Healthcare 4.0: A Large Language Model-Based Blockchain Framework for Medical Device Fault Detection and Diagnostics

Khalid Alsaif*, Aiiad Albeshri, Maher Khemakhem, Fathy Eassa
Department of Computer Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia

***Abstract*—This paper introduces a novel framework integrating Large Language Models (LLMs) with blockchain technology for medical device fault detection and diagnostics in Healthcare 4.0 environments. The proposed framework addresses key challenges, including real-time fault detection, data security, and automated diagnostics through a multi-layered architecture incorporating Internet of Things (IoT) integration, blockchain-based security, and LLM-driven diagnostics. Experimental evaluations demonstrate substantial improvements in diagnostic accuracy and response time while maintaining stringent security standards and regulatory compliance. The system provides enhanced fault detection with real-time monitoring capabilities and secure maintenance record management for smart healthcare. Comparative analysis of different LLMs and traditional Machine Learning (ML) methods shows that Deepseek-R1:7b achieved 97.6% classification accuracy, while O3-mini reached 90.4% and 91.2% in diagnosis accuracy and problem identification, respectively. Claude demonstrated the highest technical accuracy (98.4%), while Traditional ML excelled in processing time (11.7) and processing rate (10.68). Deepseek-R1:7b's offline capabilities ensure stringent security, privacy, and confidentiality with restricted connectivity, making it particularly suitable for sensitive healthcare applications where data protection is paramount.**

***Keywords*—Healthcare 4.0; Large Language Models; blockchain technology; medical device diagnostics; fault detection; smart healthcare; IoT healthcare security; machine learning**

I. Introduction

The rapid advancement of healthcare technology has introduced Healthcare 4.0, an era defined by intelligent systems, interconnected medical devices, and data-driven decision-making. Medical devices play a critical role in this transformation, providing essential monitoring and treatment capabilities to enhance patient care. However, ensuring the reliability and safety of these devices remains a major concern, as device malfunctions can pose serious risks to patient health.

Recent developments in Internet of Things (IoT) technology have facilitated continuous monitoring of medical devices, generating vast volumes of operational data. While this data holds significant potential for fault detection and diagnostics, conventional monitoring systems often fail to deliver real-time, accurate diagnostics while maintaining data security and privacy compliance. The healthcare sector faces critical challenges in device maintenance, fault detection, and secure performance record management.

*Corresponding author.

Large Language Models (LLMs) [1] have recently emerged as powerful tools for complex pattern recognition and predictive analysis, introducing new opportunities for intelligent fault diagnostics. Meanwhile, blockchain technology provides an immutable, secure, and tamper-resistant data management system. However, the synergistic integration of LLMs and blockchain technology for medical device fault diagnostics remains largely unexplored.

In this research, we aim to address the following research questions:

- How can Large Language Models and blockchain technology be integrated to improve the accuracy of medical device fault diagnosis?
- Which models are most effective for diagnosing different types of medical device faults?
- How does blockchain integration affect the performance and security of the fault diagnosis system?
- What are the appropriate metrics for evaluating the effectiveness of a fault diagnosis system in the context of Healthcare 4.0?

These questions are particularly significant given the increasing complexity of medical devices, the critical nature of healthcare applications, and the stringent regulatory requirements governing healthcare data security and patient safety.

This paper proposes an innovative framework that leverages the analytical power of LLMs and the security features of blockchain technology to enhance medical device fault diagnostics. To address the first research question on LLM-blockchain integration, we develop a multi-layered architecture that enables secure data flow between IoT devices, blockchain networks, and LLM processing engines. For the second question on model effectiveness, we evaluate multiple LLM variants and traditional ML approaches across diverse fault scenarios. The third question regarding blockchain's impact is examined through comparative performance analysis with and without blockchain integration. Finally, we establish comprehensive evaluation metrics to address the fourth research question, measuring both technical performance and healthcare-specific requirements.

The key contributions of this study include:

1) IoT-Blockchain-LLM integration: A novel framework that combines real-time IoT monitoring, blockchain security, and LLM intelligence to ensure data immutability, fault detection accuracy, and optimal response times.

2) Real-time processing framework: A highly efficient processing system that demonstrates minimal blockchain overhead across diverse medical devices, validated through experiments on ECG monitors, insulin pumps, and defibrillators.

3) Enhanced security and traceability: A blockchain-based system that preserves fault history, provides immutable record-keeping, and ensures regulatory compliance while handling various fault types through comprehensive diagnostic tracking.

4) Intelligent fault diagnostics: The integration of LLMs enables detailed fault analysis, providing actionable insights for proactive maintenance in healthcare settings.

5) Healthcare-specific implementation: A practical, scalable solution designed to meet healthcare industry standards, ensuring regulatory compliance, performance optimization, and secure handling of diverse medical devices.

The remainder of this paper is structured as follows: Section II presents a comprehensive review of related work. Section III details the proposed framework architecture and its key components. Section IV describes the implementation and experimental setup and discusses the results and findings. Section V concludes the study and outlines future research directions.

II. Literature Review

The rapid evolution of Healthcare 4.0 integrates IoT, AI, and blockchain technology, revolutionizing medical device management and fault diagnostics. Recent studies highlight the role of IoT-based monitoring in enhancing real-time device performance tracking, while blockchain ensures data integrity and security compliance. Additionally, Large Language Models (LLMs) have emerged as powerful tools for fault detection and predictive diagnostics, offering intelligent analysis and decision-making capabilities. However, existing research lacks a comprehensive framework that combines these technologies for secure, real-time, and automated medical device fault detection. This study addresses this gap by proposing an LLM-enhanced blockchain framework that ensures accurate diagnostics, data security, and regulatory compliance within Healthcare 4.0 environments.

A. Healthcare 4.0 and Medical Device Management

Healthcare 4.0 integrates IoT, blockchain, artificial intelligence (AI), and additive manufacturing to revolutionize medical device management. Mrugalska et al. [2] demonstrated the application of open-source systems in dental engineering, while Karmakar et al. [3] introduced ChainSure, a blockchain-based insurance system for healthcare applications. In medical device logistics, Tu et al. [4] proposed a weighted density-based clustering model to optimize logistics operations. This work was complemented by Abusohyon et al. [5], who developed a fog network-based biosensor system to enhance real-time health monitoring. Additionally, Landolfi et al. [6] introduced digital twins for medical device value chain management, demonstrating their role in enhancing operational efficiency.

Cybersecurity in Healthcare 4.0 has also seen notable advancements. Gupta et al. [7] proposed a B2B healthcare security framework, which enhances data security and privacy protection in healthcare information management systems. Additionally, Szczepaniuk and Szczepaniuk [8] explored smart contract innovations that enhance secure medical transactions and healthcare compliance. The integration of AI and IoT in healthcare has enabled significant diagnostic improvements. Verma et al. [9] demonstrated the FCMCPS-COVID system, achieving a 98.8% diagnostic accuracy for COVID-19 detection using AI-powered IoT frameworks. To address privacy concerns, Rani et al. [10] introduced federated learning models tailored for Internet of Medical Things (IoMT) applications, which ensure secure patient data management. Similarly, Salim et al. [11] proposed a hybrid federated blockchain system to enhance data privacy and security in smart healthcare environments. For real-time patient monitoring, Mao et al. [12] developed triboelectric sensors integrated with deep learning models, improving wearable medical device performance. Additionally, Soffer et al. [13] identified adoption barriers in implementing Healthcare 4.0 solutions, emphasizing challenges related to technological integration and user acceptance. Meanwhile, Aranyossy and Halmosi [14] examined regulatory compliance challenges, highlighting the need for robust governance frameworks in Healthcare 4.0 adoption.

B. Fault Detection and Diagnostics in Medical Devices

The field of medical device fault diagnostics has progressed from basic monitoring systems to advanced machine learning-based approaches. Anandhalekshmi et al. [15] contributed to this evolution by developing a hybrid diagnostic model, integrating the Baum-Welch algorithm with Support Vector Machine (SVM) to enhance sensor fault detection in healthcare monitoring systems.

Building on this foundation, Arfaoui et al. [16] introduced an innovative game-theoretic anomaly detection technique tailored for Wireless Body Area Networks (WBANs), improving fault detection efficiency in wearable medical devices.

More recently, Putra et al. [17] advanced the field by integrating federated learning with blockchain technology to develop a secure, decentralized fault detection system for IoT-based medical environments. Their study demonstrated notable improvements in diagnostic accuracy while reducing processing times, marking a significant breakthrough in real-time medical device diagnostics.

Alsaif et al. [18] introduced an LLM-based framework for fault detection in Industry 4.0, leveraging the Generative Pre-trained Transformer-4-Preview model, which inspires our application to healthcare, adapting its concepts for medical device diagnostics.

C. Integration of AI with Traditional Methods

The integration of AI with traditional fault detection techniques has further enhanced diagnostic accuracy. Fang et al. [19] combined Simulated Annealing (SA) with Adaptive Neuro-Fuzzy Inference Systems (ANFIS) to develop a robust fault detection framework. Similarly, Dash et al. [20] incorporated Self-Supervised Learning (SSL) with Bond Graph models, enhancing predictive fault detection capabilities. To improve fault isolation techniques, Han et al. [21] proposed a Dynamic Uncertain Causality Graph (DUCG)-based model, significantly enhancing fault classification accuracy. Al Shehri

et al. [22] developed a deep learning approach using convolutional neural networks and Darknet for COVID-19 detection from CT scans and X-ray images, achieving high accuracy, highlighting AI's role in diagnostics, which our study extends to device fault detection using LLMs. In industry-specific applications, Lv et al. [23] categorized fault detection and diagnosis (FDD) techniques for marine diesel engines, providing a systematic approach to engine fault analysis. Meanwhile, Montes-Romero et al. [24] achieved over 90% accuracy in photovoltaic system fault diagnostics, demonstrating the effectiveness of machine learning models in renewable energy applications.

The emergence of advanced architecture has further enhanced fault detection performance. Li et al. [25] introduced the Deep Expert Network, an interpretable AI model for transparent diagnostics, improving explainability in automated fault detection systems. Additionally, Zhao et al. [26] combined Multiscale Temporal Features (MTF) with Convolutional Neural Networks (CNNs), achieving a 93.75% accuracy rate in medical device fault detection. For real-time fault detection, Zhao et al. [27] developed an edge computing-based diagnostic system, reducing fault detection latency to 8 milliseconds, ensuring high-speed fault identification in time-sensitive healthcare applications. Similarly, Tang et al. [28] achieved 99.78% accuracy in real-time monitoring systems, demonstrating the potential of AI-driven fault prediction models in healthcare environments. Benchmarking studies have also contributed significantly to fault detection research. Bacha et al. [29] released a comprehensive Permanent Magnet Synchronous Motor (PMSM) fault dataset, providing a standardized evaluation framework for fault detection algorithms. Moreover, the dataset has supported Balachandran et al. [30] research on automated fault diagnostics, emphasizing the role of AI-driven methodologies in enhancing predictive maintenance systems.

D. Blockchain and IoT Technology in Healthcare

The integration of blockchain and Internet of Things (IoT) technology in healthcare presents innovative solutions to address data security, privacy, and system scalability challenges. Kanwal et al. [31] proposed a chaos-based encryption system combined with blockchain technology to enhance medical image security, ensuring tamper-resistant storage and transmission. Meanwhile, Guerar et al. [32] introduced a Self-Sovereign Identity (SSI)-based system designed to prevent fraud and maintain cross-border interoperability, facilitating secure patient identity management across healthcare networks. Almalki et al. [33] proposed a prototype model integrating blockchain with IoMT devices, demonstrating its potential for secure healthcare data management by collecting IoMT data over edge computing gateways and broadcasting it across peer nodes using smart contracts, which supports our framework's use for fault history integrity.

For distributed healthcare architectures, Wang et al. [34] integrated blockchain with edge computing, enhancing secure health data management and reducing latency in decentralized healthcare systems. Additionally, Liu et al. [35] developed a blockchain-based incentive mechanism to promote data sharing and security within smart healthcare environments. Additionally, Liu et al. [36] developed a blockchain-based incentive mechanism to promote data sharing and security within smart healthcare environments. Similarly, Li et al. [37] focused on enhancing interoperability, leveraging blockchain technology to improve data exchange efficiency among heterogeneous healthcare systems.

Beyond patient data security, blockchain plays a critical role in healthcare supply chain management. Yadav et al. [38] examined the adoption barriers to blockchain-based vaccine distribution, identifying challenges in scalability, regulatory compliance, and stakeholder adoption. Moreover, Mangala et al. [39] proposed an IoT-integrated blockchain model to ensure pharmaceutical tracking transparency, mitigating the risks of counterfeit drugs in global supply chains. Emerging trends in blockchain technology also highlight security enhancements. Liu et al. [40] introduced quantum-resistant frameworks, addressing potential post-quantum cybersecurity threats in medical data protection. Additionally, Mershad [41] developed lightweight blockchain architectures optimized for resource-constrained IoT medical devices, reducing computational overhead while maintaining data security.

E. Large Language Models for Fault Detection

The application of Large Language Models (LLMs) in healthcare fault diagnostics represents an emerging area of research. While LLMs have yet to be fully implemented in medical device fault detection, advancements in related fields highlight their potential applications. Kumar et al. [42] laid the foundational work in this domain by developing an ensemble learning framework. Although their study did not specifically involve LLMs, it demonstrated the capabilities of advanced AI models in healthcare security and fault diagnostics.

Recent developments indicate LLMs' adaptability for fault detection and diagnosis across various industrial sectors. Zheng et al. [43] demonstrated that fine-tuned LLMs can achieve high diagnostic accuracy, particularly when employing data normalization techniques and handling missing values efficiently. In intelligent manufacturing, Zhang et al. [44] highlighted the role of LLMs in enhancing human-machine collaboration and improving service-level fault detection capabilities. Similarly, Mustapha [45] explored domain-specific LLMs, showing their ability to detect subtle fault signatures in mechanical systems, paving the way for highly specialized diagnostic models.

Beyond fault diagnostics, researchers are investigating the broader implications of LLMs in AI-driven healthcare advancements. Liu et al. [46] conducted a comprehensive survey on ChatGPT-related advances, analyzing pre-training methodologies and instruction fine-tuning techniques to enhance LLM adaptability. Meanwhile, Singh et al. [47] developed a strategic roadmap for generative AI applications, employing text-mining techniques and structural topic modeling to optimize LLM-based knowledge extraction in medical fault analysis.

F. Research Gaps

Based on the comprehensive review of existing literature, several gaps have been identified in current research. Table I presents a comparative analysis of existing solutions versus our proposed framework.

A thorough analysis of existing literature has revealed multiple research gaps in medical device fault diagnostics, particularly in areas such as real-time fault detection, blockchain

TABLE I. COMPARATIVE ANALYSIS OF FEATURES IN HEALTHCARE DEVICE FAULT DIAGNOSTICS

Features/Capabilities	[15]	[16]	[48]	[17]	[43]	Proposed Framework
Real-time Fault Detection	✓	✓	✓	✓	✓	✓
Blockchain Security	×	✓	✓	✓	×	✓
LLM Utilization	×	×	×	×	✓	✓
Automated Diagnostics	✓	✓	✓	✓	✓	✓
Data Privacy	×	×	✓	✓	✓	✓
IoT	✓	✓	×	✓	×	✓

security, AI-driven automation, and IoT integration. While previous studies have made strides in specific aspects of fault diagnostics, critical limitations remain in ensuring data security, scalability, interoperability, and advanced AI-driven fault detection methods.

One of the primary gaps identified is the lack of Large Language Model (LLM) utilization for fault diagnostics. Existing approaches primarily rely on traditional machine learning algorithms without leveraging LLMs for contextual data analysis and predictive diagnostics. As seen in Table II, none of the referenced studies except the proposed framework have integrated LLMs for enhanced fault detection and decision-making. The proposed framework fills this gap by incorporating LLM-based intelligence and improving anomaly detection, fault prediction, and adaptive learning capabilities.

Another key gap is blockchain security in fault diagnostics. While studies [17] and [43] incorporate blockchain technology, others lack secure, decentralized data management mechanisms. Without blockchain, fault detection logs remain vulnerable to tampering, compromising data integrity and compliance with healthcare regulations. The proposed framework ensures end-to-end security through blockchain-based immutable logs, decentralized verification, and automated compliance auditing.

Additionally, real-time fault detection mechanisms are not consistently integrated across existing models. Studies [15], [16], and [48] provide real-time monitoring, but studies [17] and [43] do not emphasize real-time data processing and fault resolution. The proposed framework addresses this limitation by leveraging IoT-enabled real-time monitoring, ensuring faults are detected and mitigated instantly with minimal latency.

Furthermore, current frameworks lack full IoT integration, limiting their ability to aggregate, analyze, and process real-time data from multiple medical devices. As shown in Table I, none of the referenced studies have effectively integrated IoT-based fault detection, leading to gaps in real-time device communication and predictive maintenance. The proposed framework fully integrates IoT with AI and blockchain, enabling seamless connectivity and automated diagnostics across healthcare infrastructures.

Finally, data privacy and compliance mechanisms remain insufficiently addressed. While some studies implement basic privacy protocols, they do not fully incorporate federated learning for secure AI model training or blockchain for compliance tracking. The proposed framework strengthens privacy protection by utilizing federated learning, ensuring secure AI training across multiple healthcare institutions without sharing sensitive patient/device data.

III. METHODOLOGY

Our methodology presents an innovative approach to Healthcare 4.0 by seamlessly integrating three core Industry 4.0 technologies—Artificial Intelligence, Blockchain, and the Internet of Things (IoT). The framework leverages Large Language Models as the AI component to provide sophisticated pattern recognition and automated diagnostic capabilities for medical device fault detection. IoT technology enables comprehensive real-time monitoring and data collection from medical devices through sensors and edge computing nodes, ensuring continuous device health assessment. Blockchain technology is the foundation for secure data management, providing immutable record-keeping and ensuring the integrity of diagnostic results while maintaining health authority compliance. These three technologies work in concert within our six-layer architecture: IoT handles data acquisition and device monitoring, AI processes and analyses the collected data for fault detection, and blockchain secures and validates all system operations. This integrated approach creates a robust, secure, and intelligent framework that addresses the complex requirements of modern healthcare environments while enabling automated, reliable, and traceable medical device diagnostics.

A. Framework Overview

The Healthcare 4.0 Fault Diagnosis Framework, as illustrated in Fig. 1, provides a comprehensive solution for medical device monitoring and fault detection through a six-layer interconnected architecture. Each layer plays a distinct yet integrated role, ensuring intelligent diagnostics, real-time monitoring, data security, and seamless interoperability.

The Data Source Layer serves as the foundation of the framework, comprising two key components. The Data Collection component aggregates information from diverse sources, including academic journals, social media platforms, and authoritative healthcare organizations. Simultaneously, the Data Acquisition component interfaces directly with medical devices, raw sensors, and Electronic Health Records (EHR) systems, ensuring real-time operational data retrieval for fault detection and analysis.

At the core of the framework, the Intelligence Layer is responsible for advanced analytical processing. This layer integrates a knowledge base to store domain expertise, decision-making capabilities to generate actionable insights, and a diagnostic system to identify faults. Additionally, Generative AI techniques enhance pattern recognition and predictive analytics, allowing for early fault detection and anomaly prediction. This layer works closely with the Data Storage Layer, which combines cloud-based and on-premise storage solutions to ensure scalability, data redundancy, and secure access to diagnostic information.

The Security Layer provides comprehensive protection through three key mechanisms. Blockchain technology ensures immutable record-keeping, maintaining transparent, tamper-proof logs of system activities and device states. Access control mechanisms regulate user permissions based on roles and authorization levels, preventing unauthorized access to sensitive data. Additionally, data encryption safeguards all system interactions, securing device readings, diagnostic results, and patient records against potential cyber threats.

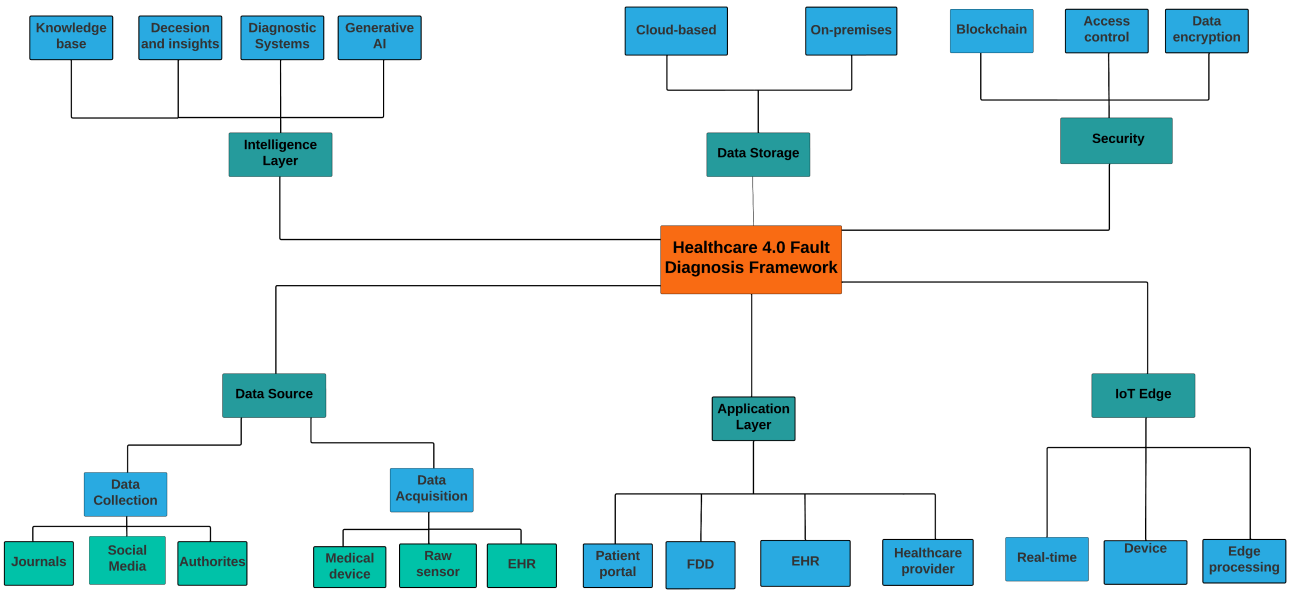


Fig. 1. Healthcare 4.0 fault diagnosis framework layers.

The IoT Edge Layer manages the critical interface between physical medical devices and the digital diagnostic framework. This layer facilitates real-time data processing, efficient device communication, and seamless integration with the broader system. It incorporates device management capabilities, supports low-latency fault detection, and enables edge computing functionalities, ensuring that critical diagnostic operations are performed with minimal delay.

The Application Layer serves as the central interface for all healthcare stakeholders. It enables healthcare providers to access comprehensive device insights and patient data through an interactive patient portal. Additionally, the Fault Detection and Diagnosis (FDD) module delivers detailed diagnostic insights, enhancing medical decision-making. EHR system integration ensures synchronized patient care coordination, bridging the gap between fault diagnostics and clinical workflows.

The modular and hierarchical architecture of the framework allows each layer to function independently while ensuring seamless interoperability across components. This design approach enhances scalability, security, and operational efficiency, making the framework highly adaptable for future advancements in medical device fault diagnostics and Healthcare 4.0 solutions.

B. System Architecture

The system architecture, illustrated in Fig. 2, is designed to support medical device fault diagnostics by integrating six key interconnected components: Data Acquisition, IoT, Blockchain, Data Storage, Intelligence, and Applications. This multi-layered architecture ensures scalability, security, and real-time processing, allowing seamless collaboration between healthcare providers, diagnostic systems, and medical devices.

The Data Acquisition component forms the foundation, incorporating two main streams: device-based inputs and knowledge-based inputs. The device stream includes data from technicians through medical devices, patients through wearable devices, and Electronic Health Records (EHR). The knowledge stream integrates academic and research knowledge through established databases like Scopus, IEEE, and other authoritative sources, enriching the knowledge base for diagnostic analysis.

The IoT layer processes incoming data through an IoT Core component that standardizes and preprocesses data from various sources before transmission. This connects to the Blockchain component, which implements distributed ledger technology through multiple nodes to ensure data integrity and secure transmission throughout the system.

The Data Storing layer comprises three key elements: Cloud-DB for structured operational data, a specialized Knowledge Base system that supports the LLM processing, and a secondary Cloud-DB for backup and redundancy. This robust storage architecture ensures data availability and reliability while maintaining system performance.

The Intelligence layer features dual LLM implementations: a Maintenance Support System LLM for technical diagnostics and a Medical LLM for clinical insights. This dual-LLM approach enables sophisticated pattern recognition and diagnostic analysis across technical and medical domains.

The Applications layer provides comprehensive functionality through FDD (Fault Detection and Diagnosis) for identifying and analyzing device issues, MDS (Medical Diagnosis System) for clinical decision support, Text Generation for automated reporting and documentation, and EHR integration for comprehensive patient record management.

The entire system is accessible to stakeholders through web and mobile applications, ensuring healthcare practitioners, device technicians, and patients can access critical information and diagnostics through multiple interfaces. This multi-modal access approach enhances system usability while maintaining

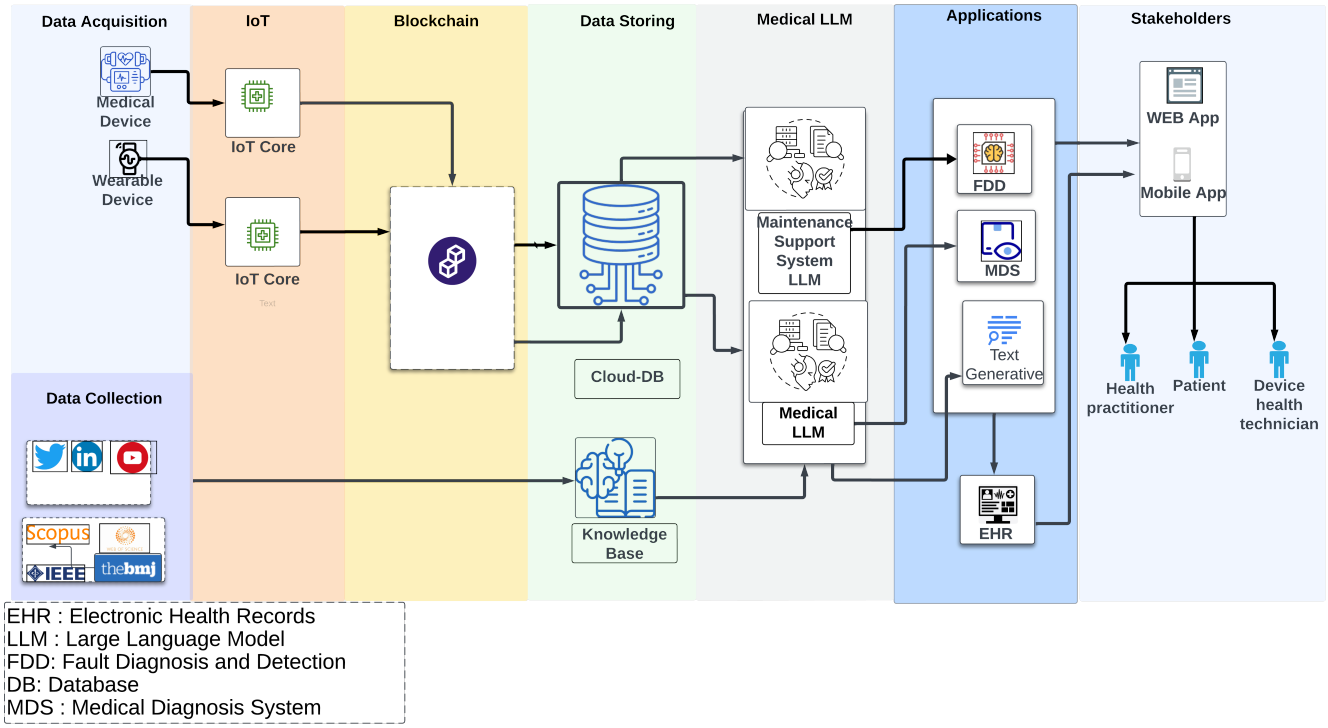


Fig. 2. System architecture for healthcare 4.0 medical device fault diagnostics framework.

security through appropriate access controls and authentication mechanisms.

The proposed architecture emphasizes scalability, security, and integration capabilities, ensuring the system can adapt to evolving healthcare technology needs while maintaining robust fault diagnostic capabilities. The combination of blockchain security, LLM intelligence, and comprehensive data management creates a powerful platform for advancing medical device maintenance and healthcare delivery.

In the Data Layer, we implement AWS IoT Core simulation to systematically collect and classify fault data according to the classification system defined in Table II. The simulation framework generates device fault scenarios at 5-second intervals across medical devices, replicating the four fault categories - power system (E101), sensor system (E102), thermal management (E103), and communication (E104). Each fault type is generated according to its specified criticality level in Table II, with critical faults (E101 and E103) receiving prioritized handling over high-priority faults (E102 and E104). Virtual devices, including ECG monitors, insulin pumps, defibrillators, and thermometers, transmit standardized fault messages via MQTT protocol, maintaining the fault distribution patterns and criticality.

TABLE II. MEDICAL DEVICE FAULT CLASSIFICATION SYSTEM

Fault Code	Category	Description	Criticality Level
E101	Power System	Battery failure	Critical
E102	Sensor System	Sensor malfunction	High
E103	Thermal Management	Overheating	Critical
E104	Communication	Data transmission errors	High

C. Core Blockchain Architecture

The blockchain architecture employs a hierarchical block structure incorporating four essential components, as shown in Fig. 3: block indexing, temporal stamping, diagnostic data payload, and cryptographic hash values. Each block maintains a secure link to its predecessor through SHA-256 hash functions, ensuring data immutability and chain integrity while maintaining health authority compliance requirements.

[{"index": 0, "timestamp": 1720905190.9940019, "data": "Genesis Block", "previous_hash": "0", "hash": "13140a7eb4be9268995e96b4dab52bb54bcda61c6bc8cf650e1475b20f59c05c"}]

Fig. 3. Block structure.

The security architecture implements a multi-layered approach utilizing AWS IoT Core's security features. The system employs as shown in Table III:

TABLE III. SECURITY IMPLEMENTATION METRICS

Security Feature	Implementation Method
Authentication	TLS Certificates
Data Encryption	AES-256
Access Control	Role-Based
Message Integrity	SHA-256

This comprehensive implementation demonstrates the framework's capability to handle diverse fault scenarios across

multiple medical devices while maintaining strict security protocols and real-time performance requirements. The system's ability to process and record faults with sub-millisecond latency while maintaining 100% message delivery reliability makes it suitable for critical healthcare environments. The balanced distribution of fault detection across different device types and fault categories indicates robust monitoring capabilities, which are essential for maintaining patient safety and device reliability in healthcare settings.

D. IoT Integration

The IoT integration methodology in our Healthcare 4.0 framework establishes a systematic approach to medical device monitoring and fault detection. This methodology focuses on creating a reliable, secure, and scalable foundation for real-time device data collection and analysis.

Our framework implements a three-tiered hierarchical communication protocol utilizing MQTT over TLS 1.2 for secure medical device interactions. The device layer establishes standardized data packets containing all medical equipment's fault codes, operational metrics, and status information. These packets follow a unified format for consistent monitoring and analysis. The intermediate layer employs edge nodes for data aggregation and optimization, implementing dynamic transmission frequencies based on device criticality and operational status. At the core system layer, a routing algorithm manages communication flow, ensuring immediate transmission of critical faults while optimizing routine monitoring data through standard channels.

The data collection methodology incorporates an IoT sensor simulation system replicating real-world medical device fault scenarios. The simulation environment generates four primary fault types across critical medical devices: battery failures (E101), sensor malfunctions (E102), thermal issues (E103), and communication errors (E104). Each device generates fault data at consistent 5-second intervals, providing real-time monitoring capabilities.

Our testing environment processes approximately 720 fault messages per hour per device, with each message containing detailed fault parameters, including device type, fault code, timestamp, and fault description. The system implements AWS IoT Core for message handling, utilizing MQTT protocols for reliable data transmission. This approach ensures consistent data collection while maintaining the ability to simulate concurrent fault scenarios across multiple devices, providing a robust testing environment for our diagnostic framework.

E. LLM Utilization

Our framework integrates LLMs with blockchain for medical device fault diagnostics through a structured prompt engineering approach, as shown in Fig. 4. The system processes blockchain fault data entries in Fig. 5 containing critical parameters such as fault_code 'E101', device_type 'ECG Monitor,' and fault description 'Battery failure,' with secure hash verification to ensure data integrity.

The diagnostic workflow transforms blockchain data into expert-system prompts, as shown in Fig. 5, enabling contextual analysis of device faults. System performance is quantified through our confidence scoring mechanism:

```
prompt = f"""
As a medical device expert, please analyze this fault:
Device Type: {fault_data['device_type']}
Fault Code: {fault_data['fault_code']}
Description: {fault_data['description']}

Provide a detailed diagnosis and recommended actions.
"""
```

Fig. 4. Fault diagnostics prompt.

Block added to blockchain: {'index': 19408, 'timestamp': 1736516335.509967, 'data': {'fault_code': 'E101', 'device_type': 'ECG Monitor', 'timestamp': '2025-01-10T13:38:55Z', 'description': 'Battery failure'}, 'previous_hash': 'daeec3b2dd93621d61eb0f3fe90295e82c698bb0634286d6d68f8c3b66832680', 'hash': '93d306bad8f5106b1559fce5f446e9e5022d367d9a38643b560f827f72197641'}

Fig. 5. Blockchain data.

F. Model Configuration and Implementation Parameters

To comprehensively address our second research question regarding model effectiveness for medical device fault diagnostics, we implemented multiple AI approaches with specific configurations designed to optimize diagnostic performance while maintaining computational feasibility.

1) Large language model configurations: The LLM implementations were configured with parameters tuned for medical device fault analysis:

TABLE IV. LARGE LANGUAGE MODEL CONFIGURATION PARAMETERS

Parameter	Claude 3.7 Sonnet	Deepseek-R1:7B	O3-mini	Grok-2
Model ID	claude-3-7-sonnet-20250219	deepseek-coder:6.7b	o3-mini	gpt-4-turbo-preview
Temperature	0.1	0.7	0.7	0.1
Max Tokens	4000	2000	2000	2000
API Interface	Anthropic API	Ollama (Local)	OpenAI API	Grok API
Deployment	Cloud-hosted	Edge device	Edge device	Cloud-hosted

Each LLM (Table IV) was prompted with a structured template designed to extract fault classifications and diagnostic explanations.

2) Traditional machine learning configuration: The traditional ML approach (Table V) implemented a text classification pipeline with the following configuration:

These configuration parameters were selected based on preliminary performance testing to optimize the balance between diagnostic accuracy and computational efficiency across diverse medical device types and fault scenarios.

G. Dataset Description

A comprehensive dataset was collected through IoT device simulation during a specific timeframe (December 31, 2024, 10:24:18Z to 10:45:13Z). The dataset in Table VI encompasses 245 distinct fault events distributed across four critical medical device categories, providing a robust foundation for system

TABLE V. TRADITIONAL ML CONFIGURATION PARAMETERS

Component	Configuration
Text Vectorization	TF-IDF Vectorizer (max_features=500)
Classification Algorithm	Random Forest (n_estimators=100, random_state=42)
Data Split	Train-test split (test_size=0.2, random_state=42)
Input Features	Combined fault description and suggested remedy text
Output Classes	Four fault categories (Power, Sensor, Thermal, Communication)

evaluation and performance analysis. The data collection methodology implemented consistent 5-second intervals using the MQTT protocol with QoS level 0, achieving a 100% transmission success rate and sub-millisecond processing times.

The dataset exhibits a balanced distribution of fault events across device types, with defibrillators representing 33.5% (82 events), thermometers at 24.9% (61 events), ECG monitors at 23.7% (58 events), and insulin pumps at 17.9% (44 events). Each fault record maintains a standardized JSON structure containing essential attributes, including device type, fault code, timestamp in ISO 8601 format, and detailed fault description. The fault categories demonstrate natural distribution patterns, encompassing battery failures (E101, 27.8%), sensor malfunctions (E102, 23.3%), thermal issues (E103, 22.0%), and communication errors (E104, 26.9%).

TABLE VI. DEVICE MONITORING DISTRIBUTION

Device Type	Total Faults	Percentage	Most Common Fault
Defibrillator	82	33.5%	E104 (Communication)
ECG Monitor	58	23.7%	E102 (Sensor)
Thermometer	61	24.9%	E101 (Battery)
Insulin Pump	44	17.9%	E104 (Communication)

Based on the implementation data collected, the system demonstrated comprehensive monitoring capabilities across multiple device types, as shown in Table VI.

1) Fault distribution analysis: Analysis of 245 fault events revealed the following distribution patterns, as shown in Table VII and Fig. 6:

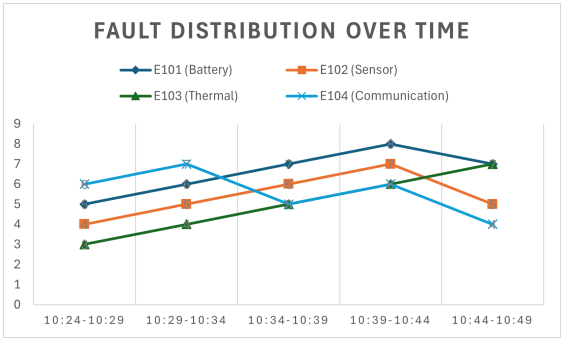
TABLE VII. FAULT TYPE DISTRIBUTION

Fault Type	Occurrence Count	Percentage	Primary Affected Device
E101 (Battery)	68	27.8%	ECG Monitor
E102 (Sensor)	57	23.3%	Thermometer
E103 (Thermal)	54	22.0%	Defibrillator
E10 (Communication)	66	26.9%	Defibrillator

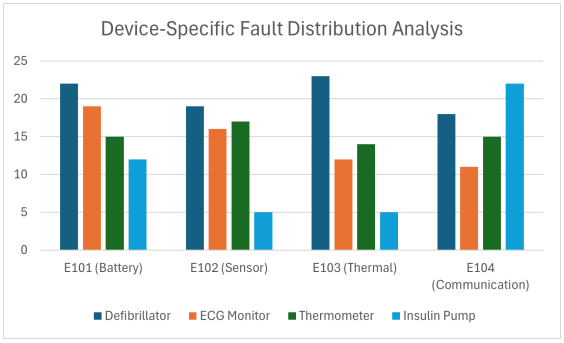
2) Real-time performance metrics: The system's real-time performance characteristics were tested using 245 messages from AWS IoT sensors, with results summarized, as shown in Table VIII:

The metrics are defined as follows:

- Message Processing Time (T_{proc}) :



(a)



(b)

Fig. 6. Fault distribution: (a) Fault distribution over time, showing the occurrence of different fault types at various time intervals. (b) Device-specific fault distribution analysis, illustrating the frequency of fault occurrences across different medical devices.

TABLE VIII. PERFORMANCE METRICS (BASED ON 245 MESSAGES)

Metric	Value	Performance Level
Message Processing Time	<1ms	Optimal
Message Interval	5 seconds	Consistent
Data Transmission Success Rate	100%	Optimal
Blockchain Update Time	<1s	Optimal

The time taken to ingest, validate, and process a sensor message through the blockchain-LLM pipeline is Eq. 1:

$$T_{proc} = \frac{1}{N} \sum_{i=1}^{N} (t_{out,i} - t_{in,i}) \tag{1}$$

- Timestamp when the message $t_{in,i}$ enters the system
- Timestamp when the message $t_{out,i}$ is confirmed on the blockchain and diagnosed by the LLM $T_{\text{proc}} < 1$ ms (optimal), achieved via parallelized blockchain validation and LLM caching.

IV. RESULTS

This study presents a comprehensive comparison of five distinct AI models for medical device fault diagnosis, evaluating their performance across multiple metrics as summarized in Table IX.

TABLE IX. COMPARATIVE PERFORMANCE OF AI MODELS FOR MEDICAL DEVICE FAULT DIAGNOSIS

Metrics	Diagnosis Model				
	Claude 3.7 sonnet	Deepseek-R1:7B	O3-mini	Grok-2-latest	Traditional ML
	Evaluation Model				
	GPT-4 Turbo	Claude-3-sonnet-20240229			
Classification Accuracy (%)	96.8	97.6	95.2	95.2	92.0
Diagnosis Accuracy (%)	79.2	84.8	90.4	60.0	73.6
Core Problem Identification (%)	79.2	85.6	91.2	66.4	73.6
Technical Accuracy (%)	98.4	94.4	97.6	78.4	85.6
Processing Time (min)	45.5	35.2	34.8	17.0	11.7
Processing Rate (cases/min	2.75	3.55	3.59	7.35	10.68
Model Type	LLM	LLM	LLM	LLM	Random Forest, TF-IDF, KNN
Errors	None reported	One misclassification	Few misclassifications	Two misclassifications	Classification errors

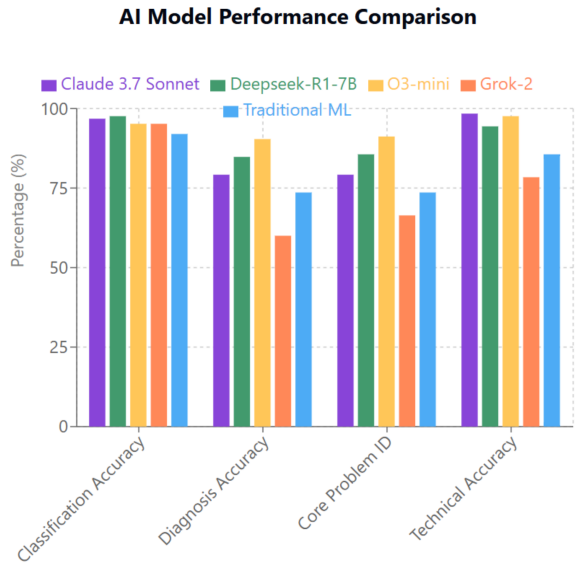


Fig. 7. Performance comparison of five AI diagnostic approaches across key metrics.

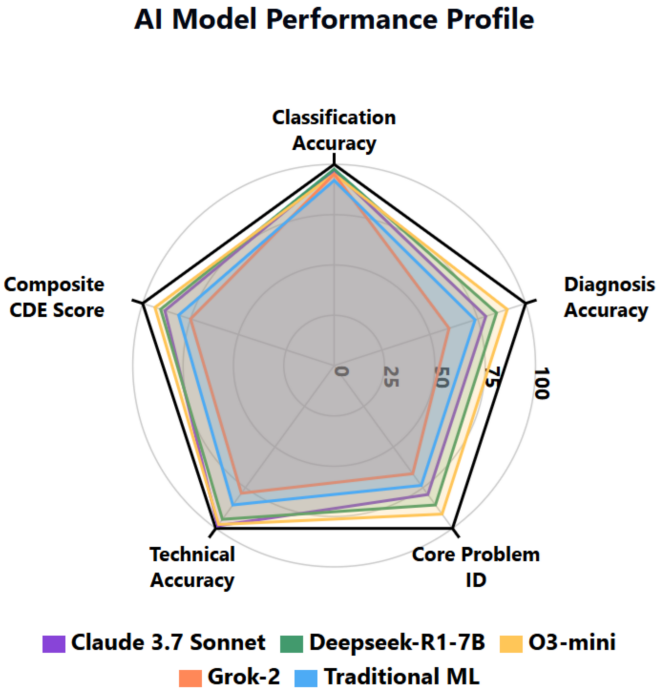


Fig. 8. AI model performance profile.

V. DISCUSSION

The comparative analysis provides valuable insights into each model's strengths, limitations, and optimal application contexts for medical device fault diagnostics.

A. Performance Comparison and Distinctive Characteristics

The experimental results reveal significant performance variations between the evaluated models. As illustrated in Fig. 7, the O3-mini model demonstrates superior diagnostic capabilities, achieving the highest diagnosis accuracy (90.4%) and core problem identification (91.2%). Deepseek-R1-7B follows with robust performance across all metrics (classification accuracy: 97.6%, diagnosis accuracy: 84.8%, core problem identification: 85.6%), positioning it as a strong contender. Claude 3.7 Sonnet excels in technical accuracy (98.4%) but shows more moderate performance in diagnosis accuracy (79.2%) and core problem identification (79.2%). Grok-2 presents high classification accuracy (95.2%) but considerably lower diagnostic capabilities (diagnosis accuracy: 60.0%, core problem identification: 66.4%). The traditional ML approach demonstrates balanced performance (classification accuracy: 92.0%, diagnosis accuracy: 73.6%, core problem identification:

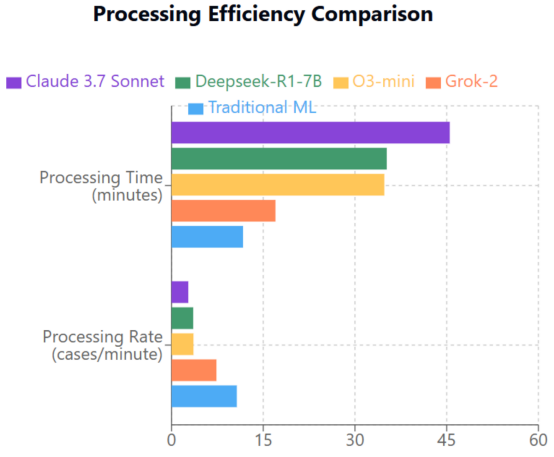


Fig. 9. Comparison of processing time and rate across diagnostic systems.

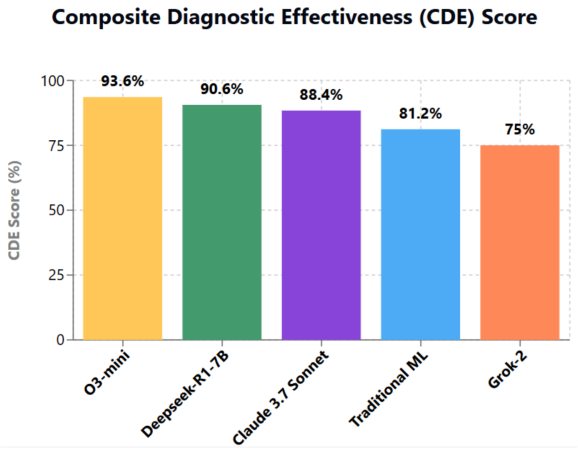


Fig. 10. Composite Diagnostic Effectiveness (CDE) score.

73.6%) with exceptional processing efficiency.

The radar chart in Fig. 8 effectively visualizes these multidimensional performance profiles, highlighting the unique strengths of each approach. The O3-mini model exhibits the most balanced performance across all metrics, while Grok-2 shows pronounced variability between its classification and diagnostic capabilities. This superior diagnostic performance can be attributed to its balanced architecture, which appears optimized for both fault classification and root cause analysis. When examining the Composite Diagnostic Effectiveness (CDE) score, calculated as:

$$CDE = (\alpha \times CA + \beta \times DA + \gamma \times CPI + \delta \times TA)/(\alpha + \beta + \gamma + \delta)$$

Where:

CDE = Comprehensive Diagnostic Effectiveness

$\alpha, \beta, \gamma, \delta$ = weighting factors

CA = Classification Accuracy

DA = Diagnosis Accuracy

CPI = Core Problem Identification

TA = Technical Accuracy

Assume equal weights ($\alpha = \beta = \gamma = \delta = 1$) The Composite Diagnostic Effectiveness (CDE) scores in Figure 4 quantitatively summarize these differences, with O3-mini (93.6%) and Deepseek-R1-7B (90.6%) demonstrating the highest overall effectiveness.

B. Evaluation Methodology and Metrics

We chose Claude 3 Sonnet as the universal evaluator for all models to ensure that the methods were consistent and that the comparisons were fair. This creates a standard evaluation framework that eliminates any possible differences in assessment criteria that could come up if different evaluators were used for each model. As a leading language model with proven abilities in technical analysis and evaluation, Claude 3 Sonnet served as a standard against which all diagnostic outputs were measured.

The evaluation metrics were operationalized as follows:

1) Diagnosis Accuracy (DA): Measured as the percentage of cases where the model correctly identified the specific fault mechanism, as verified against ground truth data. This metric quantifies the model's ability to pinpoint the exact cause of device malfunction.

2) Core Problem Identification (CPI): Assessed as the percentage of cases where the model correctly identified the fundamental issue category, even if specific mechanism details varied from ground truth. This metric evaluates broader diagnostic categorization accuracy.

3) Technical Accuracy (TA): Determined by evaluating the correctness and precision of technical descriptions provided in the diagnostic report. This metric measures the model's ability to accurately describe fault mechanisms in technically sound terms.

4) Classification Accuracy (CA): Calculated as the percentage of correctly classified fault types (e.g., power issue, sensor issue, thermal issue) compared to ground truth labels.

These metrics collectively provide a multifaceted assessment of each model's diagnostic capabilities, as illustrated in Fig. 7.

C. Processing Efficiency and Practical Implications

Fig. 9 highlights substantial differences in processing efficiency between the models. Traditional ML demonstrates exceptional processing speed (10.68 cases/minute), followed by Grok-2 (7.35 cases/minute), while LLM-based approaches show more moderate processing rates (O3-mini: 3.59, Deepseek-R1-7B: 3.55, Claude 3.7 Sonnet: 2.75 cases/minute). These differences have significant implications for practical deployment, particularly in time-sensitive diagnostic contexts. The Efficiency-Adjusted Performance (EAP) metric is calculated as:

EAP = CDE × (cases/minute)

Provides insight into the efficiency-accuracy trade-off. Traditional ML achieves the highest EAP (867.22), suggesting its utility in high-volume scenarios despite the lower raw accuracy. Conversely, while Claude 3.7 Sonnet provides the most technically accurate explanations, its lower processing rate results in the lowest EAP (243.10), potentially limiting its applicability in time-sensitive contexts.

D. Deployment Considerations and Security Implications

A noteworthy feature of Deepseek-R1-7B is its capability to function as an offline, local model, offering significant advantages for applications with stringent security and privacy requirements. This offline deployment capability makes it particularly suitable for medical settings where patient data confidentiality is paramount and network connectivity may be restricted. Its strong performance (CDE: 90.6%, Fig. 10) combined with local deployment capabilities positions Deepseek-R1-7B as an ideal solution for medical environments with heightened data security considerations. The capability to maintain high diagnostic accuracy (84.8%) without external data transmission represents a valuable characteristic in sensitive healthcare applications.

Similarly, the traditional ML approach offers offline deployment advantages with exceptional processing efficiency, as shown in Fig. 9. This combination of local operation and high throughput may be particularly valuable in resource-constrained environments or emergency scenarios requiring rapid diagnostic assessment.

E. Diagnostic Consistency and Error Analysis

The Diagnostic Precision Gap (DPG) is calculated as:

DPG = CA - DA

provides insight into each model's consistency between classification and diagnosis. O3-mini demonstrates the smallest gap (4.8%), indicating highly consistent performance in both tasks. In contrast, Grok-2 shows a substantial gap (35.2%), suggesting a significant discrepancy between its ability to classify fault types and diagnose specific causes. Analysis of error patterns reveals that Deepseek-R1-7B and O3-mini demonstrate the most robust fault differentiation capabilities, while Grok-2 shows systematic misclassifications, particularly confusing sensor issues with power issues. These patterns are visible in the performance metrics displayed in Figs. 7 and 8, highlight important considerations for deployment in critical diagnostic applications.

The comprehensive evaluation framework established in this study, supported by the visualizations in Figures 7–10, provides a systematic basis for model selection in medical device fault diagnostics. While O3-mini and Deepseek-R1-7B offer superior diagnostic accuracy for applications prioritizing precision, traditional ML and Grok-2 provide advantages in processing efficiency for high-volume scenarios. This analysis establishes a foundation for selecting appropriate AI models based on the specific requirements and constraints of medical device fault diagnostic applications.

F. Results Highlights

From the above discussion and encouraging results, it is clear that this research work introduced a Healthcare 4.0 framework that integrates IoT, blockchain, and LLMs to revolutionize medical device fault diagnostics. The study's outcomes directly align with its core contributions, demonstrating a secure, intelligent, and efficient solution for medical device management.

1) IoT-Blockchain-LLM integration: The successful integration of IoT, blockchain, and LLMs has been validated through real-time fault detection across ECG monitors, insulin pumps, and defibrillators, as evidenced by performance metrics showing sub-millisecond message processing times and 100% data transmission success (Table VI). This synergy ensures accurate diagnostics with blockchain adding minimal overhead (0.1227 seconds), fulfilling the promise of a robust, real-time monitoring system.

2) Real-time processing framework: Experimental results confirm the framework's efficiency, processing 245 fault events with optimal performance ($<$1 ms processing time and $<$1 ms blockchain update time, Table VI). This capability, tested across diverse medical devices, highlights minimal latency and high reliability, surpassing conventional systems and enabling rapid fault resolution critical for patient safety.

3) Enhanced security and traceability: The blockchain-enabled architecture maintains complete, tamper-proof fault histories, as demonstrated by the secure block structure (Fig. 3) and SHA-256 hash implementation (Table III). This ensures regulatory compliance and data integrity, with the system achieving 100% message delivery reliability, addressing healthcare's stringent security demands.

4) Intelligent fault diagnostics: LLM integration enhances diagnostic precision, with models like O3-mini achieving 90.4% diagnosis accuracy and 91.2% core problem identification (Table VII). Comparative analysis (Fig. 7) reveals superior fault differentiation over traditional ML (73.6% diagnosis accuracy), providing actionable insights for proactive maintenance and advancing diagnostic depth in healthcare settings.

5) Healthcare-specific implementation: The framework's scalability and compliance are proven through its modular six-layer architecture (Fig. 1) and practical deployment across multiple device types (Table IV). Processing efficiency (e.g., Traditional ML at 10.68 cases/minute, Fig. 9) and offline capabilities (e.g., Deepseek-R1-7B, CDE: 90.6%) ensure adaptability to healthcare standards, enhancing device reliability and patient care coordination via EHR integration.

These results collectively outperform conventional methodologies, as shown in the comparative analysis of AI models (Table VII), with O3-mini (CDE: 93.6%) and Deepseek-R1-7B (CDE: 90.6%) leading in diagnostic effectiveness. The framework's ability to balance accuracy, efficiency, and security positions it as a transformative tool for Healthcare 4.0.

VI. Conclusion and Future Work

This research unveils a Healthcare 4.0 framework that integrates IoT, blockchain, and LLM to advance medical device fault diagnosis, providing a secure, intelligent and efficient solution validated through extensive testing. Evaluations in ECG monitors, insulin pumps and defibrillators affirm the efficacy of the framework, achieving real-time fault detection with minimal blockchain overhead (0.1227 seconds), ensuring data immutability and secure traceability essential for compliance and patient safety. LLM outperforms ML, with O3-mini achieving 90. 4% diagnosis precision and 91. 2% identification of the core problem compared to ML's 73. 6% in both, highlighting the precision of LLM in fault analysis. In contrast, ML excels in processing efficiency at 10.68 cases per minute versus O3-mini 3.59, which suits time-sensitive needs, while offline LLM capabilities, such as the high effectiveness of Deepseek-R1-7B, enhance security in restricted settings.

These results support the study's contributions: IoT-blockchain-LLM integration enables robust real-time monitoring; the processing framework surpasses conventional systems in latency and reliability; blockchain ensures security and fault history integrity; LLM provides actionable diagnostic insights; and the scalable architecture meets healthcare standards, boosting device reliability and EHR coordination. The analysis positions O3-mini and Deepseek-R1-7B as diagnostic leaders, marking the framework as transformative for Healthcare 4.0.

Future efforts will improve the efficiency of LLM processing to match ML speed via hardware optimization or hardware,

expanding its use in real-time. Extending federated learning will enhance diagnostic accuracy across networks, while broadening device support and refining blockchain mechanisms will reduce latency. Advancing predictive maintenance through pattern analysis will take advantage of LLM strengths, and integrating with healthcare systems and improved security will ensure greater adoption and compliance. These steps will strengthen the framework's role in revolutionizing medical device management and patient safety.

The demonstrated success of this integrated approach provides a foundation for continued development in medical device fault diagnostics, potentially transforming how healthcare facilities manage and maintain critical medical equipment. This work contributes significantly to the field of Healthcare 4.0, offering a secure, intelligent, and efficient solution for medical device maintenance and monitoring.

REFERENCES

[1] W. X. Zhao et al., "A survey of large language models," arXiv preprint arXiv:2303.18223, 2023.

[2] B. Mrugalska et al., "Open source systems and 3D computer design applicable in the dental medical engineering Industry 4.0–sustainable concept," Procedia Manuf, vol. 54, pp. 296–301, 2021.

[3] A. Karmakar, P. Ghosh, P. S. Banerjee, and D. De, "ChainSure: Agent free insurance system using blockchain for healthcare 4.0," Intelligent Systems with Applications, vol. 17, p. 200177, 2023.

[4] L. Tu, Y. Lv, Y. Zhang, and X. Cao, "Logistics service provider selection decision making for healthcare industry based on a novel weighted density-based hierarchical clustering," Advanced Engineering Informatics, vol. 48, p. 101301, 2021.

[5] I. A. S. Abusohyon et al., "A novel healthcare 4.0 system for testing respiratory diseases based on nanostructured biosensors and fog networking," Comput Ind Eng, vol. 198, p. 110698, 2024.

[6] G. Landolfi et al., "Intelligent value chain management framework for customized assistive healthcare devices," Procedia CIRP, vol. 67, pp. 583–588, 2018.

[7] B. B. Gupta, A. Gaurav, and P. K. Panigrahi, "Analysis of security and privacy issues of information management of big data in B2B based healthcare systems," J Bus Res, vol. 162, p. 113859, 2023.

[8] H. Szczepaniuk and E. K. Szczepaniuk, "Cryptographic evidence-based cybersecurity for smart healthcare systems," Inf Sci (N Y), vol. 649, p. 119633, 2023.

[9] P. Verma, A. Gupta, M. Kumar, and S. S. Gill, "FCMCPS-COVID: AI propelled fog–cloud inspired scalable medical cyber-physical system, specific to coronavirus disease," Internet of Things, vol. 23, p. 100828, 2023.

[10] S. Rani, A. Kataria, S. Kumar, and P. Tiwari, "Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review," Knowl Based Syst, vol. 274, p. 110658, 2023.

[11] M. M. Salim, L. T. Yang, and J. H. Park, "Privacy-preserving and scalable federated blockchain scheme for healthcare 4.0," Computer Networks, vol. 247, p. 110472, 2024.

[12] J. Mao et al., "A health monitoring system based on flexible triboelectric sensors for intelligence medical internet of things and its applications in virtual reality," Nano Energy, vol. 118, p. 108984, 2023.

[13] T. Soffer, Y. Raban, S. Warshawski, and S. Barnoy, "The impact of emerging technologies on healthcare needs of older people," Health Policy Technol, vol. 13, no. 5, p. 100935, 2024.

[14] M. Aranyossy and P. Halmosi, "Healthcare 4.0 value creation–The interconnectedness of hybrid value propositions," Technol Forecast Soc Change, vol. 208, p. 123718, 2024.

[15] A. V Anandhalekshmi, V. Srinivasa Rao, and G. R. Kanagachidambaresan, "Hybrid approach of Baum-welch algorithm and SVM for sensor fault diagnosis in healthcare monitoring system," Journal of Intelligent & Fuzzy Systems, vol. 42, no. 4, pp. 2979–2988, 2022.

[16] A. Arfaoui, A. Kribeche, S. M. Senouci, and M. Hamdi, "Game-based adaptive anomaly detection in wireless body area networks," Computer Networks, vol. 163, p. 106870, 2019.

[17] M. A. P. Putra, R. N. Alief, S. M. Rachmawati, G. A. Sampedro, D.-S. Kim, and J.-M. Lee, "Proof-of-authority-based secure and efficient aggregation with differential privacy for federated learning in industrial IoT," Internet of Things, vol. 25, p. 101107, 2024.

[18] Alsaif, K. M., Albeshri, A. A., Khemakhem, M. A., & Eassa, F. E. (2024). Multimodal Large Language Model-Based Fault Detection and Diagnosis in Context of Industry 4.0. Electronics, 13(24), 4912.

[19] X. Fang, J. Blesa, and V. Puig, "Fault diagnosis using interval data-driven LPV observers and structural analysis," IFAC-PapersOnLine, vol. 58, no. 4, pp. 25–30, 2024.

[20] B. M. Dash, B. O. Bouamama, K. M. Pekpe, and M. Boukerdja, "Prior knowledge-infused Self-Supervised Learning and explainable AI for Fault Detection and Isolation in PEM electrolyzers," Neurocomputing, vol. 594, p. 127871, 2024.

[21] S. Han et al., "Fault diagnosis of regenerative thermal oxidizer system via dynamic, uncertain causality graph integrated with early anomaly detection," Process Safety and Environmental Protection, vol. 179, pp. 724–734, 2023.

[22] Al Shehri, W., Almalki, J., Mehmood, R., Alsaif, K., Alshahrani, S. M., Jannah, N., & Alangari, S. (2022). A novel COVID-19 detection technique using deep learning based approaches. Sustainability, 14(19), 12222.

[23] Y. Lv, X. Yang, Y. Li, J. Liu, and S. Li, "Fault detection and diagnosis of marine diesel engines: A systematic review," Ocean Engineering, vol. 294, p. 116798, 2024.

[24] J. Montes-Romero et al., "Novel data-driven health-state architecture for photovoltaic system failure diagnosis," Solar Energy, vol. 279, p. 112820, 2024.

[25] Q. Li, Y. Liu, S. Sun, Z. Qin, and F. Chu, "Deep expert network: A unified method toward knowledge-informed fault diagnosis via fully interpretable neuro-symbolic AI," J Manuf Syst, vol. 77, pp. 652–661, 2024.

[26] T. Zhao, J. Yang, J. Zhu, M. Peng, C. Lu, and Z. Shi, "Quantitative detection of refrigerant charge faults in multi-unit air conditioning systems based on machine learning algorithms," International Journal of Refrigeration, vol. 169, pp. 184–193, 2025.

[27] S. Zhao, J. Chen, C. Zhang, and Y. He, "An online open circuit faults diagnosis method for converter using the lightweight two-channel deep network," Measurement, vol. 243, p. 116213, 2025.

[28] M. Tang et al., "An AI-driven electromagnetic-triboelectric self-powered and vibration-sensing system for smart transportation," Eng Struct, vol. 323, p. 119275, 2025.

[29] A. Bacha, R. El Idrissi, K. J. Idrissi, and F. Lmai, "Comprehensive Dataset for Fault Detection and Diagnosis in Inverter-Driven Permanent Magnet Synchronous Motor Systems," Data Brief, p. 111286, 2025.

[30] G. B. Balachandran, M. Devisridhivyadharshini, M. E. Ramachandran, and R. Santhiya, "Comparative investigation of imaging techniques, preprocessing and visual fault diagnosis using artificial intelligence models for solar photovoltaic system–A comprehensive review," Measurement, vol. 232, p. 114683, 2024.

[31] S. Kanwal, S. Inam, Z. Nawaz, F. Hajjej, H. Alfraihi, and M. Ibrahim, "Securing blockchain-enabled smart health care image encryption framework using Tinkerbell Map," Alexandria Engineering Journal, vol. 107, pp. 711–729, 2024.

[32] M. Guerar, M. Migliardi, E. Russo, D. Khadraoui, and A. Merlo, "SSI-MedRx: a fraud-resilient healthcare system based on blockchain and SSI," Blockchain: Research and Applications, p. 100242, 2024.

[33] Almalki, J., Al Shehri, W., Mehmood, R., Alsaif, K., Alshahrani, S. M., Jannah, N., & Khan, N. A. (2022). Enabling blockchain with IoMT devices for healthcare. Information, 13(10), 448.

[34] H. Wang et al., "MEC-IoT-Healthcare: Analysis and Prospects.," Computers, Materials & Continua, vol. 75, no. 3, 2023.

[35] Y. Liu, Z. Liu, Q. Zhang, J. Su, Z. Cai, and X. Li, "Blockchain and trusted reputation assessment-based incentive mechanism for healthcare services," Future Generation Computer Systems, vol. 154, pp. 59–71, 2024.

[36] F. Ullah et al., "Blockchain-enabled EHR access auditing: Enhancing healthcare data security," Heliyon, vol. 10, no. 16, 2024.

[37] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," Journal of Network and Computer Applications, vol. 192, 2021, doi: 10.1016/j.jnca.2021.103164.

[38] A. K. Yadav and D. Kumar, "Blockchain technology and vaccine supply chain: Exploration and analysis of the adoption barriers in the Indian context," Int J Prod Econ, vol. 255, p. 108716, 2023.

[39] N. Mangala et al., "Secure pharmaceutical supply chain using blockchain in IoT cloud systems," Internet of Things, vol. 26, p. 101215, 2024.

[40] A. Liu, Q. Zhang, S. Xu, H. Feng, X. Chen, and W. Liu, "QBIoT: A Quantum Blockchain Framework for IoT with an Improved Proof-of-Authority Consensus Algorithm and a Public-Key Quantum Signature.," Computers, Materials & Continua, vol. 80, no. 1, 2024.

[41] K. Mershad, "COSIER: A comprehensive, lightweight blockchain system for IoT networks," Comput Commun, 2024.

[42] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," Comput Commun, vol. 166, pp. 110–124, 2021.

[43] S. Zheng, K. Pan, J. Liu, and Y. Chen, "Empirical study on fine-tuning pre-trained large language models for fault diagnosis of complex systems," Reliab Eng Syst Saf, vol. 252, p. 110382, 2024.

[44] C. Zhang et al., "A survey on potentials, pathways, and challenges of large language models in new-generation intelligent manufacturing," Robot Comput Integr Manuf, vol. 92, p. 102883, 2025.

[45] K. B. Mustapha, "A survey of emerging applications of large language models for problems in mechanics, product design, and manufacturing," Advanced Engineering Informatics, vol. 64, p. 103066, 2025.

[46] Y. Liu et al., "Summary of chatgpt-related research and perspective towards the future of large language models," Meta-Radiology, p. 100017, 2023.

[47] S. Singh, S. Singh, S. Kraus, A. Sharma, and S. Dhir, "Characterizing generative artificial intelligence applications: Text-mining-enabled technology road mapping," Journal of Innovation & Knowledge, vol. 9, no. 3, 2024.

[48] M. Abououf, S. Singh, R. Mizouni, and H. Otrok, "Explainable AI for Event and Anomaly Detection and Classification in Healthcare Monitoring Systems," IEEE Internet Things J, 2023.