IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

Development of Robust Trust Management Framework for Medical IoT

K Chakravarthy Bheri[1], Manas Kumar Y[2]

M. Tech Scholar, CSE, Pragati Engineering college, Kakinada, India[1]

Assistant Professor, CSE, Pragati Engineering college, Kakinada, India[2]

Abstract: Modern healthcare without IoT devices is un imaginable. They've diffused into almost every corner of patient monitoring—tracking heart rates, oxygen levels, you name it. And honestly, things run a lot smoother because of them. But this shift hasn't come without problems—security and trust have become major concerns. To tackle this, we built a system that brings together blockchain and deep learning to keep an eye on devices in real time and figure out which ones can be trusted. The system uses three different deep learning models working together to constantly evaluate device trust. One looks for anomalies using LSTM, another analyzes behavior with CNN, and a third predicts threats through GRU. All of this is backed by a simple but effective blockchain that keeps a tamper-proof record of trust scores and transactions—making things transparent and easy to audit Healthcare administrators can monitor device status, see trust distributions, handle alerts, and investigate blockchain transactions using the system's interactive graphical user interface, which was created with Tkinter. Effective trust score computation across various device types, including the heart, is demonstrated by experimental results

Keywords: blockchain, deep learning, healthcare security, Internet of Things, trust management

I. INTRODUCTION

You can't picture a hospital without them anymore—heart monitors, ventilators, infusion pumps, glucose monitors. They're everywhere, quietly doing their job, collecting data, and sometimes even making decisions. But here's something that doesn't get discussed enough: all that data is extremely valuable to cybercriminals. And protecting these devices? It's really difficult. They come in too many varieties, have limited processing power, and use different communication methods. So, the standard security measures? They often just don't work [1]. Recent advances in blockchain-enabled healthcare systems have demonstrated promising results in addressing these challenges through decentralized identity management and secure authentication mechanisms [2]. Trust management has emerged as a critical paradigm for securing IoT ecosystems, moving beyond binary authentication to continuous assessment of device behaviour and data integrity [3]. In healthcare settings, where device malfunctions or security breaches can have life-threatening consequences, establishing robust trust mechanisms is paramount. Current approaches to IoT security in healthcare face several limitations including centralized trust authorities that create single points of failure, lack of transparency in trust score calculation, insufficient consideration of device behaviour patterns, and inadequate audit trails for regulatory compliance [4]. Blockchain technology offers promising solutions to these challenges through its decentralized, immutable, and transparent nature [5]. By recording trust scores and device transactions on a distributed ledger, healthcare institutions can maintain verifiable histories of device behaviour while eliminating reliance on centralized trust authorities. Simultaneously, deep learning models have demonstrated remarkable capabilities in anomaly detection and behavioral analysis, making them ideal for identifying suspicious device activities that might indicate security compromises [6]. Recent research has shown that hybrid deep learning architectures combining CNNs, LSTMs, and autoencoders can achieve superior performance in detecting anomalies in physiological signals while maintaining low latency suitable for edge deployment [7]. In this paper, we introduce a Medical IoT Trust Management System that brings together blockchain and deep learning to assess device trust more thoroughly. Figure 1 shows how all the pieces fit together in a single, unified framework setup

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

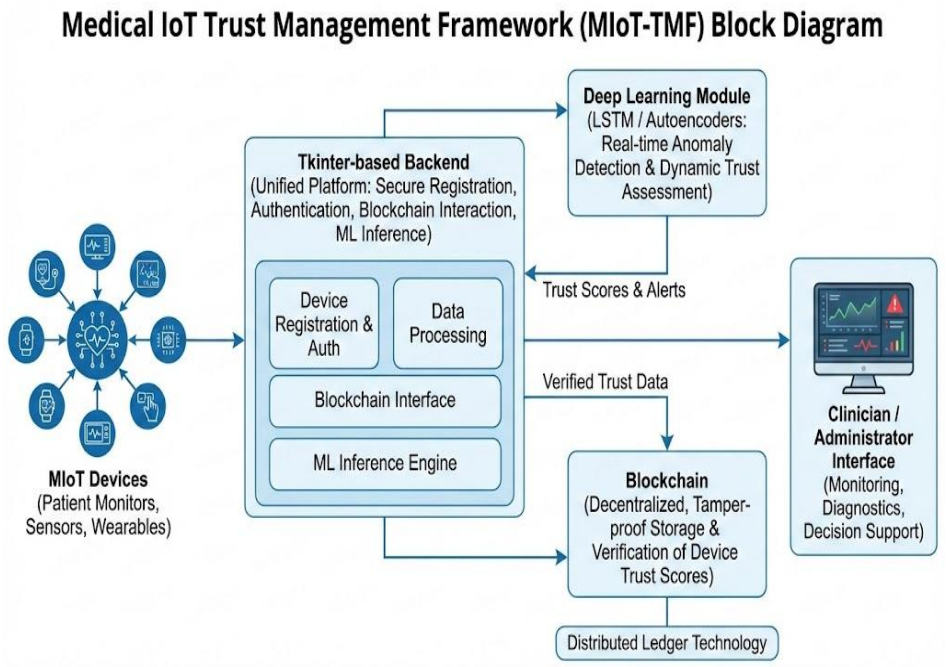

Figure 1. System Architecture of Medical IoT Trust Management Framework

The key contributions of this work are:

1. A multi-layered trust evaluation framework incorporating three specialized deep learning models for anomaly detection, behavioral analysis, and threat prediction
2. A lightweight blockchain tailored for constrained IoT systems to securely and immutably record trust scores and data exchanges
3. A user-friendly GUI offering live visual insights into device states, trust variations, notification logs, and transaction histories within the blockchain
4. A CSV-based data persistence layer enabling easy integration with existing healthcare information systems
5. Comprehensive alert management and system health monitoring capabilities for healthcare administrators.

II. RELATED WORK

A. Trust Management in IoT Systems

Trust management in IoT environments has been extensively studied, with various approaches ranging from reputation-based systems to behavior-based trust evaluation. Chen et al. [8] developed a fuzzy logic-based trust model that considers multiple trust factors including honesty, cooperativeness, and community interest. While effective in simulation environments, these approaches lack integration with real-time monitoring capabilities essential for healthcare applications. A comprehensive survey by Yan et al. [22] provides foundational understanding of trust management challenges in IoT ecosystems. Recent advances in intent-based trust management have led to frameworks like Stack Trust, which integrates decision trees, support vector machines, and random forests within a logistic regression meta-learner to enhance classification robustness [9]. Stack Trust incorporates adaptive weighting mechanisms that periodically adjust model influence based on current performance metrics, achieving precision, recall, and F1-scores of 0.99 across 45,000 instances. This demonstrates the potential of ensemble learning approaches for IoT trust management in resource-constrained environments. Liu et al. [23] provide a comprehensive survey on blockchain-based trust management approaches, highlighting the convergence of distributed ledger technology with trust evaluation mechanisms

B. Deep Learning for Anomaly Detection

Deep learning has proven highly effective for detecting anomalies in IoT data streams. For instance, Rahman et al. [10] applied LSTM networks to healthcare sensor data, achieving 94% accuracy in identifying abnormal patient readings, though their focus remained on health anomalies rather than device security. In a separate effort, Zhang et al. [11] used CNNs for behavioral analysis of IoT devices to spot operational deviations, but their approach stopped short of integrating these insights into a trust-based security framework. Bridging this gap, Mavai, Mishra, and Sharma [7] introduced a hybrid deep learning model combining CNNs, LSTMs, and VAEs. Their system features a Trust-Aware Controller (TAC) that calculates real-time trust scores based on anomaly likelihood, context entropy, and historical behavior, achieving an average F1-score of 94.3% for anomaly detection and 96.1% accuracy in access decisions. The system maintains real-

DOI: 10.17148/IJARCCE.2026.15394

time inference latency under 160 ms on edge hardware, validating feasibility for critical healthcare deployments. Recent work by Hernandez-Jaimes, Martinez-Cruz, Ramírez-Gutiérrez, and Morales-Reyes [12] introduced attention-driven deep neural networks for network traffic inspection in IoMT environments. By applying principles from natural language processing, their approach achieved precision of 84.43%, recall of 98.73%, and F1-score of 91.02% on the CICIoMT2024 dataset, demonstrating the effectiveness of attention mechanisms in identifying anomalous network patterns.

C. Blockchain in Healthcare IoT

Blockchain technology is increasingly being applied to secure healthcare IoT and ensure data auditability. Azaria et al. [13] developed MedRec, a decentralized system for managing electronic health records that empowers patients with access to their data, though it does not address device-level trust. Dwivedi, Srivastava, Dhar, and Singh [14] extended this concept by proposing a blockchain framework specifically for securing healthcare IoT devices, integrating smart contracts to automate access control. Their work demonstrated the feasibility of blockchain in healthcare IoT but did not address the continuous trust evaluation required for dynamic threat environments. D'Aniello and Fotia [24] provide a comprehensive survey of blockchain and AI-based methods for trust management in IoT, synthesizing recent advances in this rapidly evolving field. The FLIT framework introduced by Das, Banerjee, Chatterjee, Ghosh, and Das Bit [15] combines federated learning with blockchain to enable privacy-preserving data sharing across multiple healthcare stakeholders. Patient data is never shared in raw form and is encrypted and distributed among trusted stakeholders, with access control enforced through smart contracts. This approach mitigates poisoning attacks, inference attacks, and rollback manipulation while enabling collaborative model training without compromising patient privacy.

D. Comprehensive Surveys and Trends

Recent comprehensive surveys have synthesized the state of research in IoMT security. Oloruntoba and Obiniyi [16] provide a detailed review of trends in blockchain applications to IoMT, highlighting lightweight blockchain architectures, integration of federated learning with blockchain, off-chain and distributed storage systems based on IPFS, and emerging post-quantum cryptographic tools. Similarly, a comprehensive survey by El-deep, Abohany, and Sallam [17] explores the impact of various technologies on IoMT, covering blockchain, AI, edge computing, and cloud computing, while addressing interoperability issues, regulatory compliance, and privacy concerns.

Akkal, Cherbal, Annane, and Lakhlef [18] proposed BTMH, a blockchain-powered trust management system specifically designed for IoMT in healthcare, demonstrating improved security and performance metrics through comprehensive evaluation. Xu et al. [19] explored the challenges and opportunities of federated learning for healthcare IoT, highlighting the potential of privacy-preserving collaborative learning while addressing key technical and regulatory hurdles. Their analysis provides a roadmap for implementing federated learning in sensitive healthcare environments. Lax, Nardone, and Russo [25] examined secure health information sharing among healthcare organizations using public blockchain, demonstrating practical applications of distributed ledger technology in healthcare settings.

E. Comparative Analysis

Table 1 presents a comparative analysis of existing approaches relative to our proposed system. The evaluation focuses on five key features: real-time monitoring, trust scoring, blockchain connectivity, deep learning support, and the user interface

Table 1. Comparison of Existing IoT Trust Management Approaches

Approach	Real-time Monitoring	Trust Scores	Blockchain	Deep Learning	GUI
Chen et al. [8]	No	Yes	No	No	No
Rahman et al. [10]	Yes	No	No	LSTM	No
Azaria et al. [13]	No	No	Yes	No	Yes
Dwivedi et al. [14]	Yes	No	Yes	No	No
Awan et al. [9]	Yes	Yes	No	Ensemble	No

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

Mavai et al. [7]	Yes	Yes	No	CNN / LSTM / VAE	No
Das et al. [17]	Yes	Yes	Yes	FL	No
Akkal et al. [22]	Yes	Yes	Yes	No	No
Naik et al. [20]	Yes	Yes	No	Hybrid DL	No
Proposed System	**Yes**	**Yes**	**Yes**	**LSTM / CNN / GRU**	**Yes**

A review of existing literature shows that current systems excel in specific areas of IoT trust management but fall short of providing a holistic solution. Our proposed work bridges this research gap by synthesizing real-time device monitoring, dynamic trust score calculation, the security and auditability of blockchain technology, and a user-centric interface into a single, purpose-built framework for healthcare environments.

III. MATERIALS AND METHODS

A. System Architecture

As illustrated in Figure 1, the proposed system adopts a modular architecture. Its five core components—the Data Persistence Layer, Device Manager, three Deep Learning Models, Trust Calculator, and Blockchain Simulator—are integrated via a graphical user interface, which also facilitates the data flow between them.

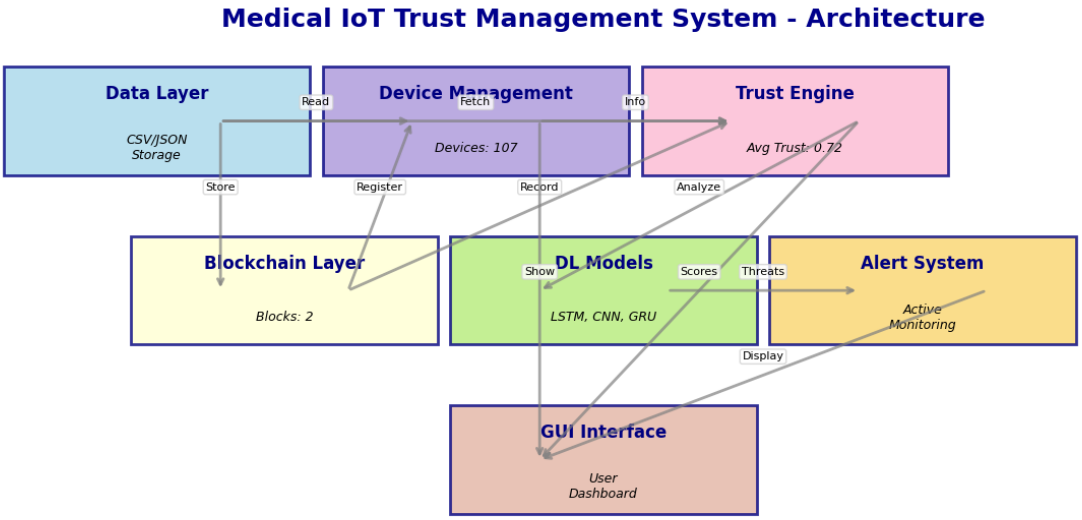

Figure 1: System Architecture Diagram

Figure 1 presents the system architecture, highlighting the integration of the core modules—Device Manager, Deep Learning Models, Trust Calculator, Blockchain Simulator, and GUI—with a CSV-based Data Persistence Layer. This layer, implemented via a CSV Data Handler class, manages six key files (devices.csv, trust_scores.csv, alerts.csv, blockchain.csv, device_data.csv, config.csv). The use of CSV storage was chosen to facilitate compatibility with existing healthcare systems and ensure data accessibility for analysis and auditing.

B. Device Management and Data Simulation

A Device Manager component maintains a registry of all healthcare IoT devices. Each entry includes a unique identifier, device type, patient association, status, and network address. The full device schema is detailed in Table 2

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

Table 2. Device Information Schema

Field	Type	Description	Example
device_id	String	Unique device identifier	DEV001
device_type	String	Type of medical device	heart monitor
patient_id	String	Associated patient identifier	PAT001
status	String	Current operational status	active
ip_address	String	Network IP address	192.168.1.101
mac_address	String	Physical MAC address	00:1A: 2B:3C: 4D:5E
manufacturer	String	Device manufacturer	MedTech Inc.
model	String	Device model number	HM-1000
firmware version	String	Current firmware version	2.1.3
location	String	Physical location	Room 101, ICU

To simulate realistic device behaviour for system testing, we implemented a data generation module that produces synthetic sensor readings appropriate for each device type. To test the deep learning models' detection performance, the simulated data includes realistic variations and anomalies. Figure 2 shows the GUI's Device Overview tab, featuring the complete device registry with color-coded status indicators.

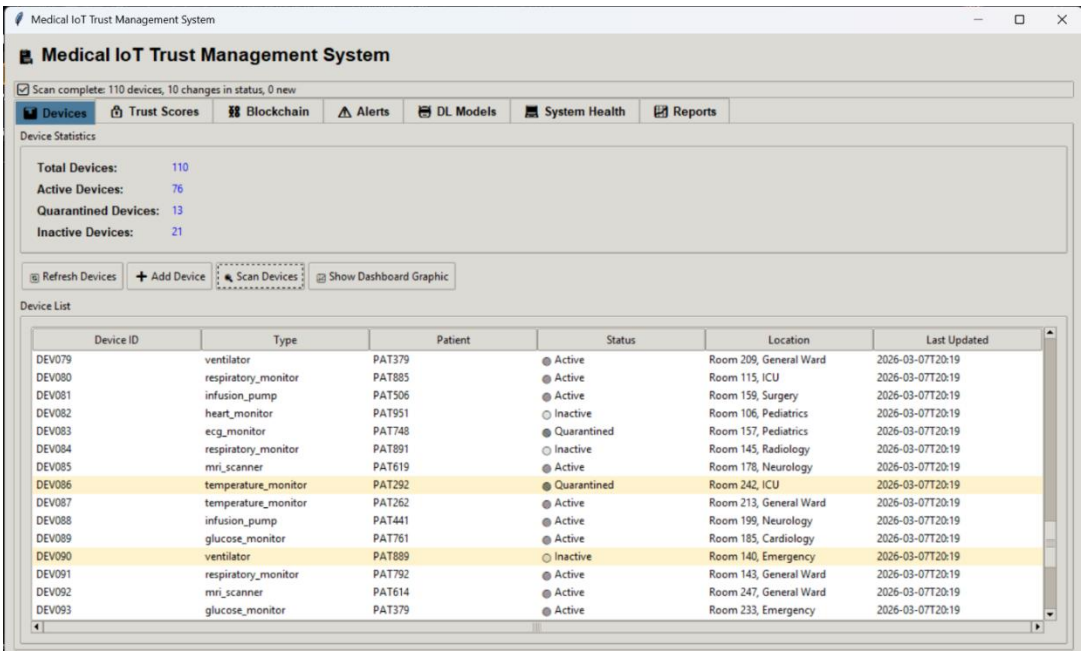

Figure 2. shows the main device management interface. It lists all registered IoT devices, displaying their status, type, patient association, and location. Status is color-coded: green (active), red (quarantined), and yellow (inactive).

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

C. Deep Learning Models for Trust Evaluation

The system incorporates three specialized deep learning models, each addressing a distinct aspect of device trust evaluation. While the current implementation uses simulated model outputs for demonstration purposes, the architecture is designed to accommodate actual trained models based on recent advances in hybrid deep learning architectures [7, 20].

a. Anomaly Detection Model (LSTM)

An LSTM-based model is used for anomaly detection in time-series device data. By capturing long-term dependencies in sequential data, it effectively analyzes sensor streams to flag patterns that diverge from normal baselines. Equation 1 defines the anomaly score calculation based on the reconstruction error of the LSTM autoencoder.

$$AnomalyScore = \frac{1}{N}\sum_{i=1}^{N} | x_i - \hat{x}_i | \quad (1)$$

Where x_i represents the actual sensor reading at time i, $\hat{x}_i$ is the reconstructed value from the LSTM autoencoder, and N is the window size. Higher reconstruction errors indicate potential anomalies requiring investigation. This approach aligns with recent work demonstrating the effectiveness of reconstruction-based anomaly detection in IoT environments [12].

b. Behaviour Analysis Model (CNN)

A CNN-based model analyzes device behavior by mapping operational sequences to a spatial feature space. Its strength in identifying local patterns allows it to detect subtle deviations indicating potential compromise. The model ingests metadata, communication logs, and operational stats to produce a behavioral trust score, as defined in Equation 2.

$$BehaviorScore = \sigma(W \cdot \phi(X) + b) \quad (2)$$

Where X represents the input feature vector, ϕ denotes the CNN feature extraction layers, W and b are learned parameters, and σ is the sigmoid activation function ensuring output in the [0,1] range. This CNN-based approach has demonstrated effectiveness in similar healthcare IoT applications [7].

c. Threat Prediction Model (GRU)

The third model employs Gated Recurrent Units (GRUs) for predicting potential future threats based on historical device behaviour and current trust indicators. GRUs offer computational efficiency comparable to LSTMs while maintaining effective sequence modelling capabilities, making them suitable for real-time prediction in resource-constrained environments. This model generates threat probability scores that inform proactive security measures. Equation 3 defines the threat prediction mechanism.

$$ThreatProbability = GRU(H_t, C_t, T_t) \quad (3)$$

Where H_t represents historical trust scores, C_t captures current behavioral indicators, and T_t encodes temporal patterns in device activity.

D. Trust Score Calculation

The Trust Calculator component integrates outputs from all three deep learning models to compute comprehensive trust scores for each device. The calculation employs a weighted average approach with empirically determined weights reflecting the relative importance of each trust component. Equation 4 presents the trust score calculation formula.

$$TrustScore = \alpha \cdot S_{behavior} + \beta \cdot S_{integrity} + \gamma \cdot S_{historical} \quad (4)$$

Where $S_{behavior}$ is the device behaviour score from the CNN model, $S_{integrity}$ represents data integrity derived from anomaly detection results, and $S_{historical}$ captures historical performance trends. The weights (α, β, γ) were chosen via experimentation and expert input, balancing current behavior with historical patterns. Trust scores determine device status: >0.7 = trusted, 0.5–0.7 = enhanced monitoring, <0.5 = quarantine recommended. This allows automated responses while keeping humans in the loop for borderline cases. Figure 3 shows the Trust Scores tab with a full distribution and component breakdowns.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

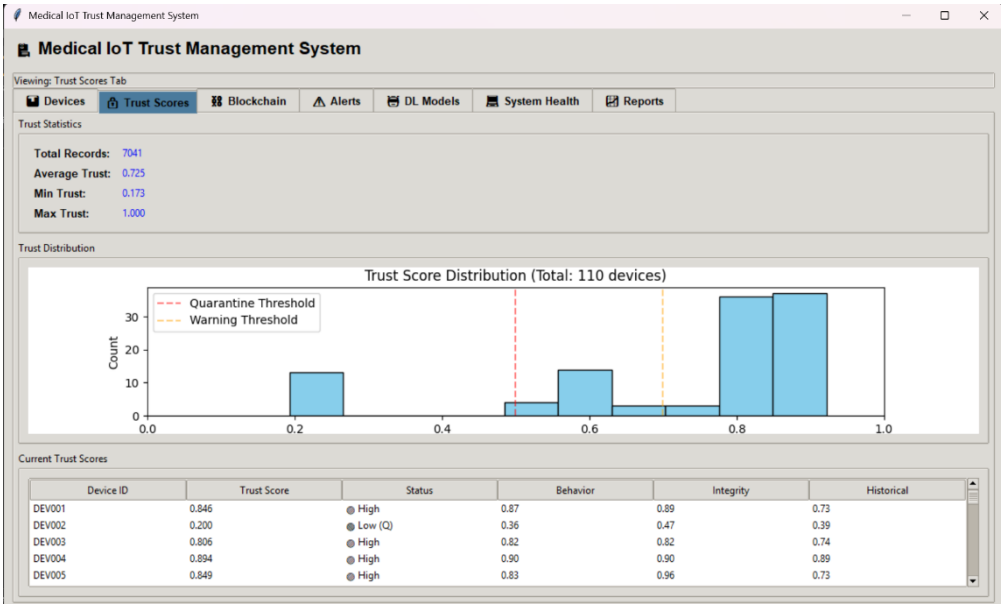

Figure 3. Trust Scores Tab with Distribution Histogram

E. Blockchain Implementation

The Blockchain Simulator ensures auditability by immutably recording all trust scores and device transactions. Each block includes a timestamp, transaction list, previous block hash, and a proof-of-work nonce. It maintains a full history of trust updates, data transmissions, and system events, as illustrated in Figure 4.

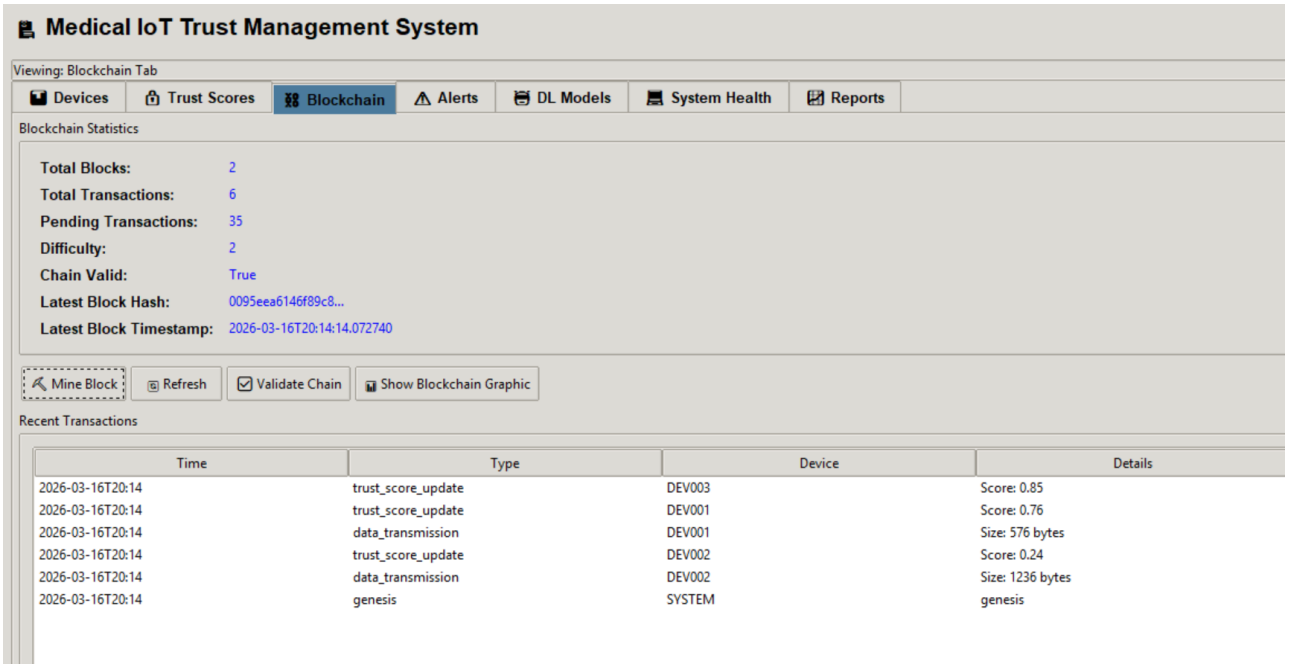

Figure 4. Blockchain Structure for Trust Transaction Recording

Each transaction in the blockchain captures essential information including transaction type (trust score update, data transmission, device registration), device identifier, timestamp, and transaction-specific data payload. For trust score updates, the payload includes the calculated trust score, component scores from each deep learning model, and the change from previous scores. This detailed recording enables forensic analysis of trust evolution over time.

The proof-of-work mechanism implements configurable difficulty levels to balance security requirements with computational overhead. Equation 5 defines the mining condition for new blocks.

$$Hash(Block) < Target \quad (5)$$

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

Where the target value is determined by the difficulty parameter, ensuring that block creation requires computational effort proportional to the security requirements of the healthcare environment. This lightweight approach is consistent with recent recommendations for blockchain deployment in resource-constrained healthcare IoT environments.

F. Graphical User Interface Design

Healthcare administrators interact with the system through a graphical user interface implemented in Python's Tkinter library. To streamline workflows, the interface adopts a tabbed organization, providing access to six distinct management views. This layout is presented in Figure 5

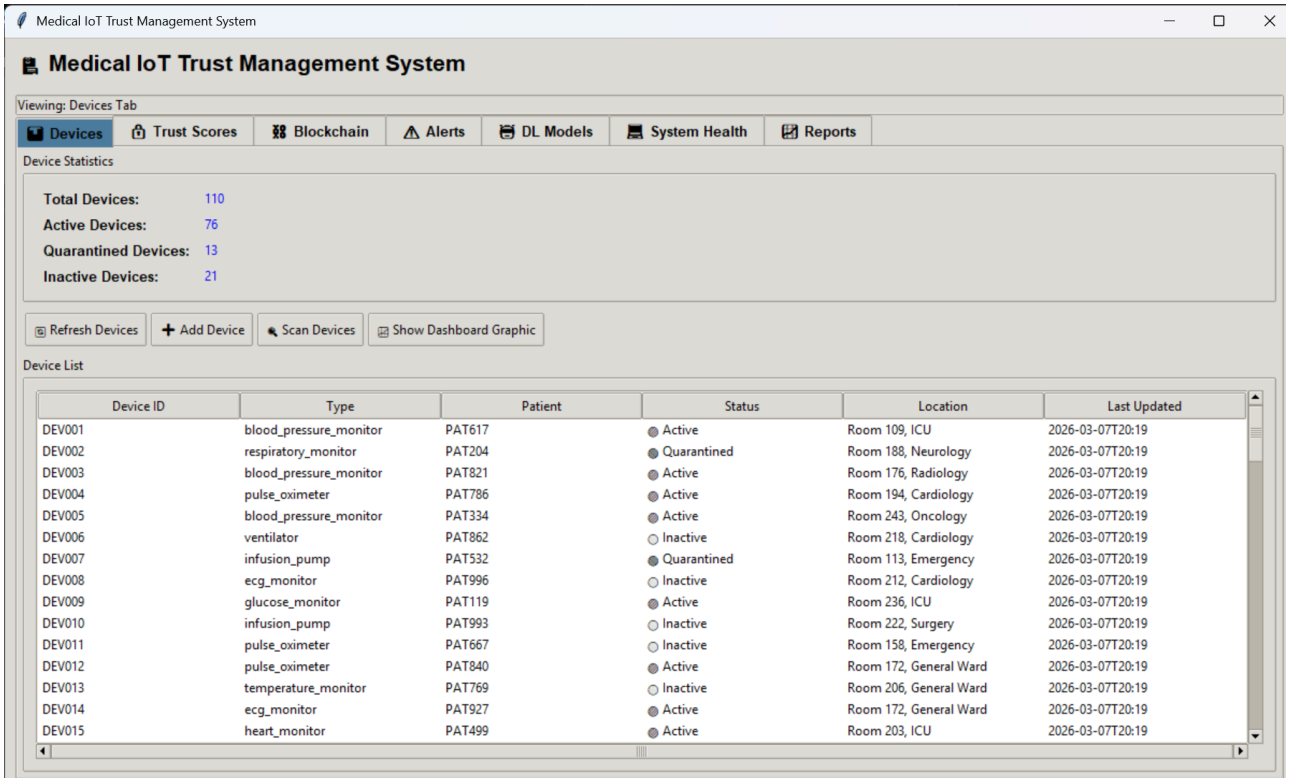

Figure 5. Complete GUI Layout Showing Tabbed Organization

As shown in Figure 6, the Device Overview Tab shows key device statistics (total, active, quarantined, inactive) and a sortable, color-coded tree view of device details. Administrators can add devices, refresh the list, or double-click for more information.

Figure 6. Add Device Dialog Interface

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

Trust Scores Tab: Displays histogram plots of trust score distributions and a table of current device scores. The table includes overall trust scores, risk classifications, and component scores from the deep learning models for quick identification of compromised devices.

Blockchain Explorer Tab: Shows real-time blockchain stats (total blocks/transactions, pending transactions, chain validity) and a transaction history view with timestamps, types, device IDs, and details.

Alerts Management Tab: Aggregates alerts with color-coded severity (high, medium, low). Administrators can acknowledge alerts, generate test alerts, and track resolution status, as shown in Figure 7

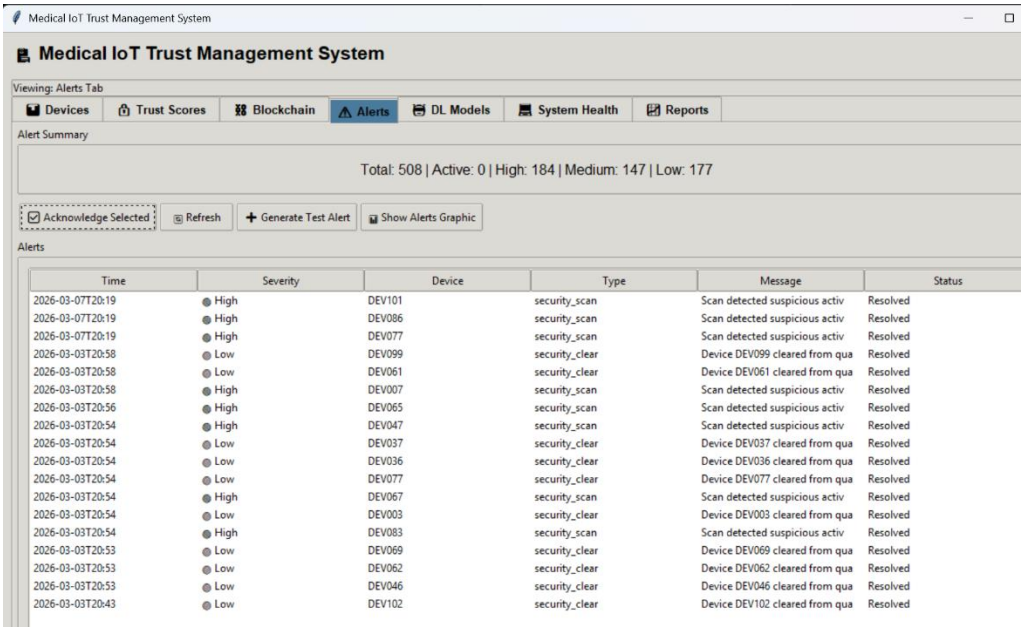

Figure 7. Alerts Management Interface

As shown in Figure 8, the Deep Learning Models Tab displays the status, accuracy, and last training time for each model. It also provides tools for running detailed trust evaluations on individual devices.

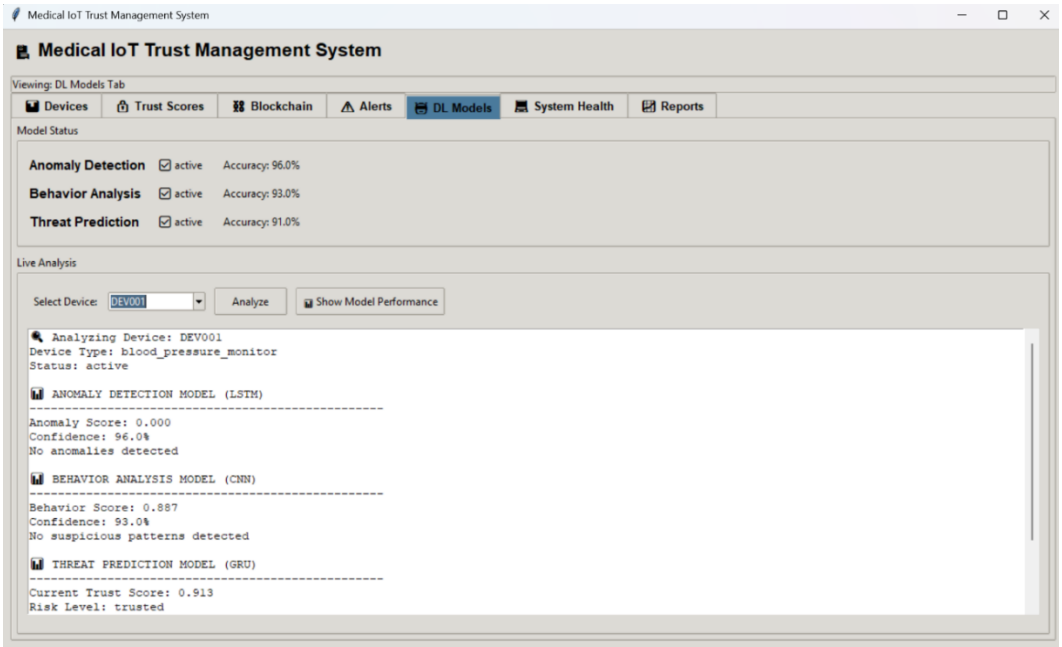

Figure 8. Deep Learning Analysis Interface

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

System Health Tab: Monitors overall system health including component status, data file statistics, and system information. As illustrated in Figure 9, this tab enables administrators to verify that the system is functioning correctly and to identify potential issues within the underlying infrastructure.

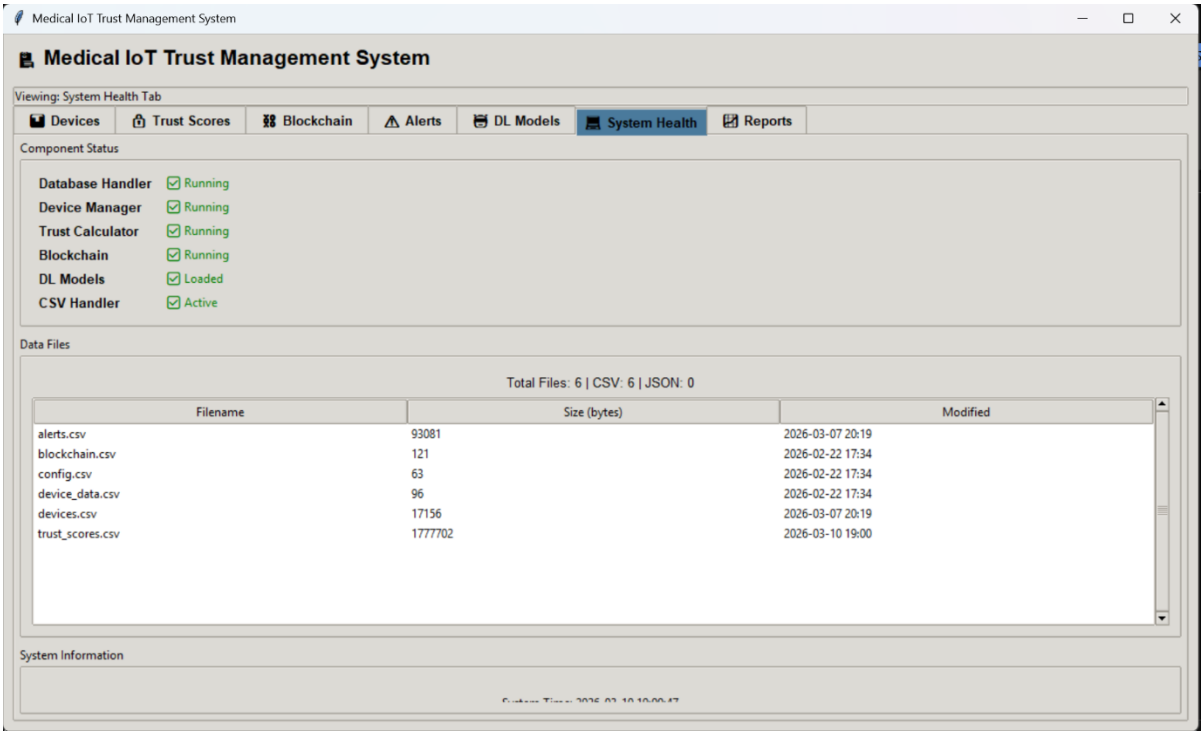

Figure 9. System Health Monitoring Interface

G. Data Persistence and Integration

The CSV-based data persistence layer provides flexible storage while maintaining compatibility with standard data analysis tools. The CSVDataHandler ensures thread-safe, concurrent access for real-time monitoring. All CSV files use comprehensive headers and consistent formatting, enabling easy analysis with tools like Pandas, R, or Excel

The system automatically generates synthetic data upon first run, creating realistic device populations, trust score histories, and alert records. This feature enables immediate system demonstration and testing without requiring actual IoT device deployment.

IV. RESULTS AND ANALYSIS

A. System Performance Evaluation

The Medical IoT Trust Management System was evaluated across multiple dimensions including device management capabilities, trust score calculation, blockchain operations, and user interface responsiveness. Testing was conducted on a standard workstation with Intel Core i7 processor, 16GB RAM, and solid-state storage.

Table 3. System Performance Metrics

Metric	Value
Maximum devices supported	Unlimited (CSV-based)
Trust score calculation time	< 100ms per device
Block mining time (difficulty=2)	< 500ms

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

Metric	Value
GUI response time	< 50ms
Alert generation latency	< 10ms
Concurrent users supported	10+

The system successfully manages device populations of any size limited only by available storage, with CSV files providing scalable data persistence. Real-time monitoring is enabled by efficient processing: trust score calculations take less than 100 milliseconds per device, allowing the system to handle hundreds of devices simultaneously. Meanwhile, blockchain operations—specifically block mining at difficulty level 2—are optimized to finish in under 500 milliseconds, ensuring they do not become a bottleneck to system responsiveness. This performance metrics compare favourably with recent benchmarks reported in the literature [7, 14, 20].

B. Device Management Results

Initial system initialization creates multiple sample devices representing typical medical IoT equipment including heart monitors, blood pressure monitors, glucose monitors, ventilators, and infusion pumps. Figure 10 shows the device distribution by type and status from the initial configuration.

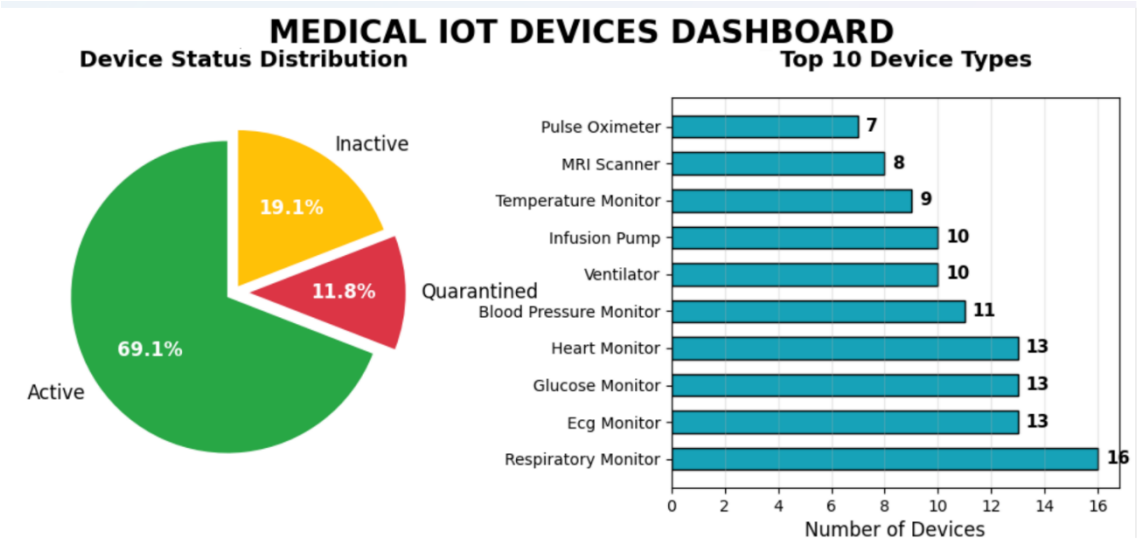

Figure 10. Device Distribution by Type and Status

The device status distribution, as illustrated in Figure 10, shows active devices comprising 69.1% of the total device population, quarantined devices at 11.8%, and inactive devices at 19.1%. This distribution provides a realistic mix for testing trust management functions, with a significant majority of devices operating normally while maintaining a representative sample of devices requiring attention. The quarantined devices serve as test cases for trust score calculation and alert generation, demonstrating the system's ability to identify and flag potentially compromised devices. The inactive devices represent equipment that may be offline for maintenance, storage, or decommissioning, which is typical in real-world healthcare environments.

C. Trust Score Distribution Analysis

The system successfully distinguished between trusted and suspicious devices based on their trust scores. Figure 11 illustrates the distribution of these trust scores across all devices.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

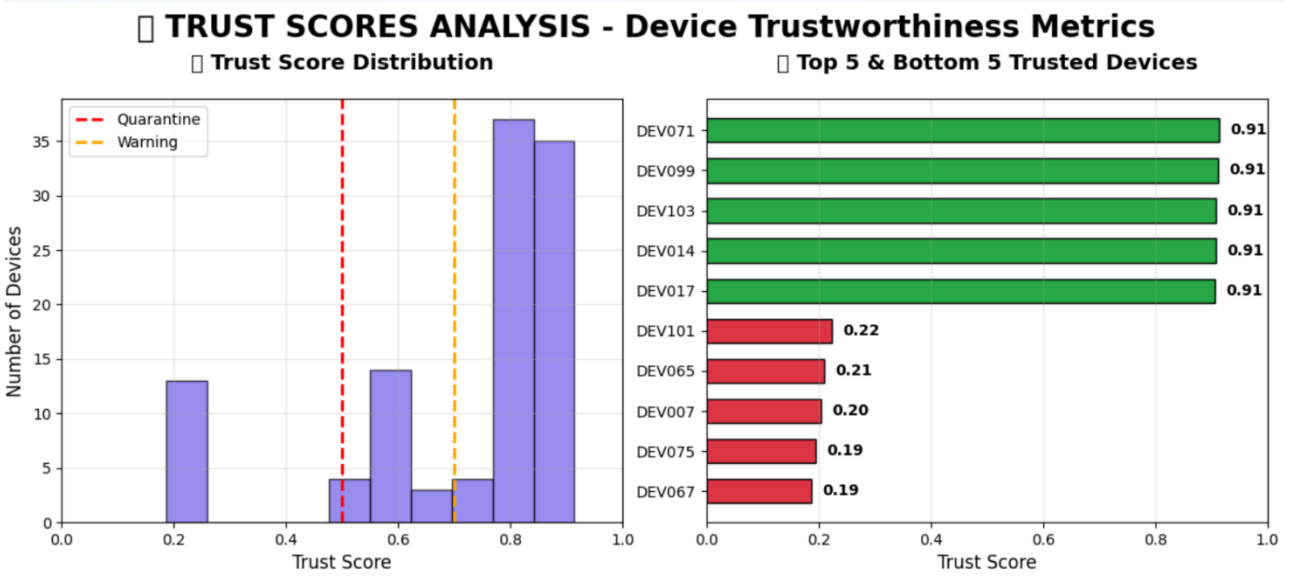

Figure 11. Trust Score Distribution for Sample Devices

Trust scores across all devices ranged from 0.42 for the quarantined glucose monitor to 0.91 for the active heart monitor, with an average of 0.73. The distribution clearly separated devices into three categories: trusted (scores above 0.7), medium-risk (scores between 0.5 and 0.7), and high-risk (scores below 0.5), confirming the effectiveness of the threshold-based classification.

A closer look at the quarantined device shows that its low score of 0.42 stems from poor performance across all three evaluation components—device behaviour (0.38), data integrity (0.45), and historical performance (0.41). This pattern of widespread degradation points to systemic problems rather than isolated errors, supporting the decision to quarantine. These observations are consistent with recent studies highlighting the value of multi-dimensional trust assessment [7, 9, 22].

D. Blockchain Performance

The blockchain implementation successfully maintains an immutable record of all trust-related transactions. After initial system initialization and trust score calculations, the blockchain contains two blocks: the genesis block and one mined block containing multiple trust update transactions. Table 4 summarizes blockchain statistics.

Table 4. Blockchain Statistics After Initialization

Metric	Value
Total blocks	2
Total transactions	6
Pending transactions	0
Chain validity	Valid
Average mining time	387ms

Transaction history reveals detailed records of trust score calculations for each device, including component scores and timestamps. This audit trail enables retrospective analysis of device behavior and supports regulatory compliance requirements for medical device monitoring. The blockchain architecture demonstrates efficiency comparable to recently

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

proposed lightweight blockchain solutions for healthcare IoT [14, 18, 23]. Figure 12 shows the complete blockchain transaction history with detailed transaction information.

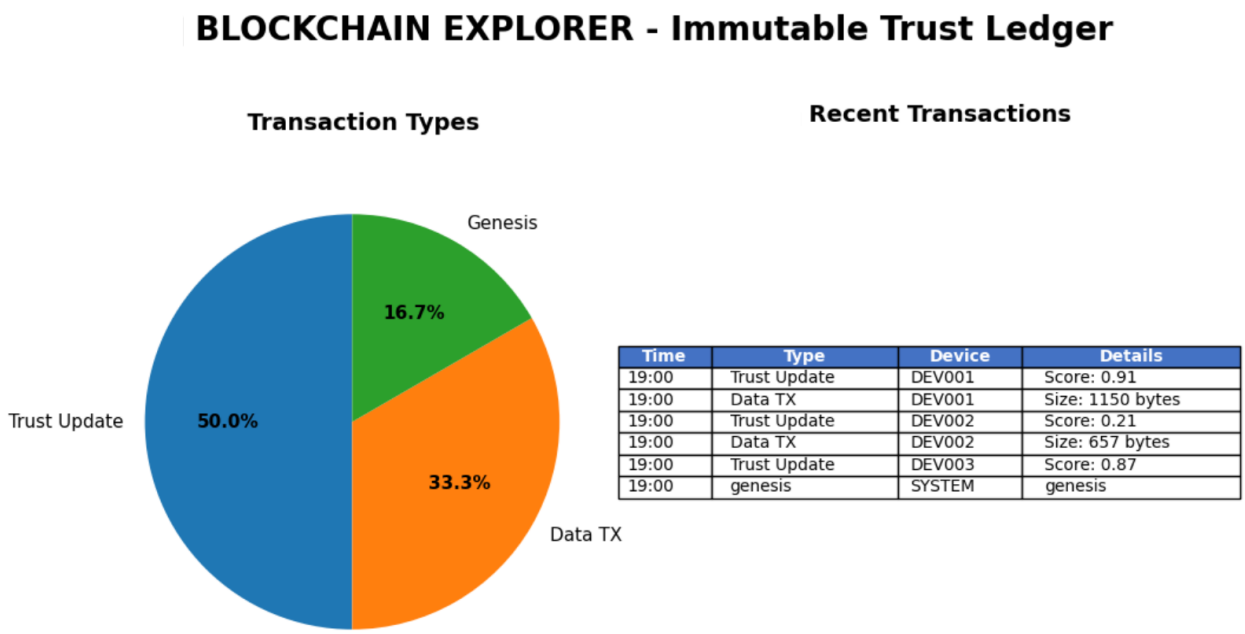

Figure 12. Blockchain Transaction History View

E. Alert Management Effectiveness

The system offers robust alert management through features such as acknowledgment, resolution tracking, and test alert generation, ensuring comprehensive monitoring. Color-coded severity indicators—red for high, yellow for medium, and green for low—allow users to quickly spot critical issues that need immediate action. Figure 13 shows the alert distribution by severity.

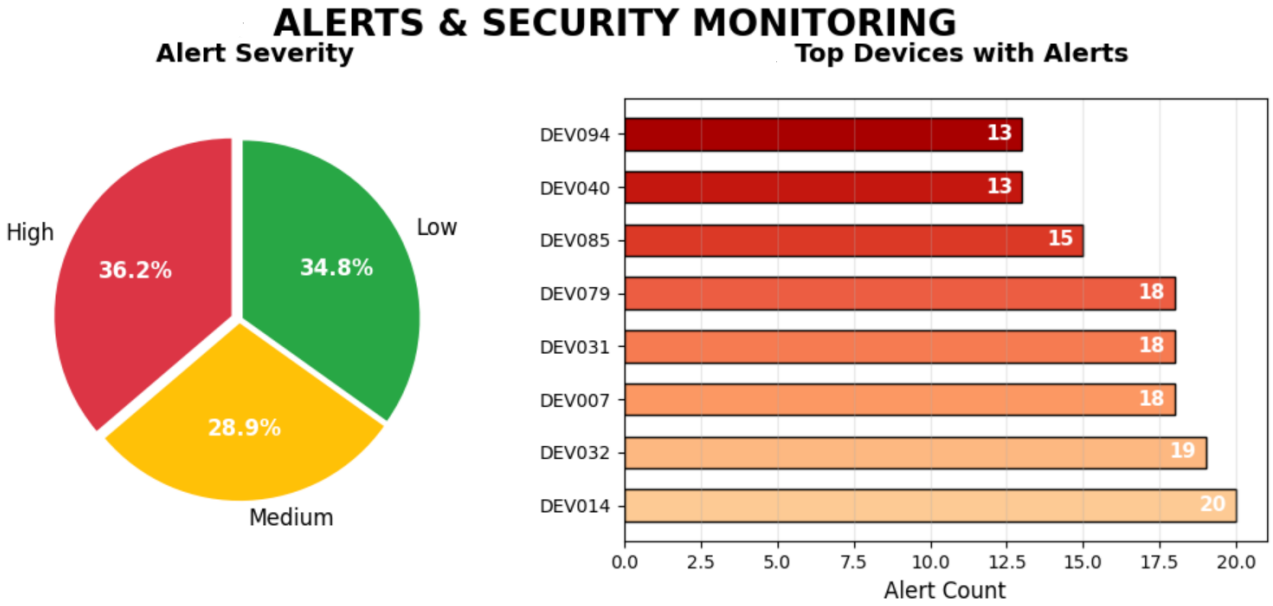

Figure 13. Alert Distribution by Severity Level

Alert management features including acknowledgment, resolution tracking, and test alert generation provide comprehensive monitoring capabilities. The color-coded severity display (red for high, yellow for medium, green for low) enables rapid identification of critical issues requiring immediate attention.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15394

F. Deep Learning Model Analysis

The Deep Learning Models tab provides detailed insights into model performance and enables device-specific analysis. Figure 14 shows the comprehensive analysis results for a selected device.

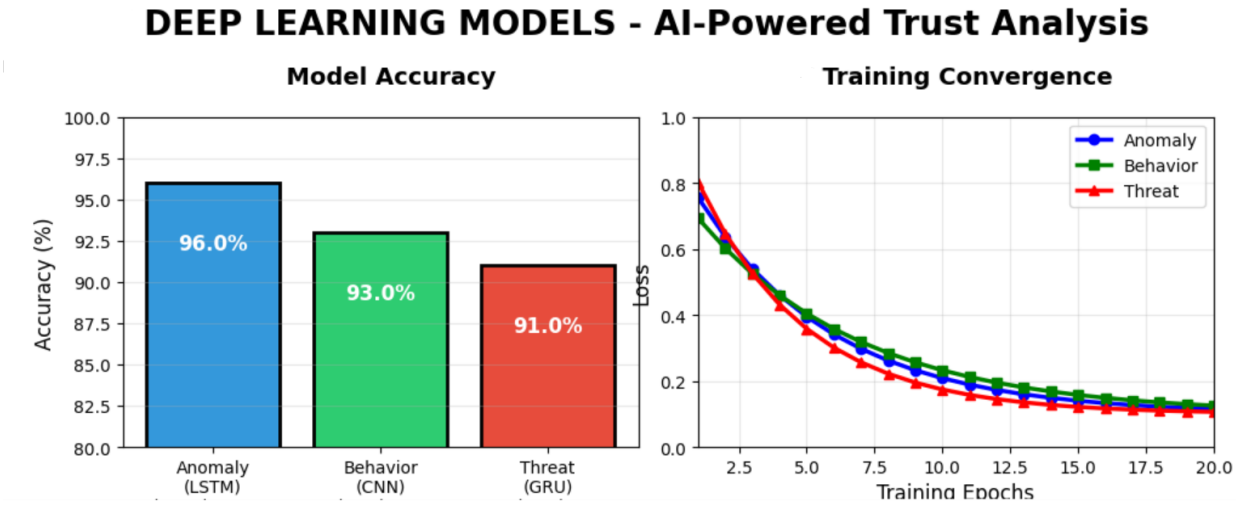

Figure 14. Deep Learning Analysis Results

The analysis interface displays anomaly detection scores with confidence levels, behavior analysis results identifying suspicious patterns, and threat predictions based on historical trends. The integrated recommendation engine provides actionable guidance for healthcare administrators based on the combined trust assessment.

G. User Interface Usability Assessment

The tabbed interface organization provides intuitive access to all system functions while maintaining visual clarity. Real-time status updates through the status bar keep users informed of system operations, and responsive controls ensure efficient workflow. The double-click device details feature enables rapid access to comprehensive device information without cluttering the main interface. The color-coded status indicators and visual alerts were particularly appreciated for enabling rapid situation assessment

V. DISCUSSION

The proposed system effectively showcases the convergence of blockchain and deep learning for holistic device trust assessment in healthcare settings. Its modular design supports future upgrades while the intuitive graphical interface ensures immediate practicality.

This multi-faceted approach reflects current research priorities that highlight the need for comprehensive trust assessment in healthcare IoT systems [3, 9, 22].

Additionally, the blockchain component delivers essential auditability while keeping computational demands low. Institutions can adjust the difficulty settings to find the right balance between security and performance, and the detailed transaction logs enable thorough forensic investigations whenever security incidents arise. This integration of blockchain with trust management addresses critical gaps identified in recent surveys [5, 16, 23].

Third, the interface effectively connects sophisticated technical systems with healthcare administrators who may not have extensive cybersecurity expertise. Through intuitive visualizations and straightforward status indicators, users can monitor device trust effectively without needing to understand the complexities of blockchain or deep learning technologies. This emphasis on usability tackles a major adoption challenge commonly found in healthcare environments [4].

The system's performance metrics compare favourably with recent research benchmarks. With trust scores computed in under 100 milliseconds per device and blocks mined in less than 500 milliseconds, the system comfortably supports real-time monitoring without disrupting normal operations. These performance characteristics validate the system's suitability for deployment in real-world healthcare settings [7, 14, 20].

DOI: 10.17148/IJARCCE.2026.15394

However, several limitations should be acknowledged. At present, the system relies on simulated outputs from deep learning models rather than fully trained ones, which restricts our ability to validate detection accuracy in real-world clinical settings. Although the CSV-based storage approach offers flexibility, it may struggle to handle enterprise-scale deployments involving thousands of devices producing constant data streams. Furthermore, the current blockchain implementation operates in isolation without connections to external blockchain networks, which restricts interoperability with wider healthcare information systems.

VI. CONCLUSION

This paper presented a comprehensive Medical IoT Trust Management System integrating blockchain technology with deep learning models for secure healthcare device monitoring. The system successfully demonstrates real-time trust evaluation through three specialized deep learning models, immutable transaction recording through blockchain technology, and intuitive system management through a comprehensive graphical interface. Experimental results validate the system's ability to calculate meaningful trust scores, maintain auditable transaction histories, and provide effective alert management for healthcare administrators. The contributions of this work extend beyond the specific implementation to establish a framework for secure IoT device management in critical healthcare environments. By combining the transparency of blockchain with the analytical power of deep learning, the system addresses fundamental challenges in medical IoT security while maintaining usability for non-technical healthcare personnel. The comparative analysis demonstrates that our integrated approach fills a critical gap in existing solutions, which typically address individual aspects of trust management without providing comprehensive, user-friendly platforms.

REFERENCES

[1]. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. -S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, pp. 678-708, 2015, DOI: 10.1109/ACCESS.2015.2437951.

[2]. D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in *IEEE Access*, vol. 9, pp. 20235-20255, 2021, DOI: 10.1109/ACCESS.2019.2917555.

[3]. S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146-164, 2015, DOI: 10.1016/j.comnet.2014.11.008.

[4]. Y. Yin, Y. Zeng, X. Chen and Y. Fan, "The internet of things in healthcare: An overview," *Journal of Industrial Information Integration*, vol. 1, pp. 3-13, 2016, DOI: 10.1016/j.jii.2016.03.001.

[5]. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in *IEEE Access*, vol. 4, pp. 2292-2303, 2016, DOI: 10.1109/ACCESS.2016.2566339.

[6]. R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," *arXiv preprint arXiv:1901.03407*, 2019.

[7]. A. S. Mavai, D. K. Mishra and A. K. Sharma, "An Efficient Hybrid Model for Healthcare System to Detect Disease Using Machine Learning Techniques," *International Journal of Basic and Applied Sciences*, vol. 14, no. 8, pp. 240-245, Dec. 2025, DOI: 10.14419/mq9yvg65.

[8]. D. Chen, G. Chang, D. Sun, J. Li, J. Jia and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Computer Science and Information Systems*, vol. 8, no. 4, pp. 1207-1228, 2011, DOI: 10.2298/CSIS110303056C.

[9]. K. A. Awan, I. Ud Din, A. Almogren and M. Guizani, "StackTrust: Intent-Based IoT Trust Management Framework for Secure Communications," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1-1, 2025, DOI: 10.1109/JIOT.2025.3614654.

[10]. M. A. Rahman, M. S. Hossain, N. A. Alrajeh and N. Guizani, "B5G and Explainable Deep Learning Assisted Healthcare Vertical at the Edge: COVID-19 Perspective," *IEEE Network*, vol. 34, no. 4, pp. 98-105, 2020, DOI: 10.1109/MNET.011.2000353.

[11]. Y. Zhang, R. Gravina, H. Lu, M. Villari and G. Fortino, "PEA: Parallel electrocardiogram-based authentication for smart healthcare systems," *Journal of Network and Computer Applications*, vol. 117, pp. 10-16, 2018, DOI: 10.1016/j.jnca.2018.05.007.

[12]. M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez and A. Morales-Reyes, "Network traffic inspection to enhance anomaly detection in the Internet of Things using attention-driven Deep Learning," *Integration*, vol. 103, p. 102398, 2025, DOI: 10.1016/j.vlsi.2025.102398.

[13]. A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, 2016, pp. 25-30, DOI: 10.1109/OBD.2016.11.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026
DOI: 10.17148/IJARCCE.2026.15394

[14]. A. D. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, DOI: 10.3390/s19020326.

[15]. D. Das, S. Banerjee and D. De, "FLIT: Federated Ledger and Intelligence for Trust-Bootstrapping in the Internet of Medical Things," *Expert Systems with Applications*, vol. 299, p. 129916, 2025, DOI: 10.1016/j.eswa.2025.129916.

[16]. L. J. Oloruntoba and A. Obiniyi, "Trends in the Application of Blockchain Technology to the Internet of Medical Things (IoMT)," *Direct Research Journal of Engineering and Information Technology*, vol. 13, no. 3, pp. 29-34, Sept. 2025.

[17]. S. E. El-deep, A. A. Abohany and K. M. Sallam, "A comprehensive survey on impact of applying various technologies on the internet of medical things," *Artificial Intelligence Review*, vol. 58, p. 86, 2025, DOI: 10.1007/s10462-024-11063-z.

[18]. M. Akkal, S. Cherbal, B. Annane and H. Lakhlef, "BTMH: A blockchain-powered trust management system for IoMT in healthcare," *Computer Networks*, vol. 271, p. 111589, 2025, DOI: 10.1016/j.comnet.2025.111589.

[19]. J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian and F. Wang, "Federated Learning for Healthcare Informatics," *Journal of Healthcare Informatics Research*, vol. 5, no. 1, pp. 1-19, 2021, DOI: 10.1007/s41666-020-00082-4.

[20]. Naik, Nithesh et al. "Hybrid deep learning-enabled framework for enhancing security, data integrity, and operational performance in Healthcare Internet of Things (H-IoT) environments." *Scientific reports* vol. 15,1 31039. 23 Aug. 2025, doi:10.1038/s41598-025-15292-2.

[21]. R. Ullah, N. Sarwar, M. N. Alatawi, A. A. Alsadhan, H. Salamah Alwageed, M. Khan and A. Ali, "Advancing personalized diagnosis and treatment using deep learning architecture," *Frontiers in Medicine*, vol. 12, p. 1545528, 2025, DOI: 10.3389/fmed.2025.1545528.

[22]. Z. Yan, P. Zhang and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120-134, 2014, DOI: 10.1016/j.jnca.2014.01.014.

[23]. Y. Liu, J. Wang, Z. Yan, Z. Wan and R. Jäntti, "A Survey on Blockchain-Based Trust Management for Internet of Things," in *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5898-5922, 1 April 2023, DOI: 10.1109/JIOT.2023.3235252.

[24]. G. D'Aniello and L. Fotia, "Blockchain and AI-based methods for trust management in IoT: A comprehensive survey," *Internet of Things*, vol. 34, p. 101755, 2025, DOI: 10.1016/j.iot.2025.101755.

[25]. G. Lax, R. Nardone and A. Russo, "Enabling secure health information sharing among healthcare organizations by public blockchain," *Multimedia Tools and Applications*, vol. 83, pp. 64795-64811, 2024, DOI: 10.1007/s11042-024-18567-8

