed on the blockchain exhibited low gas consumption (~22,500 units) and low latency (0.013 sec), supporting efficient execution and scalability. The encryption process achieved a throughput of 57.75 MB/s, which indicates good cryptographic performance for secure data management. Proof of Authority (PoA) was selected as the consensus mechanism to balance low latency and high throughput for private healthcare or consortium networks. With PoA, transactions can be recorded quickly by reputable validator nodes such as hospitals or insurers, making transaction processing much faster and cheaper than with Proof of Work. This directly contributes to the observed ultralow latency (0.013 s) and low gas consumption (~22,500 units per transaction) during the experiments. The PoA model is efficient, secure, and well governed; its attributes therefore make it a suitable consensus protocol for telehealth settings, which are strictly regulated, demand transparency, and must safeguard data privacy. Collectively, these results demonstrate that the proposed framework effectively integrates predictive intelligence with blockchain-enabled data assurance, thereby presenting a robust, transparent, and high-performance telehealth environment capable of addressing the urgent concerns of current digital healthcare systems.

4.1 Confusion Matrix

The performance of a classification model that predicts risk levels as Low, Medium, and High is shown in the confusion matrix in Figure 7. Correct predictions are reflected in the high values on the diagonal (1592 for Low Risk cases, 304 for Medium Risk cases, and 647 for High Risk cases). Only one Low Risk case was misclassified as Medium Risk. This indicates the high accuracy of the model and its ability to distinguish between categories.

4.2 Performance Metrics

Figure 8 presents the performance of the classification model as a bar chart of accuracy, precision, recall, and F1-score, all of which are very high. The model's precision is 99.89%, indicating that the false positive count is minimal, while the overall accuracy is 99.96%. A recall of 99.98% demonstrates the model's ability to detect almost all true positives. An F1-score of 99.93% indicates that the model achieves a very good balance between precision and recall, reflecting its superb predictive performance.

4.3 FPR vs FNR

The false positive rate (FPR) and false negative rate (FNR) of the model are shown in Figure 9. The FPR is remarkably low at just 0.02%, which indicates that very few false positives were predicted. In contrast, the FNR is slightly higher at 0.04%, which means that the model misses only a tiny frac-

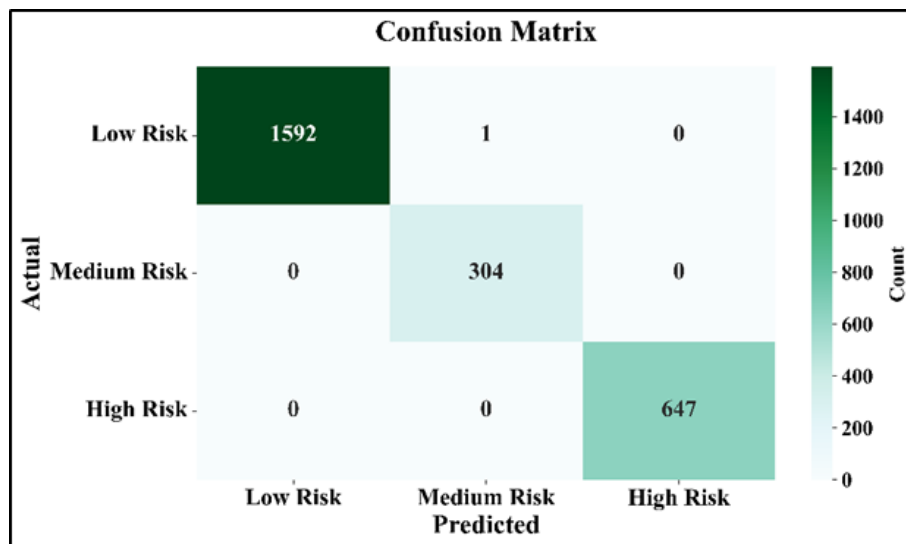


Fig. 7. Confusion matrix

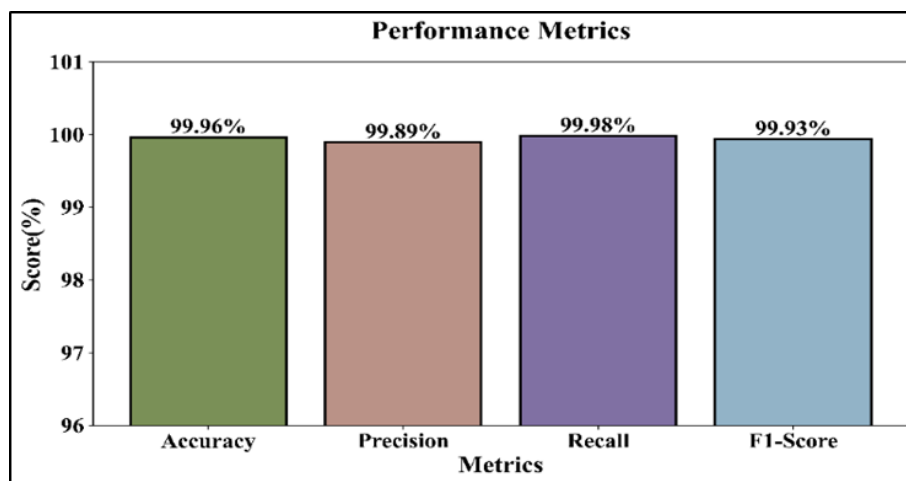


Fig. 8. Performance metrics

tion of the positive cases. Both rates are very low, confirming the model's high reliability and strong classification performance with very few misclassifications.

4.4 Precision-Recall Curve

The Precision-Recall curve illustrates the relationship between precision and recall for the three risk categories, Low, Medium, and High, as shown in Figure 10. The curves are almost perfect, as they lie very close to the top-right corner, which indicates excellent model performance. The Average Precision (AP) scores of 0.999999 for Low Risk, 0.999968 for Medium Risk, and 1.000000 for High Risk are extremely high. These results show that the model maintains very high precision and recall for all classes, with almost no trade-off between the two.

4.5 ROC Curve

The ROC curve is a graphical representation of the model's ability to separate the Low, Medium, and High Risk categories, as shown in Figure 11. Each curve is very close to perfect, hugging the upper-

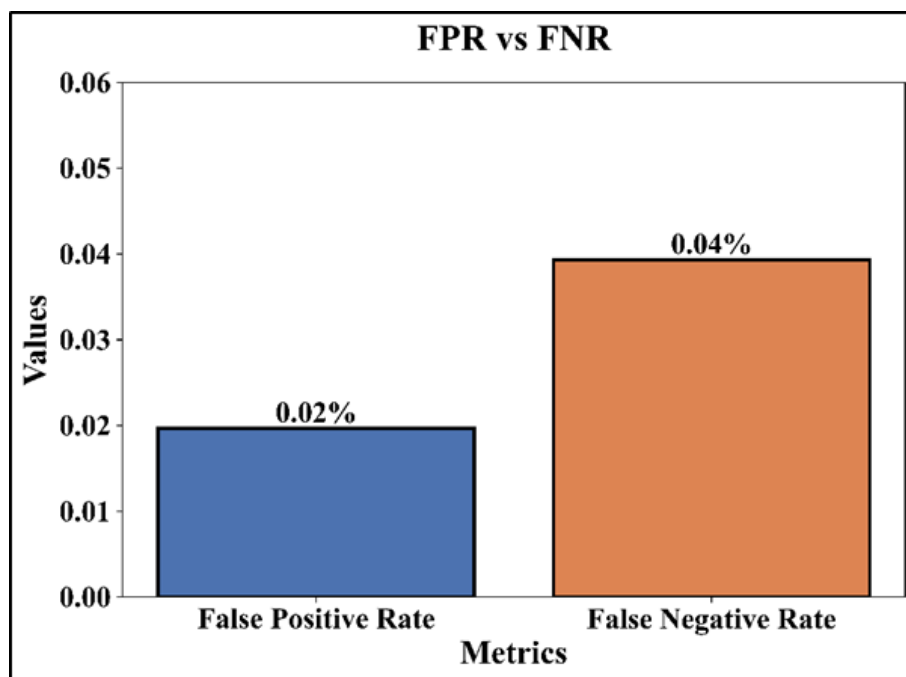


Fig. 9. FPR vs FNR

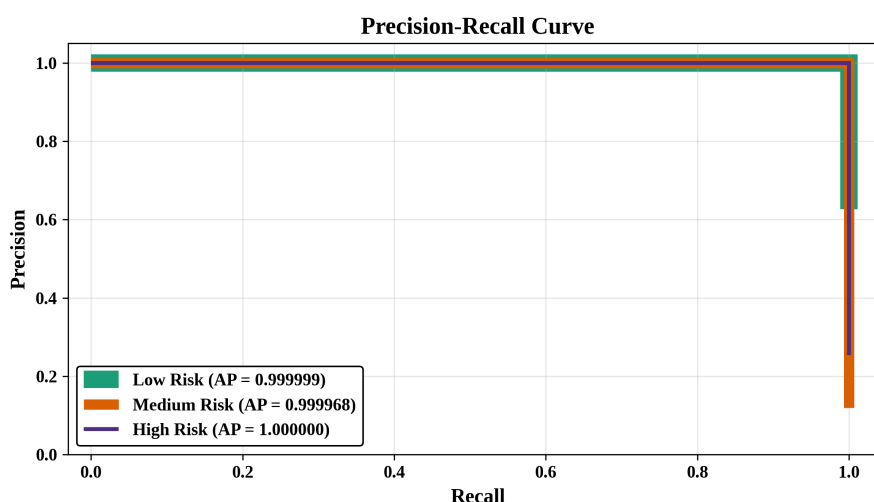


Fig. 10. Precision recall curve

left corner of the plot, which indicates excellent classification performance. The Area Under the Curve (AUC) values are extremely high: 0.999998 for Low Risk, 0.999996 for Medium Risk, and 1.000000 for High Risk. These near-perfect AUC scores indicate that the model has excellent discrimination power, with practically no false positives or false negatives.

4.6 Gas Consumption per Transaction

The bar graph displays the gas consumption of two transaction executions on the blockchain network. Transaction execution 1 consumed 22,600 gas (22.6 kgas), and transaction execution 2 consumed 22,504 gas (22.5 kgas), as shown in Figure 12. The small difference of 96 gas between the two transactions indicates that both transactions have nearly the same computational cost. This suggests

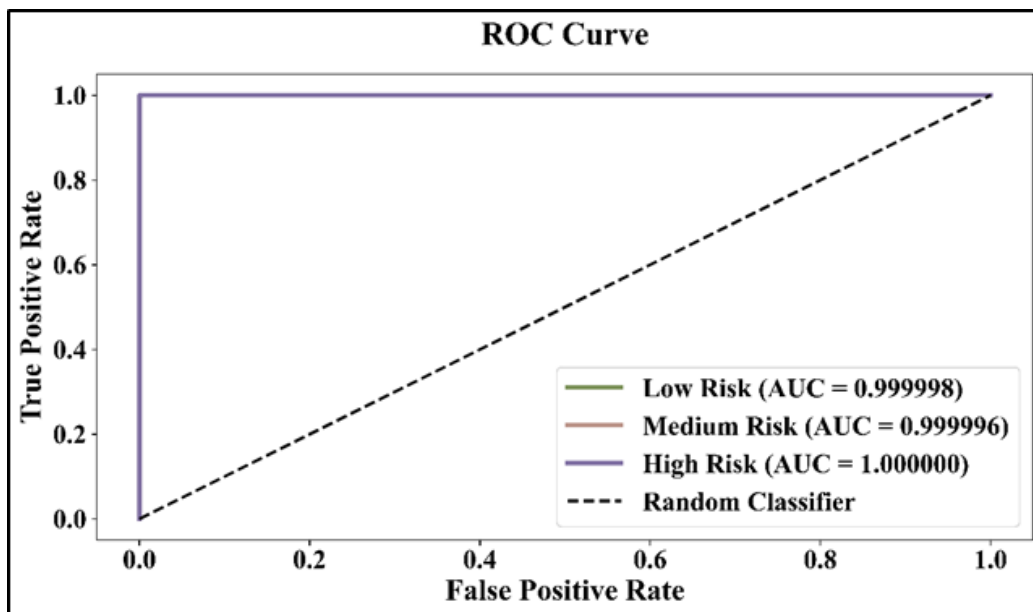


Fig. 11. ROC curve

that gas consumption is consistent across executions.

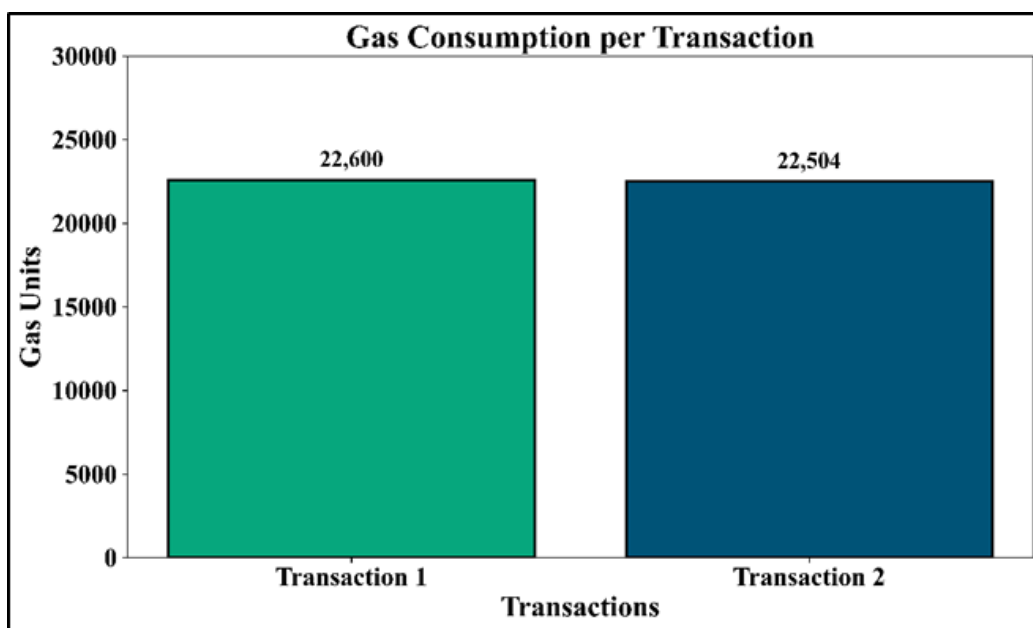


Fig. 12. Gas consumption per transaction

4.7 Blockchain Transaction Latency

The graph shows the latency of two blockchain transactions, that is, the time each takes to complete. Transaction 1 had a latency of 0.0181 seconds, while Transaction 2 completed faster, at 0.0130 seconds (Figure 13). This suggests that Transaction 2 was executed more efficiently, with less delay. Overall, both transactions show very low latency, which suggests a high-performance blockchain system.

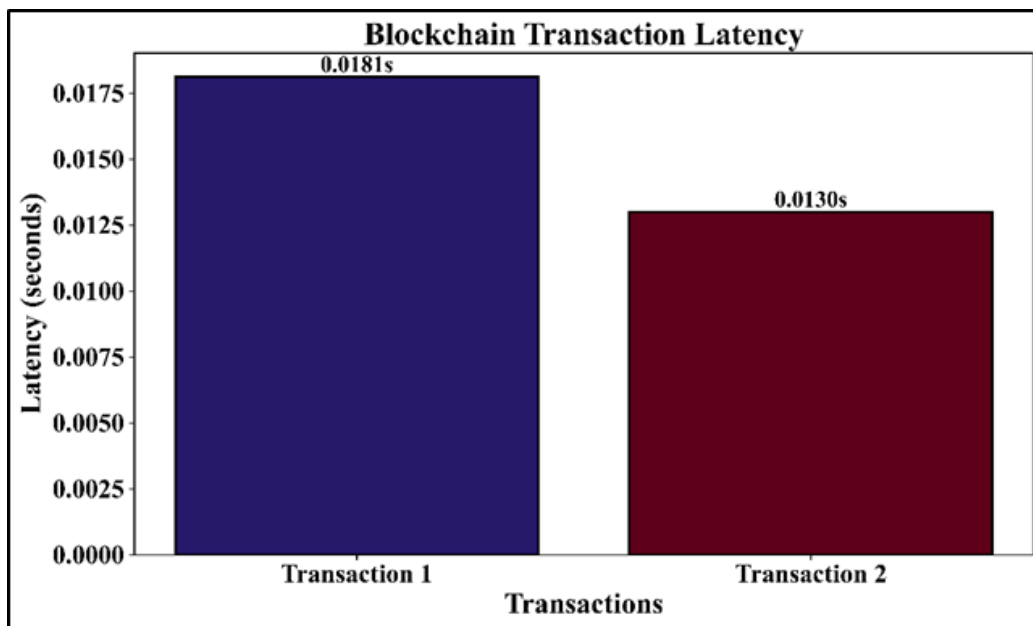


Fig. 13. Blockchain transaction latency

4.8 Encryption Throughput

The bar graph compares the encryption throughput of the two files, measured in megabytes per second (MB/s). As shown in Figure 14, File 1 achieved an excellent throughput of 57.75 MB/s, which was much higher than that of File 2. File 2, the slower of the two, reached only 5.18 MB/s, indicating poor encryption performance. This wide discrepancy suggests that file size and system resources may be among the factors that affect the efficiency of the encryption process.

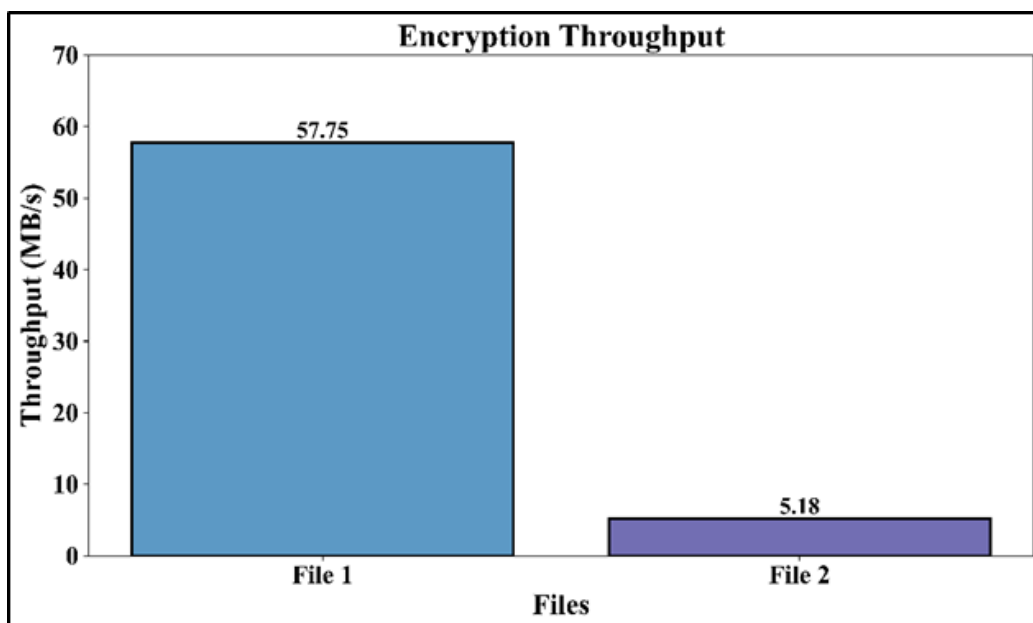


Fig. 14. Encryption throughput

4.9 Encryption Time per File

Measured in megabytes per second (MB/s), the bar graph compares the encryption throughput of the two files. The AES-256 algorithm in Galois/Counter Mode (GCM), implemented with the Py-Cryptodome library, was used to encrypt the data. As shown in Figure 15, File 1 achieved a throughput of 57.75 MB/s, indicating that the encryption is very efficient and suitable for real-time secure health transactions. GCM was chosen because it provides both confidentiality and authentication with a very low computational cost.

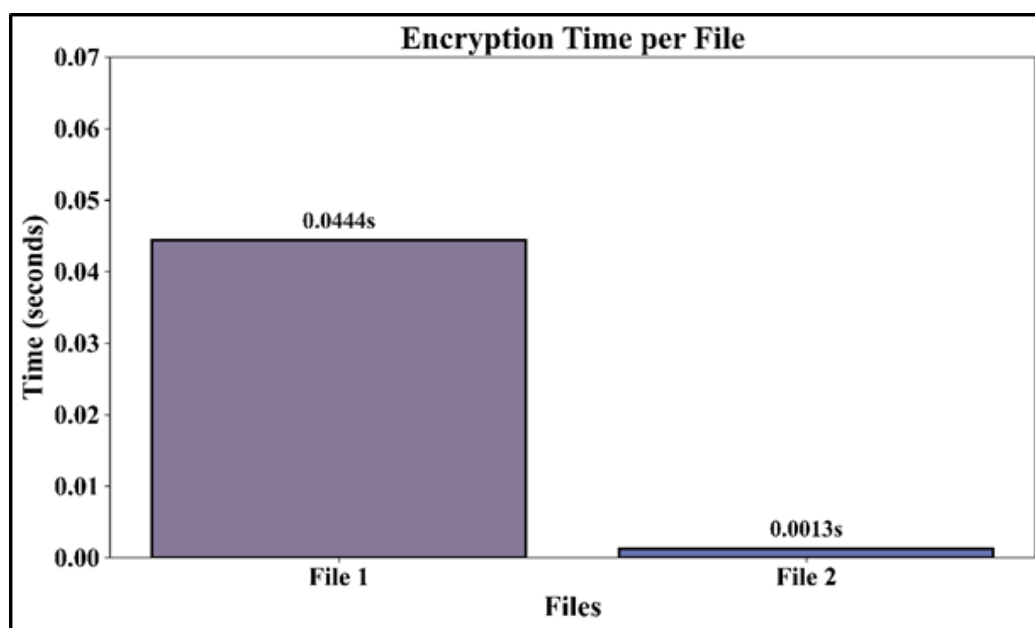


Fig. 15. Encryption time per file

4.10 Ethereum Transaction Details

Figure 16 shows the details of an Ethereum blockchain transaction. It includes the transaction hash, the sender and recipient addresses, the gas used (22,504), the gas price, and the gas limit (300,000). Most importantly, no ETH is transferred during the transaction (0.00 ETH), which indicates a smart contract operation. In addition, the current block number, the transaction status, and the input data (TX Data) for the performed operation are highlighted.



Fig. 16. Ethereum transaction details

4.11 Ethereum Smart Contract Transaction Overview

Figure 17 shows an Ethereum transaction that involves a smart contract. The transaction details show the hash, the sender address, and the contract address, with 0.00 ETH transferred, indicating that the transaction was a contract interaction rather than a value transfer. A total of 22,588 gas units was used, against a gas limit of 300,000, at a gas price of 634,262,332 wei. The transaction was successfully mined in block 7, and it contains encoded TX Data representing the contract function call.

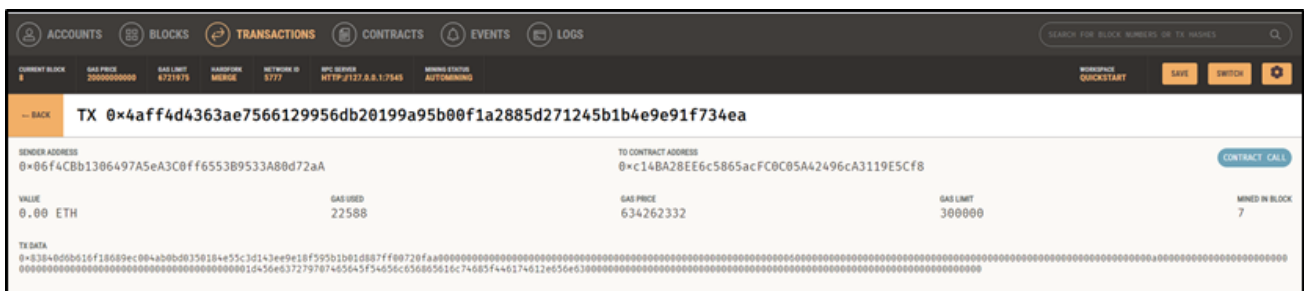


Fig. 17. Ethereum smart contract transaction

4.12 Ethereum Smart Contract Creation

Figure 18 shows the details of the transaction that creates a smart contract on the Ethereum blockchain. The figure displays the transaction hash, the sender address, and the newly created contract address as proof of deployment. The transaction had a gas limit of 3,000,000 and a gas price of 20,000,000,000 wei, and no ETH was transferred. The TX Data field contains compiled smart contract bytecode, which represents the logic of the deployed contract.

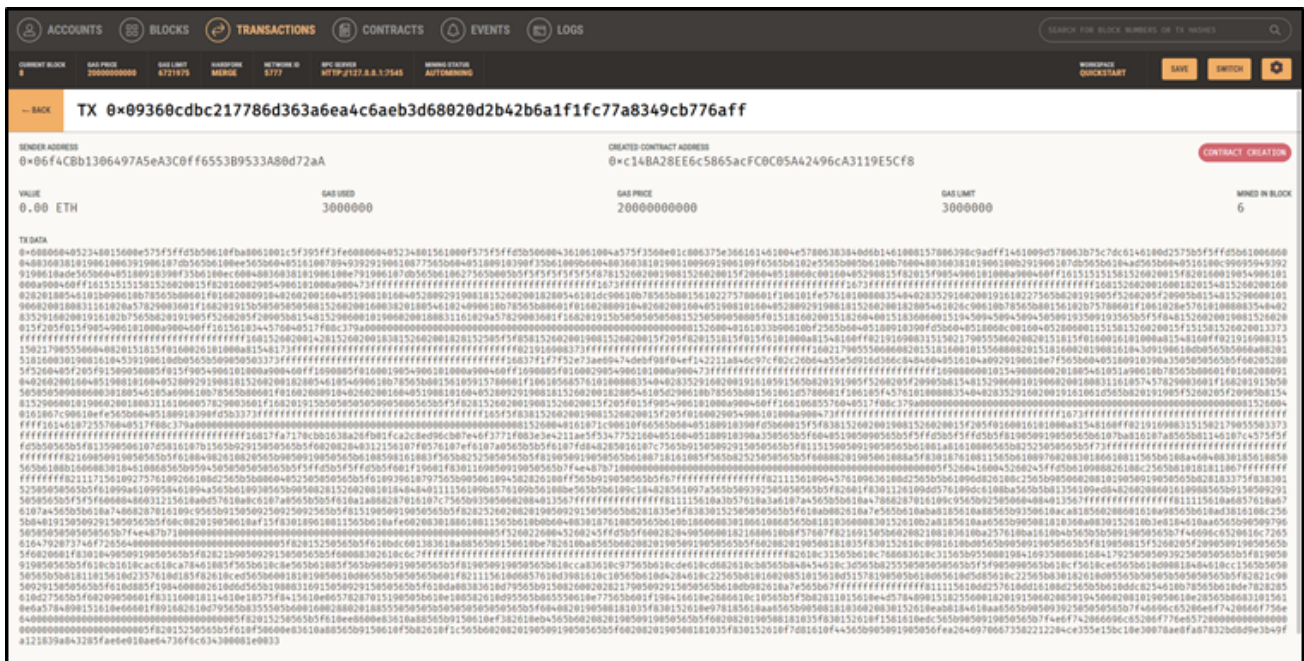


Fig. 18. Ethereum smart contract creation

4.13 Overview of Blockchain Transactions

Figure 19 shows three Ethereum blockchain transactions listed under the “Transactions” tab. The first two entries are contract calls, in which the sender interacts with an existing smart contract, each using around 22,500 gas units. The third transaction is a contract creation, in which a new smart contract is deployed using 3,000,000 gas units. All transactions were sent from the same sender address, demonstrating both contract deployment and subsequent interaction.

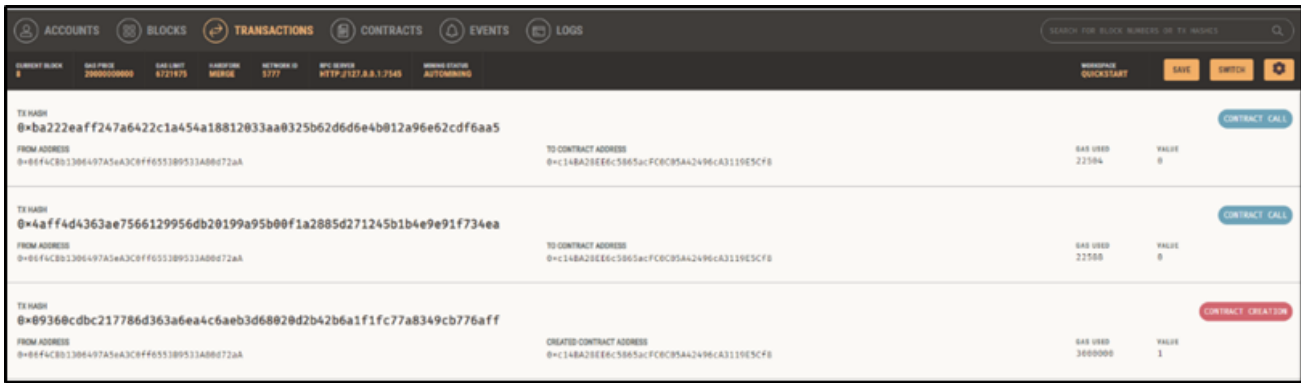


Fig. 19. Blockchain transactions

4.14 Ethereum Block Details

As illustrated in Figure 20, the Blocks section of an Ethereum blockchain interface shows blocks 6, 7, and 8, with one transaction each. The blocks were mined in sequence, with gas usage of 3,000,000 for block 6 and 22,500 for blocks 7 and 8. This indicates that block 6 contained a contract creation, while the following blocks executed contract calls.

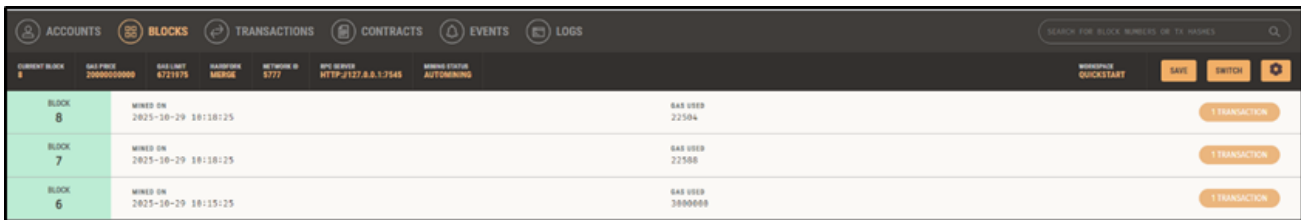


Fig. 20. Ethereum block details

4.15 Smart Contract Deployment Transaction

The details of the contract deployment transaction are displayed in the Ethereum interface, as shown in Figure 21. The screen shows the transaction hash, the sender address, and the smart contract address. The display also shows that 3,000,000 gas units were assigned to the deployment transaction. The absence of an ETH value transfer, together with the contract address created by the transaction, identifies it as a contract deployment rather than a contract interaction.

4.16 Ethereum Accounts Overview

Figure 22 shows the Accounts section of an Ethereum development environment, which lists the addresses of blockchain wallets. Each account has a unique address, a balance, and a transaction

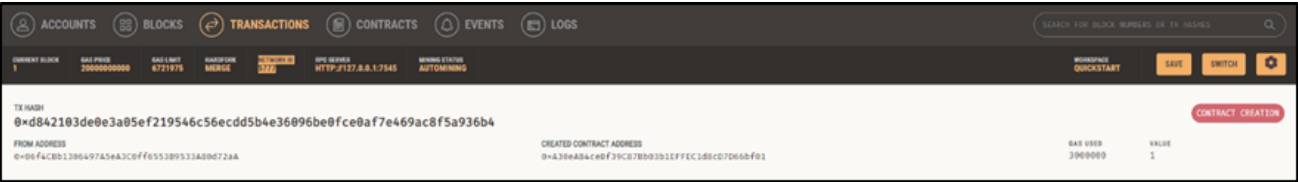


Fig. 21. Smart contract deployment transaction

count (TX Count). Most accounts hold 100 ETH, while the first account holds slightly less, 99.94 ETH, indicating that it has already sent transactions. The mnemonic phrase at the top represents the seed used to generate these addresses deterministically, solely for testing or development purposes.

ACCOUNTS						TRANSACTIONS		CONTRACTS		EVENTS		LOGS	
ACCOUNTS						TRANSACTIONS		CONTRACTS		EVENTS		LOGS	
MNEMONIC						TX COUNT		INDEX		INDEX		INDEX	
crew bergain chef hub very arctic mind earth wisdom beef pond blossom						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0x06f4C8b1306497A5eA3C8ff6553B9533A80d72aA						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
99.94 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0x00237eE3FAFEE22D58Ced094017a5361f170C894						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0x65F5b06a889a1ae127cb13dD365AAa215E357C5d						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0xC1a58FA9028618B1708c991B60C3c001Abc2a278						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0xd0e7A1516EEB25610190aab83447668cB1ed5602						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0x483225765f3c62852955302f28640e23d1009088						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0xfEF370D170148fe17aCB425F4C158Cb2Eb7D056						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0xBC23538DA672732289d7564E441E62216ef35fb						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0x72902005389cCed2Fd84C3AC4ec555DD64999E						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	
ADDRESS						TX COUNT		INDEX		INDEX		INDEX	
0xc5F96D06FC262145298A82bf83De75dcE9c259A2						TX COUNT		INDEX		INDEX		INDEX	
BALANCE						TX COUNT		INDEX		INDEX		INDEX	
100.00 ETH						TX COUNT		INDEX		INDEX		INDEX	

Fig. 22. Ethereum accounts overview

4.17 MetaMask Contract Deployment Confirmation

Figure 23 shows a MetaMask confirmation window for deploying the smart contract via Remix. It indicates that the contract will be deployed from “Imported Account 1,” with a transaction amount of less than 0.000001 ETH and an estimated network fee of 0.06 ETH. The user can now either click Confirm to proceed with the contract deployment or click Cancel to abort the transaction.

4.18 MetaMask Connection Request

Figure 24 shows a MetaMask pop-up requesting the connection of the website remix.ethereum.org to the user’s wallet. It shows “Imported Account 1” with a balance of \$0.00, and it offers options to edit the selected accounts. The user can either click Connect to authorize the connection or click Cancel to reject it.

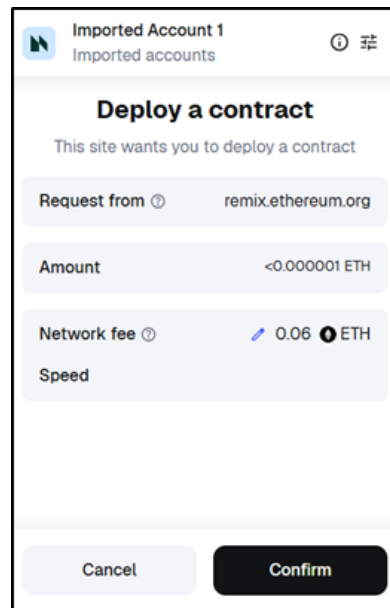


Fig. 23. MetaMask contract deployment confirmation

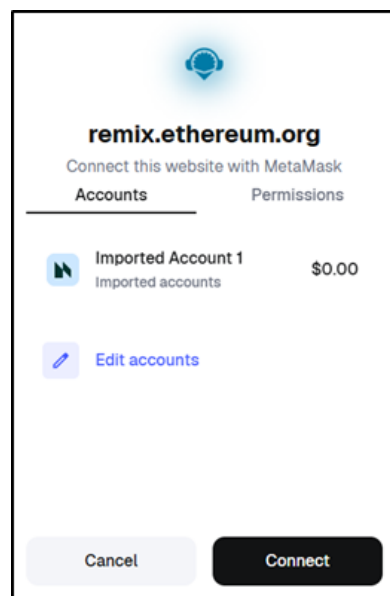


Fig. 24. MetaMask connection request

4.19 Ethereum Accounts Overview

The Accounts tab in the Ethereum Remix IDE displays a list of generated Ethereum accounts along with their respective addresses, balances, transaction counts, and index numbers, as shown in Figure 25. Each account is loaded with 100 ETH, except the first account, which has 99.94 ETH because of earlier transactions. The mnemonic phrase at the top can be used to generate and restore these accounts.

ACCOUNTS									
ACCOUNTS BLOCKS TRANSACTIONS CONTRACTS EVENTS LOGS SEARCH FOR BLOCK NUMBERS OR TX HASHES WORKSPACE BOOKMARKS SAVE SWITCH									
MINIMUM crew bargain chef hub very arctic mind earth wisdom beef pond blossom MAXIMUM 0x4'0B'0'Baccount_index									
ADDRESS	BALANCE				TX COUNT		INDEX		
0x06f4Cbb1306497A5eA3C0ff6553B9533A80d72aA	100.00 ETH				0		0		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xD0237eE3FAFEE22D58Ced094017a5361f170CB94	100.00 ETH				0		1		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x65F5b06aB89a1ae127cb13d0365AAa215E357C5d	100.00 ETH				0		2		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xC1a58FA9028618B1700c991B68C3c001Abc2a278	100.00 ETH				0		3		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xd0e7A1516EEB25610190aab83447668cB1ed5602	100.00 ETH				0		4		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x483225765f3c62852955302f28640e23d100908B	100.00 ETH				0		5		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xfEF370D170148fe17aCBF425F4C158Cb2Eb7D056	100.00 ETH				0		6		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xBC23538DA6727352289d7564E441E62216ef35fb	100.00 ETH				0		7		
ADDRESS	BALANCE				TX COUNT		INDEX		
0x729028085389cCed2Fd84C3AC4ec5555D064999E	100.00 ETH				0		8		
ADDRESS	BALANCE				TX COUNT		INDEX		
0xc5F96D06FC262145298AB2bf83De75dcE9c259A2	100.00 ETH				0		9		

Fig. 25. Ethereum accounts overview

4.20 Performance Comparison of Proposed Framework with Existing Methods

Table 1 shows that the comparison demonstrates the superiority of the proposed AI-Enhanced Blockchain Telehealth Framework over existing systems. Conventional IoT methods offer reasonable precision but suffer from significant latency and poor data security because of their centralized infrastructures. Blockchain-based health systems usually improve security and transparency, but most lack integrated predictive intelligence and are therefore less efficient in diagnostics. In contrast, the proposed framework achieves near-perfect classification performance, with 99.96% accuracy and a 99.93% F1-score, using the GBM model and blockchain-secured data handling. A latency of 0.013 seconds indicates very rapid validation of transactions and data, making the system well suited for real-time telehealth services. Moreover, combining AI analytics with decentralized blockchain improves integrity, privacy, and reliability in decision-making, making it a robust and scalable solution for next-generation remote healthcare systems.

Table 1
Performance comparison

Method / Framework	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC Score	Latency (sec)	Data Security Level
IoT-Based Healthcare Monitoring System [32]	92.45	90.82	91.36	91.08	0.935	0.245	Moderate
Blockchain-Based Smart Healthcare [33]	95.78	94.65	94.92	94.78	0.972	0.112	High
Proposed AI-Enhanced Blockchain Telehealth Framework	99.96	99.89	99.98	99.93	0.9999	0.013	Very High

5. Conclusion and Future Scope

The AI-enhanced blockchain telehealth system is a breakthrough in the secure, intelligent, and transparent delivery of remote healthcare services. By combining predictive analytics with AI and blockchain, it provides a framework of security, privacy, and trust that supports the immutability and auditability of data management, which are issues endemic to the telehealth landscape. Using the Telehealth Services for Medicaid and CHIP Population dataset, the GBM model classified users into

Low, medium, and high risk categories based on telehealth access and usage patterns. The model's performance is excellent, with an accuracy of 99.96%, a precision of 99.89%, a recall of 99.98%, and an F1-score of 99.93%, which indicate strong predictive ability to identify disparities in telehealth access. Operationally, the system is efficient, with around 22,500 gas units per transaction on the blockchain, a latency as low as 0.013 seconds, and an AES-256-GCM encryption throughput of 57.75 MB/s, confirming fast and secure data handling. Taken together, these results suggest that the system can be used to provide telehealth services in a trustworthy, privacy-preserving, and high-performance manner. Future work will scale the system using energy-efficient consensus protocols and Layer-2 blockchain architectures, and will integrate federated learning for privacy-preserving AI model training and support interoperability with healthcare data standards such as HL7 and FHIR. Real-world experiments on several longitudinal datasets will assess fairness, adaptability, and resilience, positioning this framework as a step toward a global, ethical, and inclusive telehealth ecosystem.

Acknowledgement

This research was not funded by any grant.

Conflicts of Interest

The authors declare no conflicts of interest.

References

- [1] Almadani, B., Kaisar, H., Thoker, I. R., & Aliyu, F. (2025). A systematic survey of distributed decision support systems in healthcare. *Systems*, 13(3), 157. <https://doi.org/10.3390/systems13030157>
- [2] Chaparro-Cárdenas, S. L., Ramírez-Bautista, J.-A., Terven, J., Córdova-Esparza, D.-M., Romero-Gonzalez, J.-A., Ramírez-Pedraza, A., & Chavez-Urbiola, E. A. (2025). A technological review of digital twins and artificial intelligence for personalized and predictive healthcare. *Healthcare*, 13(14), 1763. <https://doi.org/10.3390/healthcare13141763>
- [3] Pool, J., Akhlaghpour, S., Hassandoust, F., Fatehi, F., & Burton-Jones, A. (2025). Towards a model for understanding failures in health data protection: A mixed-methods study. *Behaviour & Information Technology*, 45(7), 1381–1406. <https://doi.org/10.1080/0144929x.2025.2551568>
- [4] Karim, M. M., Van, D. H., Khan, S., Qu, Q., & Kholodov, Y. (2025). Ai agents meet blockchain: A survey on secure and scalable collaboration for multi-agents. *Future Internet*, 17(2), 57. <https://doi.org/10.3390/fi17020057>
- [5] Pillay, T. S., Topcu, D. İ., & Yenice, S. (2025). Harnessing ai for enhanced evidence-based laboratory medicine (ebim). *Clinica Chimica Acta*, 569, 120181. <https://doi.org/10.1016/j.cca.2025.120181>
- [6] Cirillo, F., De Santis, M., & Esposito, C. (2025). Applications of solid platform and federated learning for decentralized health data management. In *Artificial intelligence techniques for analysing sensitive data in medical cyber-physical systems* (pp. 95–111). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-70775-9_6
- [7] Nazir, A., Hussain, A., Singh, M., & Assad, A. (2024). Deep learning in medicine: Advancing healthcare with intelligent solutions and the future of holography imaging in early diagnosis. *Multimedia Tools and Applications*, 84(17), 17677–17740. <https://doi.org/10.1007/s11042-024-19694-8>
- [8] Rathore, N., Kumari, A., Patel, M., Chudasama, A., Bhalani, D., Tanwar, S., & Alabdulatif, A. (2024). Synergy of ai and blockchain to secure electronic healthcare records. *SECURITY AND PRIVACY*, 8(1). <https://doi.org/10.1002/spy2.463>

- [9] Alserhani, F. (2025). Intrusion detection and real-time adaptive security in medical iot using a cyber-physical system design. *Sensors*, 25(15), 4720. <https://doi.org/10.3390/s25154720>
- [10] Kotb, Y., Oueida, S., Mostafa, N., & Ali, N. (2025). Online federated deep probabilistic learning-based smart healthcare on multi-cloud systems. *IEEE Access*, 13, 75265–75293. <https://doi.org/10.1109/access.2025.3557877>
- [11] Elhanashi, A., Saponara, S., Zheng, Q., Almutairi, N., Singh, Y., Kuanar, S., Ali, F., Unal, O., & Faghani, S. (2025). Ai-powered object detection in radiology: Current models, challenges, and future direction. *Journal of Imaging*, 11(5), 141. <https://doi.org/10.3390/jimaging11050141>
- [12] Sayed, S., Famous, M. S., Mazumder, R., Khan, R. T., Kaiser, M. S., Hossain, M. S., Andersson, K., & Khondoker, R. (2025). Blockchain and interplanetary framework for decentralized and secure electronic health record management. *Blockchains*, 3(4), 12. <https://doi.org/10.3390/blockchains3040012>
- [13] Yadegari, F., & Asosheh, A. (2025). A unified iot architectural model for smart hospitals: Enhancing interoperability, security, and efficiency through clinical information systems (cis). *Journal of Big Data*, 12(1). <https://doi.org/10.1186/s40537-025-01197-4>
- [14] Adeleke, O. J., Jovanovich, K. D., Ogunbunmi, S., Samuel, O., & Kehinde, T. O. (2025). Comprehensive exploration of smart cities: A systematic review of benefits, challenges, and future directions in telecommunications and urban development. *IEEE Sensors Reviews*, 2, 228–245. <https://doi.org/10.1109/sr.2025.3569239>
- [15] Dash, S. P. (2020). The impact of iot in healthcare: Global technological change & the roadmap to a networked architecture in india. *Journal of the Indian Institute of Science*, 100(4), 773–785. <https://doi.org/10.1007/s41745-020-00208-y>
- [16] Chen, L., Zheng, X., Sun, Z., & Li, X. (2025). Study on the development of an intelligent regional health security monitoring and emergency medical response system in less developed regions. *Journal of Computing and Electronic Information Management*, 16(1), 74–82. <https://doi.org/10.54097/ydgagy87>
- [17] Lakhwani, T. S., Sinjana, Y., & Kapoor, A. P. (2025). Beyond numbers: A novel iot and drone framework for enhancing healthcare logistics. *Discover Health Systems*, 4(1). <https://doi.org/10.1007/s44250-025-00187-w>
- [18] Alharbi, S. H., Alzahrani, A. M., Syed, T. A., & Alqahtany, S. S. (2024). Integrity and privacy assurance framework for remote healthcare monitoring based on iot. *Computers*, 13(7), 164. <https://doi.org/10.3390/computers13070164>
- [19] Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2023). Securing ai-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. *Transactions on Emerging Telecommunications Technologies*, 35(1). <https://doi.org/10.1002/ett.4884>
- [20] Saxena, S., Saxena, S., Tahilramani, N., & Charanarur, P. (2025). Blockchain enhanced smart healthcare management for chronic diseases. *Discover Computing*, 28(1). <https://doi.org/10.1007/s10791-025-09574-6>
- [21] Pinto-Coelho, L. (2023). How artificial intelligence is shaping medical imaging technology: A survey of innovations and applications. *Bioengineering*, 10(12), 1435. <https://doi.org/10.3390/bioengineering10121435>
- [22] Rashid, Z., Ahmed, H., Nadeem, N., Zafar, S. B., & Yousaf, M. Z. (2025). The paradigm of digital health: Ai applications and transformative trends. *Neural Computing and Applications*, 37(17), 11039–11070. <https://doi.org/10.1007/s00521-025-11081-0>
- [23] Saini, B., Singh, D., Sharma, K. C., & Saini, D. K. (2025). Ai-enhanced telemedicine: Transforming resource allocation and cost-efficiency analysis via advanced queueing model. *Scientific Reports*, 15(1). <https://doi.org/10.1038/s41598-025-15664-8>

- [24] Khamaj, A. (2025). Ai-enhanced chatbot for improving healthcare usability and accessibility for older adults. *Alexandria Engineering Journal*, 116, 202–213. <https://doi.org/10.1016/j.aej.2024.12.090>
- [25] Huang, G., Chen, X., & Liao, C. (2025). Ai-driven wearable bioelectronics in digital healthcare. *Biosensors*, 15(7), 410. <https://doi.org/10.3390/bios15070410>
- [26] Ghadi, Y. Y., Shah, S. F. A., Waheed, W., Mazhar, T., Ahmad, W., Saeed, M. M., & Hamam, H. (2025). Integration of wearable technology and artificial intelligence in digital health for remote patient care. *Journal of Cloud Computing*, 14(1). <https://doi.org/10.1186/s13677-025-00759-4>
- [27] Aldhaen, F. S. (2025). Ai-powered transformation of healthcare: Enhancing patient safety through ai interventions with the mediating role of operational efficiency and moderating role of digital competence—insights from the gulf cooperation council region. *Healthcare*, 13(6), 614. <https://doi.org/10.3390/healthcare13060614>
- [28] Moray, R. (2025). An investigation of factors impacting the acceptance of telehealth in rural india. *Discover Social Science and Health*, 5(1). <https://doi.org/10.1007/s44155-025-00250-0>
- [29] Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. (2025). Blockhealthsecure: Integrating blockchain and cybersecurity in post-pandemic healthcare systems. *Information*, 16(2), 133. <https://doi.org/10.3390/info16020133>
- [30] Barbaria, S., Jemai, A., Ceylan, H. İ., Muntean, R. I., Dergaa, I., & Boussi Rahmouni, H. (2025). Advancing compliance with hipaa and gdpr in healthcare: A blockchain-based strategy for secure data exchange in clinical research involving private health information. *Healthcare*, 13(20), 2594. <https://doi.org/10.3390/healthcare13202594>
- [31] Ewoh, P., Vartiainen, T., & Mantere, T. (2025). Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: Scoping review. *Journal of Medical Internet Research*, 27, e75584. <https://doi.org/10.2196/75584>
- [32] Chen, Q., & Sheng, N. (2024). A novel health monitoring system for vital signs using iot. *Scientific Reports*, 14(1). <https://doi.org/10.1038/s41598-024-69257-y>
- [33] Du, X., Chen, B., Ma, M., & Zhang, Y. (2021). Research on the application of blockchain in smart healthcare: Constructing a hierarchical framework (Y.-Z. Jiang, Ed.). *Journal of Healthcare Engineering*, 2021, 1–13. <https://doi.org/10.1155/2021/6698122>