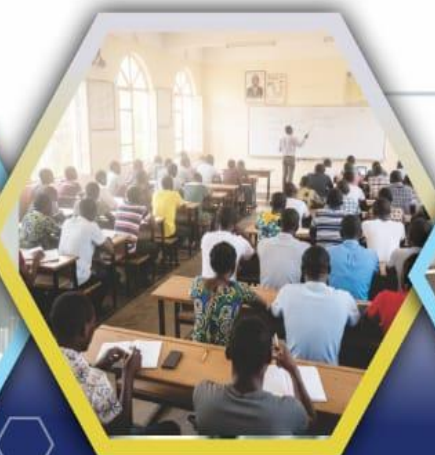




JOURNAL OF SCIENCE, TECHNOLOGY AND EDUCATION (JSTE)



**A PUBLICATION OF THE
DEPARTMENT OF SCIENCE,
TECHNOLOGY AND MATHEMATICS
EDUCATION (STME),
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA**



VOLUME 10

ISSN: 2651-5539

A SECURED AI-BLOCKCHAIN-ENABLED FRAMEWORK FOR DATA-DRIVEN MEDICAL DIAGNOSTIC SYSTEM

^{1*}Anazia, K., E. ²Onovughe, A., O. and ³Emma-Osiebe, A., O.

1: Department of Information Systems and Technology, Southern Delta University, Ozoro

2: Department of Software Engineering, Southern Delta University, Ozoro

3: Department of Information and Communication Technology, Delta State Polytechnic

*Corresponding author: anaziake@sdu.edu.ng

Citation: Anazia, K., E. Onovughe, A., O., & Emma-Osiebe, A. O. (2026). A Secured AI-Blockchain-Enabled Framework for Data-Driven Medical Diagnostic System. *Journal of Science, Technology, and Education (JSTE)*; www.nsukjste.com/. 10(34), 447-462.

Abstract

In the present day, the increasing adoption of digital healthcare technologies has generated vast amounts of medical data, creating opportunities for intelligent disease diagnosis while simultaneously raising concerns regarding data security, privacy and integrity. Conventional medical diagnostic systems often suffer from limitations such as lower predictive accuracy, vulnerability to data tampering and inadequate access control mechanisms. To address these challenges, this study presents a secured AI-blockchain-enabled framework for data-driven medical diagnostic systems that integrates Artificial Intelligence (AI) and blockchain technologies to enhance diagnostic performance and healthcare data security. The framework incorporates AI-driven predictive analytics for disease detection and blockchain-based mechanisms for secured data storage, integrity verification and decentralized access management. The system was evaluated using key performance metrics, including accuracy, precision, recall, F1-score, AUC-ROC, data integrity rate, and access control success rate, and was compared with a conventional diagnostic approach. Experimental results demonstrate that the AI-blockchain framework

achieved an accuracy of 97.28%, precision of 97.28%, recall of 97.68%, F1-score of 97.45% and AUC-ROC of 98.25%, significantly outperforming the conventional method, which recorded 85.93%, 85.33%, 85.93%, 85.58% and 87.35%, respectively. Furthermore, the secured AI-blockchain framework improved the data integrity rate from 88.88% to 99.0% and the access control success rate from 87.93% to 99.63%, highlighting its effectiveness in securing sensitive healthcare information. The AI-blockchain framework also achieved an average performance rate of 98.21%, compared to 86.70% for the conventional method, representing an overall improvement of 11.51%. The findings demonstrate that the synergistic integration of AI and blockchain technologies provide a robust, accurate and secured platform for medical diagnosis. The framework offers significant potential for deployment in modern healthcare environments where reliable decision-making and trustworthy data management are critical.

Keywords: Artificial Intelligence, Blockchain, Medical Diagnosis, Healthcare Security, Machine Learning and Data Integrity

Introduction

The rapid advancement of digital healthcare technologies has transformed medical diagnostic systems through the integration of Artificial Intelligence (AI), blockchain, big data analytics, cloud computing and the Internet of Medical Things (IoMT). These technologies enable intelligent analysis of healthcare data from electronic health records, medical imaging systems, wearable devices and smart sensors, thereby improving disease prediction, clinical decision-making, patient monitoring and healthcare management (Tagde et al., 2021; Liu & Hu, 2026).

AI has become a key driver of modern healthcare diagnostics due to its ability to process large and complex datasets with high accuracy. Technologies such as machine learning, deep learning, neural networks, and natural language processing and computer vision have been successfully applied to disease prediction; medical image analysis and clinical decision support (Anazia et al, 2025). AI-driven systems have demonstrated effectiveness in diagnosing diseases including cancer, diabetes, cardiovascular disorders and neurological conditions. However, challenges such as biased datasets, adversarial attacks, and limited explainability and data integrity issues continue to affect diagnostic reliability and trustworthiness (Liu & Hu, 2026; Shinde et al., 2026).

Blockchain technology has emerged as a secure and decentralized approach to healthcare data management. Through distributed ledger mechanisms, blockchain provides transparency, immutability, traceability and cryptographic security for healthcare transactions. It supports secure electronic health records, patient-controlled data access, identity management, interoperability and trusted information exchange among healthcare stakeholders (Eti et al, 2025). Smart contracts further automate authentication, authorization and healthcare transaction processes, reducing risks associated with centralized storage, unauthorized access, data tampering and cyberattacks (Houssein et al., 2026). Nevertheless, issues such as scalability, transaction latency, computational overhead and regulatory concerns remain significant challenges (Abbas et al., 2026).

The integration of AI and blockchain offers a promising solution for developing secure, intelligent and scalable healthcare systems. While AI provides advanced analytics and predictive capabilities, blockchain ensures secure and trustworthy data governance.

Artificial Intelligence (AI) has significantly transformed medical diagnosis by enabling automated disease detection, prediction and clinical decision support. Between 2020 and 2026, AI evolved from experimental diagnostic tools into clinically deployable systems used

across medical imaging, oncology, cardiology, neurology, pathology and infectious disease diagnosis (Rajpurkar et al, 2022; Esteva et al., 2021). Through advanced machine learning and deep learning techniques, AI has demonstrated remarkable effectiveness in detecting diseases, predicting clinical outcomes and supporting healthcare professionals in decision-making processes. During the COVID-19 pandemic, AI-based systems played a crucial role in disease screening, prognosis prediction and healthcare resource management (Maduabuchukwu et al., 2026, Anazia, 2026). Furthermore, AI-powered Clinical Decision Support Systems (CDSS) have improved diagnostic accuracy and reduced medical errors by providing evidence-based recommendations to clinicians (Jiang et al., 2022; Maduabuchukwu et al 2026). Despite these advancements, concerns relating to data privacy, transparency, explainability and clinician trust continue to hinder widespread adoption, thereby stimulating increased research into Explainable Artificial Intelligence (XAI) (Arrieta et al., 2020).

Blockchain technology on its own has emerged as a promising solution for addressing healthcare data security, integrity and interoperability challenges. As a decentralized and immutable ledger technology, blockchain facilitates the secure storage, sharing and management of healthcare information while ensuring transparency, traceability and

auditability (Kumar et al., 2023). Since 2020, blockchain applications in healthcare have expanded beyond Electronic Health Record (EHR) management to include medical imaging, telemedicine, genomic data sharing and secure diagnostic data exchange (Agbo et al., 2021). In addition, smart contracts enhance healthcare operations by automating patient consent management, access control and data-sharing processes (Nguyen et al., 2022). Although AI-driven healthcare systems have demonstrated remarkable capabilities in disease prediction, diagnosis and clinical decision support, concerns regarding data privacy, security, explainability and trust remain significant challenges. Also, blockchain technology provides a secure and transparent framework for healthcare data management; however, many blockchain-based healthcare solutions continue to face issues with scalability, computational efficiency, and system performance (Hussien et al., 2022).

Consequently, the integration of AI and blockchain has gained significant attention in contemporary medical diagnostics. AI provides intelligent disease prediction, classification and diagnostic analytics, while blockchain ensures data integrity, provenance, privacy and trustworthiness throughout the diagnostic lifecycle (Kumar et al., 2023). The complementary strengths of these technologies present an opportunity to develop secure, transparent and reliable healthcare diagnostic

systems capable of addressing the limitations of existing standalone approaches.

Despite the growing body of research on AI and blockchain in healthcare, a significant gap remains in the development of a unified framework that effectively integrates AI-driven diagnostic intelligence with blockchain-enabled security, privacy preservation and decentralized healthcare data management. To address this gap, this study proposes a secure AI-blockchain-enabled framework for data-driven medical diagnostic systems aimed at enhancing diagnostic accuracy, healthcare data security, interoperability, transparency and trustworthy clinical decision-making.

Methodology

This study adopted a design and experimental research approach to develop and evaluate the secured AI-blockchain-enabled framework for data-driven medical diagnostic systems. The framework integrated AI and blockchain technologies to enhance diagnostic accuracy, data security, decentralized healthcare management and clinical decision support. An Agile development methodology was employed to facilitate iterative design, implementation, testing and optimization. To ensure data privacy and integrity, security mechanisms including anonymization, encryption, hashing, authentication and access control were incorporated into the framework. The performance of the framework will be

evaluated using key metrics to assess its accuracy, efficiency, reliability and security.

This study employed four publicly available healthcare datasets; the Pima Indians Diabetes, Wisconsin Breast Cancer, Heart Disease and Chronic Kidney Disease datasets, comprising 2,762 patient records and 75 diagnostic features. The datasets were preprocessed through cleaning, normalization, feature extraction and handling of missing values before being divided into training, validation and testing sets. The processed data were used to train and evaluate the AI diagnostic model, while anonymization ensured patient privacy. Diagnostic outputs and confidence scores were secured using hashing and AES encryption and stored on the blockchain to guarantee data integrity, security and traceability.

The framework was implemented using Python programming language alongside machine learning libraries such as TensorFlow, Keras, Scikit-learn and PyTorch for AI model development and evaluation. Blockchain functionalities and smart contracts were implemented using Ethereum, Hyperledger Fabric and Solidity programming language. Additional technologies like Flask, Node.js, MongoDB, MySQL, cloud databases and RESTful APIs were utilized for system integration, healthcare data management and web-based application development.

The secured AI-blockchain-enabled framework for data-driven medical diagnostic

systems consists of interconnected layers that facilitate secure and intelligent healthcare diagnosis. These layers include; Data Sources Layer, Data Acquisition and Preprocessing Layer, AI Diagnostic Intelligence Layer, Blockchain Security Layer, The Data Sources Layer, Secure Storage Layer, Application and User Layer and Cross-Cutting Security, Privacy Layer and Interoperability and Standards Layer. Data sources layer collects healthcare data from sources such as electronic health records, medical images, laboratory results, wearable devices and patient information. These data are processed in the data acquisition and preprocessing layer through cleaning, normalization, feature extraction, anonymization and encryption before being forwarded to the AI diagnostic intelligence layer for disease prediction, risk assessment and clinical decision support.

The diagnostic outputs are secured in the blockchain security layer using hashing, digital signatures, smart contracts and distributed ledger technologies to ensure integrity, transparency and traceability. The validated records are then stored in the secured storage layer using encrypted databases, cloud storage and IPFS. Authorized users access diagnostic reports and recommendations through the application and user layer. Supporting all layers are the cross-cutting security and privacy layer, which provides authentication, access control, encryption and compliance mechanisms and the interoperability and standards layer, which enables seamless data exchange among healthcare systems. Together, these layers form a secure, transparent and scalable framework for data-driven medical diagnosis as seen in figure 1.

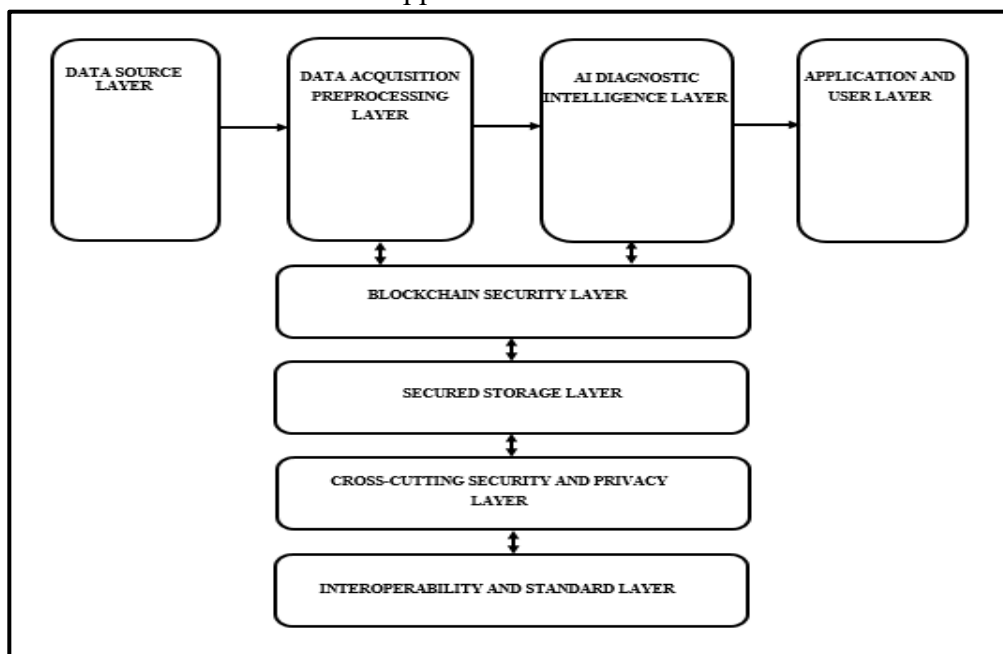


Figure 1: System's Architecture

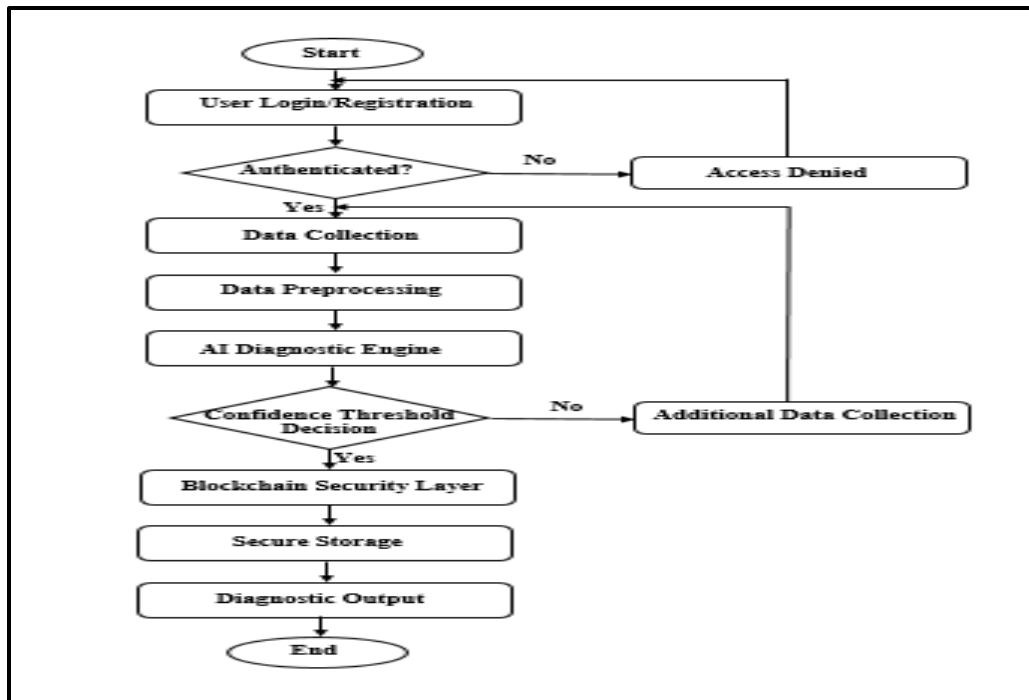


Figure 2: The System's Flowchart

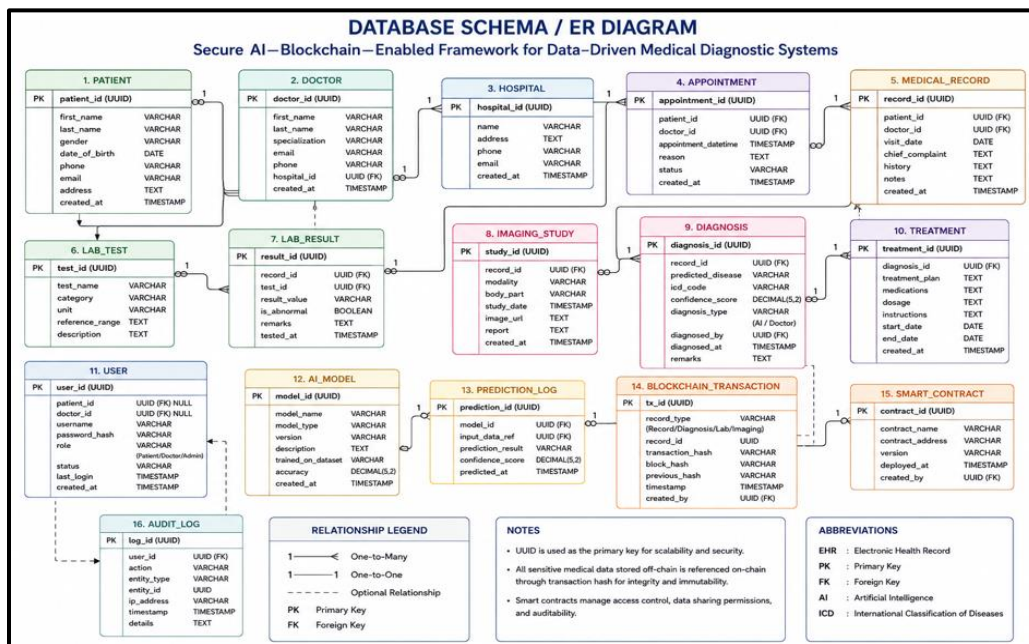


Figure 3: The Database Schema/ER Diagram of the System

The framework's algorithm is divided in five models; Healthcare data acquisition and preprocessing, AI-based medical diagnosis, blockchain-based medical record security, smart contract access control and integrated AI-blockchain diagnostic algorithm.

Algorithm 1: Healthcare Data Acquisition and Preprocessing

Input: Patient healthcare data D from EHRs, IoMT devices, wearable sensors and medical imaging systems.

Output: Cleaned and standardized dataset P.

1. Start
2. Collect healthcare data D from multiple sources.
3. Validate data completeness and format consistency.
4. Remove duplicate and corrupted records.
5. Handle missing values using suitable imputation techniques.
6. Normalize and standardize dataset attributes.
7. Extract relevant diagnostic features F.
8. Store preprocessed dataset as P.
9. End.

Algorithm 2: AI-Based Medical Diagnosis

Input: Preprocessed healthcare dataset P.

Output: Disease prediction result R and confidence score C.

1. Start
2. Load trained AI model M.
3. Input patient features F from dataset P.
4. Perform feature selection and dimensionality reduction.
5. Apply machine learning/deep learning model M.
6. Compute disease prediction probability.
7. Generate diagnostic result R.
8. Calculate confidence score C.
9. Forward results to blockchain validation module.
10. End.

Algorithm 3: Blockchain-Based Medical Record Security

Input: Diagnostic result R, patient record PR.

Output: Immutable blockchain transaction T.

1. Start
2. Receive diagnostic result R.
3. Generate cryptographic hash H of patient record PR.
4. Encrypt sensitive healthcare information using AES.
5. Create blockchain transaction T.
6. Attach hash H and encrypted data to T.
7. Broadcast transaction to blockchain network.
8. Validate transaction using consensus protocol.
9. Append validated block to distributed ledger.
10. End.

Algorithm 4: Smart Contract Access Control

Input: User request U, patient record PR.

Output: Access decision A.

1. Start
2. Receive access request U.
3. Verify user identity credentials.
4. Execute smart contract SC.
5. Check authorization permissions.
6. If permission is valid:
Grant access.
Else:
Deny access.
7. Log access activity on blockchain.
8. Return access decision A.
9. End.

Algorithm 5: Integrated AI–Blockchain Diagnostic Framework

Input: Patient healthcare data D.

Output: Secure diagnostic report SR.

1. Start
2. Acquire patient data D.
3. Preprocess data using Algorithm 1.
4. Generate diagnosis using Algorithm 2.
5. Secure diagnostic records using Algorithm 3.
6. Verify user access through Algorithm 4.
7. Generate secure diagnostic report SR.
8. Notify authorized healthcare practitioners.
9. Update distributed healthcare ledger.
10. End.

Table 1: Symbols and Meanings Used in the Algorithm

S/N	Symbol	Meaning
1	D	Raw healthcare dataset collected from Electronic Health Records (EHRs), medical imaging systems, wearable devices, IoMT sensors and other healthcare sources.
2	P	Preprocessed healthcare dataset obtained after data cleaning, normalization, transformation and feature preparation.
3	F	Set of relevant healthcare features extracted from the dataset for disease diagnosis and prediction.
4	M	Trained Artificial Intelligence (AI) model
5	R	Diagnostic result or disease prediction generated by the AI model.
6	C	Confidence score indicating the probability or certainty level associated with the diagnostic prediction.
7	PR	Patient Record containing personal, clinical, laboratory and diagnostic information of a patient.
8	H	Cryptographic hash value generated from patient records or diagnostic results.
9	T	Blockchain transaction containing encrypted healthcare information and associated metadata for ledger storage.
10	SC	Smart Contract responsible for enforcing access control, authorization and transaction validation rules.
11	U	User access request submitted by healthcare professionals, patients, researchers, or other authorized stakeholders.
12	A	Access decision returned by the smart contract, indicating whether access is granted or denied.
13	B	Blockchain ledger that stores validated and immutable healthcare transactions in a decentralized manner.
14	SR	Secure Diagnostic Report generated after AI diagnosis and blockchain verification.
15	AES	Advanced Encryption Standard used to encrypt sensitive healthcare data before blockchain storage.
16	IoMT	Internet of Medical Things comprising interconnected medical devices and healthcare sensors that generate patient data.
17	EHR	Electronic Health Record containing digital patient medical information and healthcare history.

Mathematical Representation of the Framework

Input Dataset

$$D = \{x_1, x_2, x_3, \dots, x_n\} \quad (1)$$

where:

x_i = Patient medical records.

Encryption Function

$$E_d = AES(P_d, K) \quad (2)$$

where:

E_d = Encrypted patient data

K = Encryption key

Hash Generation and AI Diagnostic Prediction

$$H_p = SH\ A256(E_d) \quad (3)$$

$$D_r = AI(F_m) \quad (4)$$

where:

F_m = Extracted medical features

D_r = Diagnostic output

Confidence Score and Blockchain Record

$$C_s = \max(P(y/F_m)) \quad (5)$$

$$B_t = \{H_p, H_d, \text{Timestamp}, \text{ProviderID}\} \quad (6)$$

where:

$P(y/F_m)$ = Probability of disease class y

H_p = Hash Pointer

H_d = Hash of the data

Performance Evaluation Metrics

The performance of the secured AI-blockchain-enabled framework for data-driven medical diagnostic systems was evaluated using Accuracy, Precision, Recall, F1-Score, Area Under the Receiver Operating Characteristic Curve (AUC-ROC), Data Integrity Rate and Access Control Success Rate. Accuracy measures overall prediction correctness, while precision, recall and F1-score assess the effectiveness of disease classification. AUC-

ROC evaluates the model's ability to distinguish between classes across different thresholds. Data integrity rate measures the protection of healthcare records from unauthorized modification, while access control success rate evaluates the effectiveness of blockchain-based access control mechanisms. Together, these metrics provide a comprehensive assessment of the framework's diagnostic performance, security and reliability.

Result and Discussion

The performance evaluation of the secured AI-blockchain framework and the conventional method was conducted using seven key metrics: accuracy, precision, recall, f1-score, AUC-roc, data integrity rate and access control success rate across four disease datasets, namely diabetes mellitus, breast cancer, heart disease and chronic kidney disease. The results presented in Table 2 indicate that the framework consistently outperformed the conventional method across all evaluated metrics and disease categories.

For accuracy, the conventional method achieved values ranging from 82.1% to 90.5%, whereas the secured AI-blockchain framework recorded significantly higher values ranging from 95.8% to 98.0%. Similarly, precision improved from a range of 81.8%–89.8% in the conventional approach to 95.8%–98.5% in the secured AI-blockchain framework. This demonstrates the framework's ability to reduce false-positive predictions and improve diagnostic reliability.

The recall values also showed substantial improvement, increasing from 82.1%–90.5% for the conventional method to 96.1%–98.9% for the secured AI-blockchain framework. High recall values indicate the framework's effectiveness in correctly identifying patients with the targeted diseases. Likewise, the F1-Score, which provides a balanced assessment of precision and recall, increased from 81.9%–

90.1% to 95.9%–98.7%, confirming the superior predictive capability of the secured AI-blockchain system.

In terms of classification performance, the AUC-ROC values improved from 84.3%–91.4% under the conventional method to 97.2%–99.1% with the AI-blockchain framework. This result demonstrates a stronger ability of the secured AI-blockchain framework to distinguish between positive and negative disease cases.

The security-related metrics further highlight the benefits of blockchain integration. The data integrity rate increased from 88.5%–89.2% for the conventional method to a near-perfect 99.9% across all disease datasets. Similarly, the access control success rate improved from 87.4%–88.3% to 99.5%–99.7%, indicating enhanced protection of sensitive medical records and improved authorization management.

The average performance results presented in Table 3 reveal that the secured AI-blockchain framework achieved superior results across all metrics. Accuracy increased from 85.93% to 97.28%, precision from 85.33% to 97.28%, recall from 85.93% to 97.68%, F1-score from 85.58% to 97.45%, AUC-ROC from 87.35% to 98.25%, data integrity rate from 88.88% to 99.90% and access control success rate from 87.93% to 99.63%. The corresponding improvements ranged from 10.90% to 11.95%, with an average improvement rate of 11.51%.

Furthermore, the overall average performance 98.21%. This significant improvement comparison in Table 4 shows that the demonstrates the effectiveness of combining conventional method achieved an overall artificial intelligence and blockchain average performance rate of 86.70%, while the technologies to enhance both diagnostic secured AI-blockchain framework achieved accuracy and healthcare data security.

Table 2: Performance Evaluation Metrics of the Frameworks

S/N	Performance Metrics	Method	Diabetes Mellitus	Breast Cancer	Heart Disease	Chronic Kidney Disease
1	Accuracy (%)	Conventional Method	82.1	90.5	84.8	86.3
		AI-Blockchain Framework	95.8	98.5	96.8	98.0
2	Precision (%)	Conventional Method	81.8	89.8	84.1	85.6
		AI-Blockchain Framework	95.8	98.5	96.8	98.0
3	Recall (%)	Conventional Method	82.1	90.5	84.8	86.3
		AI-Blockchain Framework	96.1	98.9	97.3	98.4
4	F1-Score (%)	Conventional Method	81.9	90.1	84.4	85.9
		AI-Blockchain Framework	95.9	98.7	97.0	98.2
5	AUC-ROC (%)	Conventional Method	84.3	91.4	86.2	87.5
		AI-Blockchain Framework	97.2	99.1	97.8	98.9
6	Data Integrity Rate (%)	Conventional Method	88.5	89.2	88.8	89.0
		AI-Blockchain Framework	99.9	99.9	99.9	99.9
7	Access Control Success Rate (%)	Conventional Method	87.4	88.1	87.9	88.3
		AI-Blockchain Framework	99.5	99.7	99.6	99.7

Table 3: Average Performance Evaluation Metrics/Improvement of the Frameworks

S/N	Metric	Conventional Average (%)	AI-Blockchain Average (%)	Improvement (%)
1	Accuracy	85.93	97.28	+11.35
2	Precision	85.33	97.28	+11.95
3	Recall	85.93	97.68	+11.75
4	F1-Score	85.58	97.45	+11.87
5	AUC-ROC	87.35	98.25	+10.90
6	Data Integrity Rate	88.88	99.90	+11.02
7	Access Control Success Rate	87.93	99.63	+11.70

Table 4: Overall Average Performance /Improvement Rate of the Frameworks

S/N	Method	Overall Average (%)
1	Conventional Method	86.70%
2	AI-Blockchain Framework	98.21 %

Average Performance Rate for Conventional method =

$$85.93+85.33+85.93+85.58+87.35+88.88+87.93 / 7 = 86.70\% \quad (7)$$

Average Performance Rate for AI-Blockchain Framework =

$$97.28+97.68+97.45+98.25+99.90+99.63+97.28 / 7 = 98.21\% \quad (8)$$

Average Improvement Rate =

$$11.35+11.95+11.75+11.87+10.90+11.02+11.70 / 7 = 11.51\% \quad (9)$$

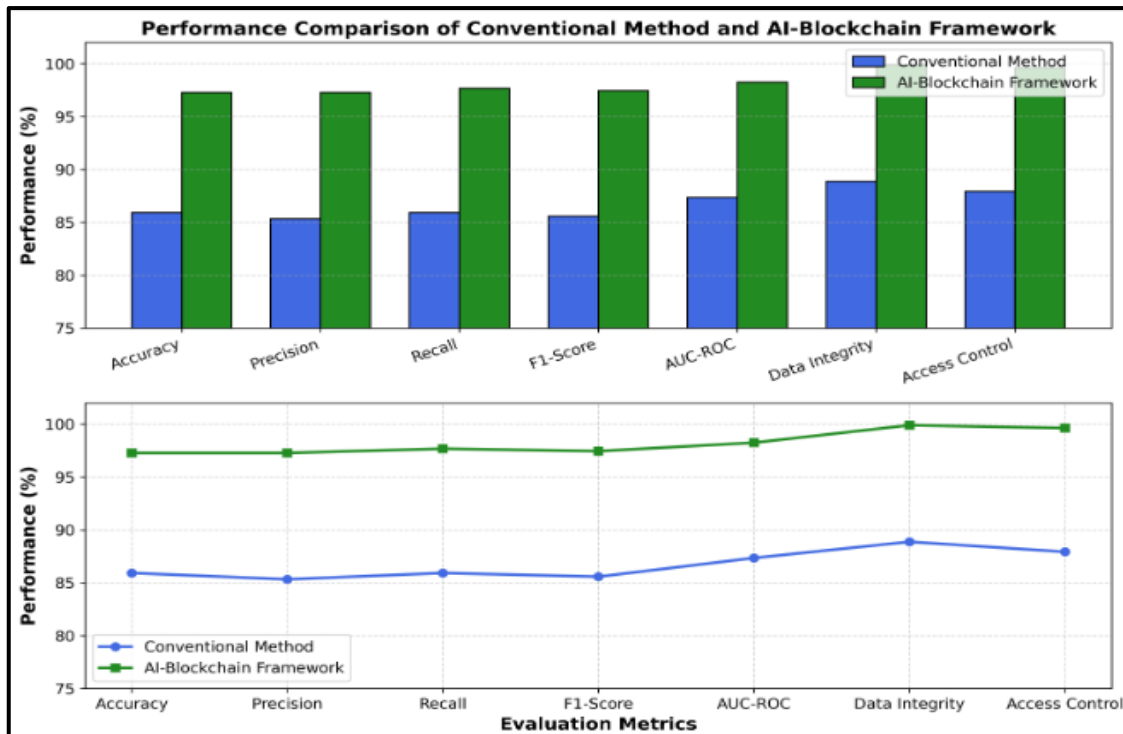


Figure 4: A combined diagram (bar chart and line graph) showing the performance comparison between the conventional method and the AI-blockchain framework. Some screenshots of the AI-blockchain framework are captured in fig 5, 6 and 7.

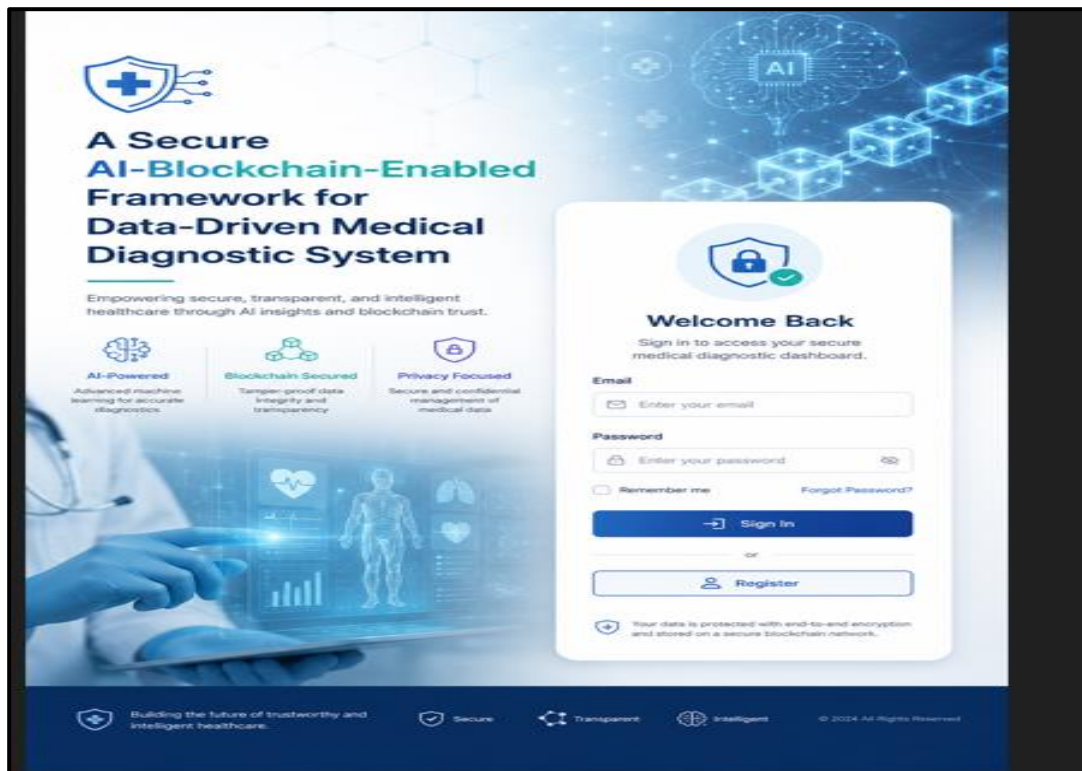


Figure 5: The Login/Welcome Page of the Framework

Enter New Patient Data
Provide comprehensive and accurate data for AI-driven diagnostic analysis.

1 Patient Information

Patient ID * Full Name * Date of Birth *

Gender * Contact Number Email

Address

2 Clinical Information

Chief Complaint / Symptoms * Duration of Symptoms *

Medical History Family History

Lifestyle Factors ☐ Smoking ☐ Alcohol ☐ Physical Activity ☐ Poor Diet ☐ Others

3 Vital Signs

Temperature (°C) Heart Rate (bpm) Blood Pressure (mmHg) Respiratory Rate (breaths/min) SpO₂ (%)

4 Laboratory & Test Results

Test Name	Result	Unit	Reference Range	Date	Action
No test data added yet.					

Data Summary

- Patient Information Incomplete
- Clinical Information Incomplete
- Vital Signs Incomplete
- Lab/Test Results Incomplete
- Overall Status Incomplete

Data Integrity
All required fields must be completed for accurate AI analysis.

Security & Privacy

- End-to-end encryption
- Blockchain recorded
- Access controlled
- HIPAA compliant

Secure. Transparent. Intelligent.
Powered by AI & Blockchain

© 2024 All Rights Reserved

Figure 6: The Input Page of the Framework

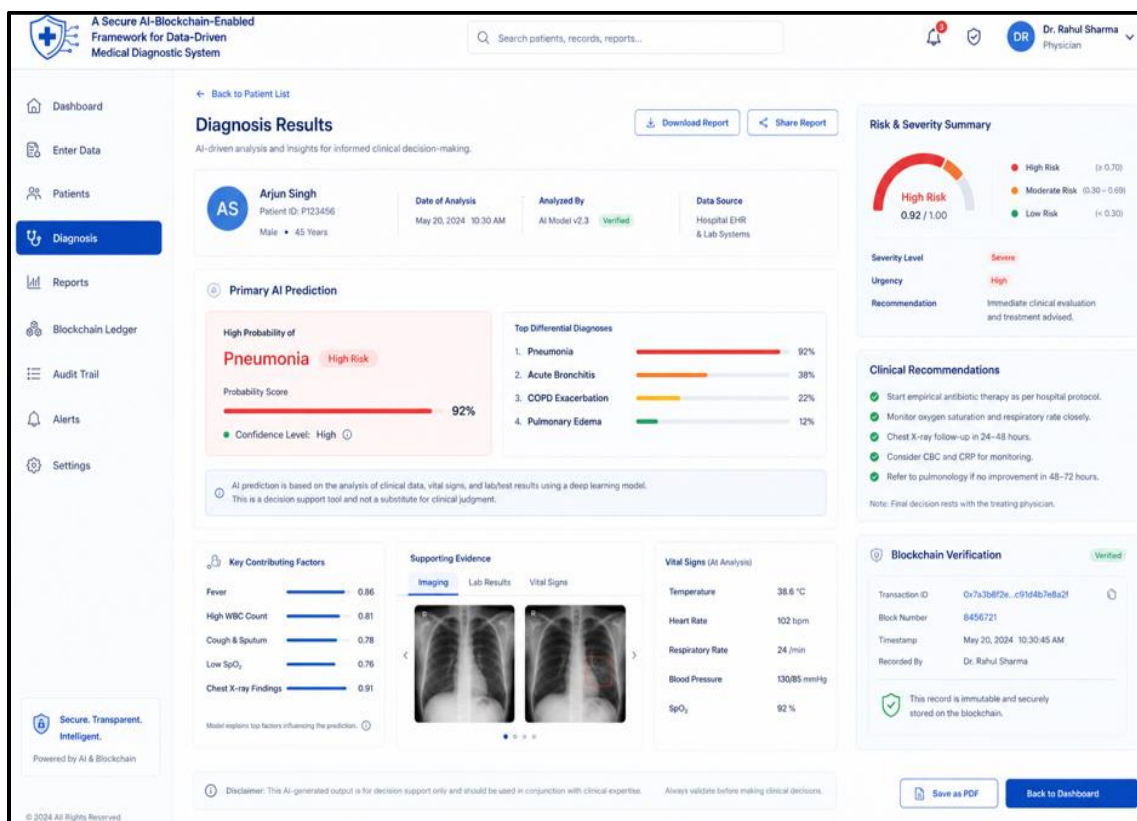


Figure 6: The Output/Information Page of the Framework

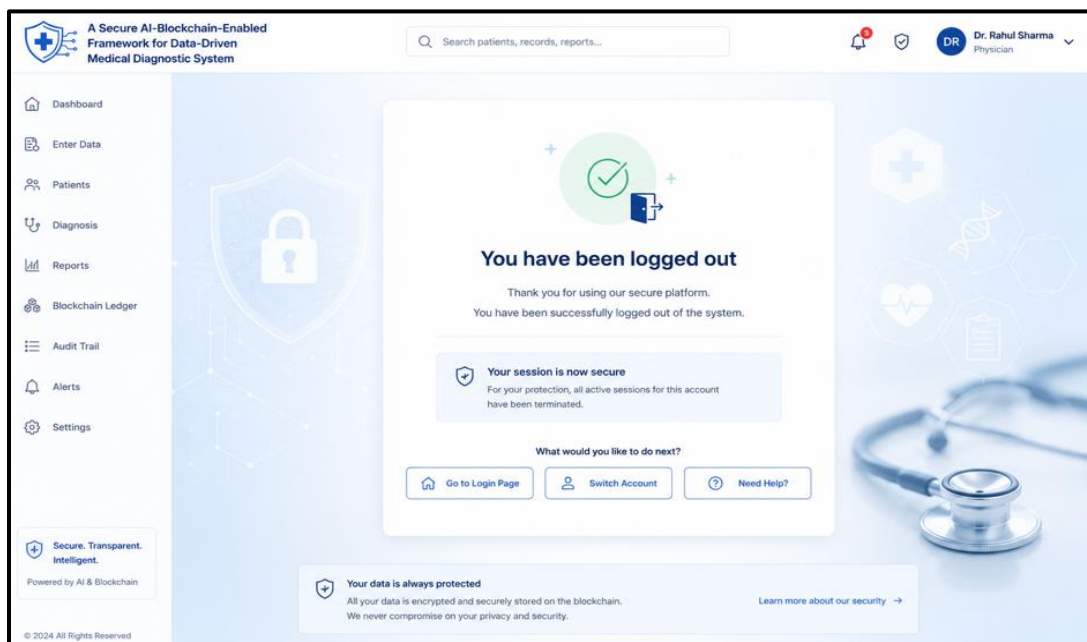


Figure 7: The Logout Page of the Framework

Conclusion

This study presents a secured AI-blockchain-enabled framework for data-driven medical diagnostic systems, designed to enhance diagnostic accuracy while ensuring the security, privacy and integrity of healthcare data. The experimental results demonstrated that the secured AI-blockchain-enabled framework consistently outperformed the conventional method across all evaluated performance metrics. Specifically, the AI-blockchain framework achieved average scores of 97.28% accuracy, 97.28% precision, 97.68% recall, 97.45% F1-score and 98.25% AUC-ROC, compared to 85.93%, 85.33%, 85.93%, 85.58% and 87.35%, respectively, for the conventional approach. Furthermore, the integration of blockchain technology significantly strengthened healthcare data protection, increasing the data integrity rate from 88.88%

to 99.90% and the access control success rate from 87.93% to 99.63%. These findings demonstrate that the AI-blockchain framework provides a highly accurate, reliable and secure platform for intelligent medical diagnosis and healthcare data management.

The secured AI-blockchain framework achieved an average performance rate of 98.21%, compared to 86.70% for the conventional system, representing an overall improvement rate of 11.51%. These results demonstrate that integrating AI and blockchain enhances both diagnostic accuracy and healthcare data security. While AI improves disease prediction performance, blockchain ensures secure and reliable management of medical records, making the framework an effective solution for modern healthcare systems.

Future research may focus on validating the framework using larger real-world clinical datasets, incorporating advanced deep learning models and exploring interoperability with emerging healthcare technologies such as the Internet of Medical Things (IoMT), federated learning and cloud-edge computing environments to further enhance scalability and practical deployment.

References

- Abbas, S. R., Khan, M. A., Alharbi, F., Alshamrani, S., Alsubhi, K., & Alzahrani, A. (2026). A systematic review of security, interoperability and AI-IoT integration in blockchain-enabled smart health systems. *Digital Health*, 12, 1–28. <https://doi.org/10.1177/20552076261420985>
- Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, 7(2), 56. <https://doi.org/10.3390/healthcare7020056>
- Anazia, K. E. (2026). Smart governance in Nigerian higher education: Integrating artificial intelligence for integrity and effective university leadership. *International Journal of Innovative Science and Research Technology*, 11(2), 66–74. <https://doi.org/10.38124/ijisrt/26feb106>
- Anazia, K. E., Maduabuchukwu, C., Idongesit, F. O., Benafa, F. C., Idama, R. O., & Eti, I. F. (2025). A novel mobile-based blood donation model for emergency situations. *International Journal of Engineering and Computer Science*, 14(10). <https://doi.org/10.18535/ijecs/v14i10.5288>
- Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115. <https://doi.org/10.1016/j.inffus.2019.12.012>
- Esteva, A., Robicquet, A., Ramsundar, B., Kuleshov, V., DePristo, M., Chou, K., Cui, C., Corrado, G., Thrun, S., & Dean, J. (2019). A guide to deep learning in healthcare. *Nature Medicine*, 25(1), 24–29. <https://doi.org/10.1038/s41591-018-0316-z>
- Eti, I. F., Anazia, K. E., Okeke, V. O., Benafa, F. C., & Orugba, K. (2025). A secured blockchain database management model for medical-based organizations. *International Journal of Advances in Engineering and Management*, 7(5), 312–323. <https://doi.org/10.35629/5252-0705312323>
- Houssein, E. H., Ibrahim, A., Hassaballah, M., Hosney, M. E., & Oliva, D. (2026). Fundamentals applications of blockchain impact on intelligent healthcare systems: A systematic review. *Discover Internet of Things*. <https://doi.org/10.1007/s43926-025-00252-z>
- Hussien, H. M., Yasin, S. M., Udzir, N. I., Zaidan, A. A., & Zaidan, B. B. (2022). A systematic review for enabling of developing a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and

- future direction. *Journal of Medical Systems*, 43(10), 320. <https://doi.org/10.1007/s10916-019-1445-8>
- Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017). Artificial intelligence in healthcare: Past, present and future. *Stroke and Vascular Neurology*, 2(4), 230–243. <https://doi.org/10.1136/svn-2017-000101>
- Kumar, R., Khan, A. A., Kumar, J., Golilarz, N. A., Zhang, S., Ting, Y., & Zheng, C. (2023). Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging. *IEEE Journal of Biomedical and Health Informatics*, 27(1), 238–249. <https://doi.org/10.1109/JBHI.2022.3217158>
- Kumar, R., Marchang, N., & Tripathi, R. (2023). Distributed and secure healthcare data management using blockchain technology: A review. *Journal of King Saud University–Computer and Information Sciences*, 35(2), 100561. <https://doi.org/10.1016/j.jksuci.2022.101561>
- Liu, J., & Hu, X. (2026). Blockchain meets AI in healthcare: A review of convergent technologies for digital health transformation. *Frontiers in Blockchain*, 9. <https://doi.org/10.3389/fbloc.2026.1766092>
- Maduabuchukwu, C., Anazia, K. E., & Nwokolo, G. A. (2026). An intelligent role-based access control model enhanced with risk-based multi-factor authentication. *International Journal of Research and Innovation in Applied Science*, 11(4), 898–907. <https://doi.org/10.51584/IJRIAS.2026.110400057>
- Maduabuchukwu, C., Anazia, K. E., Usih, M. E., & Oboro, E. (2026). A distributed AI-enabled semantic platform for research collaboration and knowledge management. *International Journal of Engineering and Computer Science*, 15(6), 28580–28586. <https://doi.org/10.18535/ijecs/v15i06.5540>
- Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud-based e-health systems. *IEEE Access*, 7, 66792–66806. <https://doi.org/10.1109/ACCESS.2019.2917555>
- Rajpurkar, P., Chen, E., Banerjee, O., & Topol, E. J. (2022). AI in health and medicine. *Nature Medicine*, 28(1), 31–38. <https://doi.org/10.1038/s41591-021-01614-0>
- Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2026). Ensuring the integrity of AI models: A blockchain-based framework for secure healthcare diagnostics. *Scientific Reports*, 16, 44040. <https://doi.org/10.1038/s41598-026-44040-3>
- Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D., Rahman, M. H., Otrisal, P., & Behl, T. (2021). Blockchain and artificial intelligence technology in e-health. *Environmental Science and Pollution Research*, 28(38), 52810–52831. <https://doi.org/10.1007/s11356-021-15175-3>