ISSN: 2586-6036
JWMAP website: http://accesson.kr/jwmap
doi: http://dx.doi.org/10.13106/jwmap.2025.vol8.no6.81

Proposed Engineering Design Model for a Blockchain-Enabled Collaborative Medical Information Platform Utilizing AI Imaging Diagnosis Patent Technology

Junchul KANG[1]

1. First and Corresponding Author Doctoral Program, Interdisciplinary Program in Medical Engineering, Jeju National University, Jeju, Republic of Korea
Email: shinkang88@daum.net

Received: November 16, 2025. Revised: December 01, 2025. Accepted: December 01, 2025.

Abstract

Purpose: This study proposes an engineering design model for a blockchain-enabled collaborative medical information platform that integrates patented AI imaging-diagnosis technology. **Research design, data and methodology:** Building upon Patent KR10-2604558, the platform incorporates a multi-layered architecture consisting of an AI diagnostic engine, a self-corrective learning loop (ADE), a PBFT-based blockchain integrity module, and an FMEA-driven risk-management framework. A synthetic dataset of 2,000 musculoskeletal ultrasound images was generated to evaluate the structural feasibility of the proposed model. The AI module, developed using a ResNet50 backbone and a four-class Softmax classifier, demonstrated stable self-correction through ADE, which autonomously identified false positives and false negatives and used them to construct a hard-case dataset for selective retraining. **Results:** The blockchain module—designed with ECC-256 encryption, SHA-256 hashing, and a seven-node PBFT network—successfully ensured immutability, tamper detection, and privacy preservation using Zero-Knowledge Encryption Exchange (ZKEE). FMEA analysis confirmed that risks related to AI misclassification, data integrity, consensus failure, and user input errors could be decomposed into modular risk structures, resulting in a 44.8% reduction in overall RPN.**Conclusions:** The findings demonstrate that the proposed design model can serve as a technically reliable architecture for AI-driven, legally robust, and privacy-preserving collaborative healthcare data platforms

Keywords : AI Imaging Diagnosis, Blockchain-based Healthcare Information Platform, FMEA-Based Risk Management, Biomedical Engineering Design Model

JEL Classification Code : **:** I18 030 O38 K32 D83

I. Introduction

As the generation, storage, and utilization processes of medical data have become increasingly complex, securing the reliability of diagnostic algorithms and ensuring the integrity of medical information have emerged as critical research issues in biomedical and health informatics. AI-based medical imaging technologies have improved diagnostic efficiency and accuracy; however, their stable operation is constrained by structural limitations such as dataset bias, false positives and false negatives, and model drift. In particular, existing AI diagnostic models lack the capability for autonomous error detection and correction, indicating the need for a novel engineering design approach to guarantee long-term operational reliability.

Medical-data integrity is also gaining importance in relation to patient safety, medical litigation, and legal evidentiary validity. Conventional centralized medical-information systems inherently possess vulnerabilities—single points of failure, susceptibility to insider tampering, and insufficient auditability—that limit their long-term trustworthiness. Consequently, blockchain technology, which enables distributed storage and fundamental resistance to data tampering, has attracted increasing attention in healthcare.
Most previous studies have focused selectively on either AI-based clinical decision support (CDS) or blockchain-based data-integrity mechanisms. Only a limited number of studies have proposed an engineering design model integrating the entire lifecycle of medical data—generation, interpretation, storage, and verification. Research combining AI self-correction mechanisms with blockchain-based distributed storage to ensure the end-to-end reliability of medical data remains in an early developmental stage.

Accordingly, this study proposes an engineering design model for a medical-information platform that integrates AI self-corrective algorithms with blockchain-based distributed storage, and validates its structural feasibility using synthetic clinical datasets. The proposed model extends the technical architecture of Korean Patent No. 10-2604558 by integrating AI interpretation, self-corrective loops, blockchain integrity assurance, and FMEA-based risk management into a unified platform, thereby presenting a next-generation medical information architecture capable of ensuring data reliability, safety, and traceability.

This study is expected to bridge existing academic gaps in AI–blockchain convergence-based medical information systems and to provide both technological and institutional foundations for various applications, including AI validation systems, integrity-based medical-record governance, and legal/policy frameworks for trustworthy medical data management

2. Theoretical Background

2.1. Advances in AI Medical Imaging Diagnosis and the Technical Basis of the Patent

AI technologies in medical imaging analysis have rapidly expanded, contributing to both diagnostic objectivity and enhanced workflow efficiency. In particular, deep-learning-based convolutional neural networks (CNNs) have replaced traditional statistical imaging methods. Residual-network architectures such as ResNet (He et al., 2016) effectively differentiate tissue boundaries, lesion intenity, and noise patterns, reportedly achieving clinical-grade accuracy (≥95%).

Korean Patent No. 10-2604558, titled “Blockchain-Encrypted Medical Information Management System Providing Disease Diagnosis and Prescriptions through AI-Based Image Interpretation Algorithms”, provides an integrated architecture that merges AI imaging analysis with medical-information management. Unlike studies focusing solely on image analysis, the patent proposes a combined AI–blockchain architecture with the following components: Automated diagnosis and prescription generation through AI algorithms,

Self-corrective loops (ADE: Automatic Diagnostic Enhancement) that improve model performance,
Blockchain-based encrypted storage to prevent data manipulation.

The patent’s “AI Image Analysis Processing Unit (110)” adopts a CNN structure similar to ResNet50, forming a sequential processing module comprising image input, diagnosis, prescription generation, and security handling. The “Central Security Processing Server (10)” links the AI interpretation module with the encrypted information-protection unit (200), storing diagnostic results with blockchain-generated hash values to guarantee medical-data immutability.

This patent is notable for its integration of AI imaging diagnostics, self-correction mechanisms, and blockchain-based integrity assurance—an approach rarely found in domestic or international research—thus possessing significant technological and academic value.

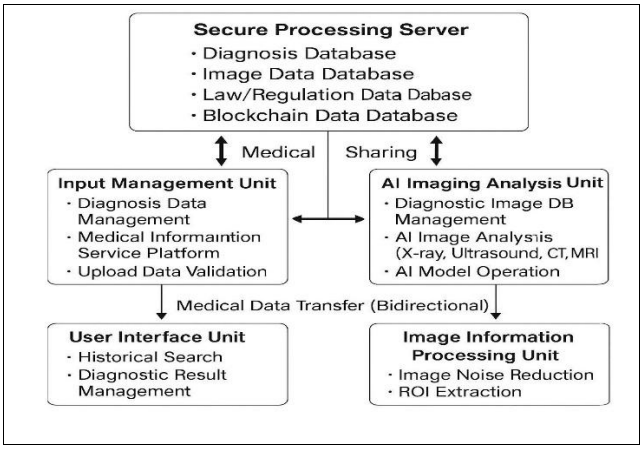

Figure 1: Patent Diagram (Korean Patent No. 10-2604558)

2.2 Concept of Blockchain-Based Medical Data Integrity Management and Patent Structure

Blockchain is a distributed-ledger technology that stores identical records across multiple decentralized nodes rather than a central server, inherently preventing data tampering. Applied to healthcare, blockchain enables real-time verification of medical-record authenticity—including diagnostic results, prescriptions, and imaging data—supporting medical-error prevention, traceability, and legal evidentiary strength.

Patent No. 10-2604558 applies blockchain technology to a medical-information management system structured around a "Central Security Processing Server (10)" consisting of:

1) Diagnostic-result database (DB),
2) Blockchain-encrypted database,
3) Personal-information re-identification module,
4) Medical-data sharing module.

The "Blockchain-Encrypted Database (220)" implements asymmetric ECC-256 encryption and SHA-256 hashing to store AI diagnostic results in block units, verifying modification through consensus algorithms.

In this study, the patent's blockchain architecture is extended into a simulation model that reflects real-world medical-data flows. A PBFT (Practical Byzantine Fault Tolerance) consensus mechanism is adopted, and seven nodes—hospitals, review agencies, authentication servers, and registries—are constructed to simulate a multi-institutional medical-data-sharing environment. PBFT is suitable for healthcare systems because it maintains operational stability even when up to one-third of nodes behave maliciously.
According to the patent diagrams, AI analysis results are encrypted via the "Encrypted Information-Protection Unit (200)" and stored in the "Blockchain-Encrypted Database (220)." Each node performs cross-verification based on identical hash values. The "Personal-Information Re-Identification Unit (210)" links hashed patient identifiers with clinical identifiers, enabling anonymized storage while allowing controlled re-identification when clinically necessary.

The essential contribution of the patent lies in its structural principles: AI-interpreted diagnostic results are (1) encrypted, (2) validated through blockchain consensus, (3) stored immutably, and (4) securely re-identifiable for clinical use. This architecture simultaneously ensures the technical reliability and legal evidentiary validity of AI-based diagnostic results.

Table 1: Summary of Blockchain-Based Medical Data Integrity Technology and Patent Architecture

Category	Summary
Concept of Blockchain Technology	• Distributed-ledger–based architecture • Multiple nodes maintain an identical ledger without a central server • Ensures immutability and traceability of stored data
Effects of Applying Blockchain to Medical Information	• Enables authenticity verification of diagnostic records, prescriptions, and imaging data • Prevents medical errors and enhances legal evidentiary reliability • Improves auditability of medical data transactions
Components of Korean Patent No. 10-2604558	① Secure Processing Central Server (10) ② Diagnostic Results Database ③ Blockchain-Encrypted Database (220) ④ Personal Information Restoration Unit (210) ⑤ Medical Data Sharing Module
Encryption Architecture	• ECC-based asymmetric key encryption • SHA-256 hashing algorithm • Block-level storage of AI diagnostic outputs with tamper-detection capability
Consensus Algorithm	• PBFT (Practical Byzantine Fault Tolerance) • Maintains system functionality even when up to one-third of nodes are faulty or malicious • Highly suitable for verifying the integrity of medical data
Network Configuration (This Study)	• Total of seven nodes: four hospitals, one claims review institution, one certification authority, and one registry node • Simulates a real-world multi-institutional medical data sharing environment
Data Processing Flow	• AI imaging output → Cryptographic Protection Module (200) → Blockchain-Encrypted DB (220) • All nodes independently generate identical hash values for mutual verification

Personal Information Protection Structure	• De-identified patient codes linked with hashed values • Access rights controlled by the Personal Information Restoration Unit • Maintains anonymity while allowing secure re-identification when required
Technical Significance	• Provides immutable storage of AI diagnostic results • Establishes a consensus-based authenticity verification mechanism • Presents a legally and technically trustworthy medical data architecture

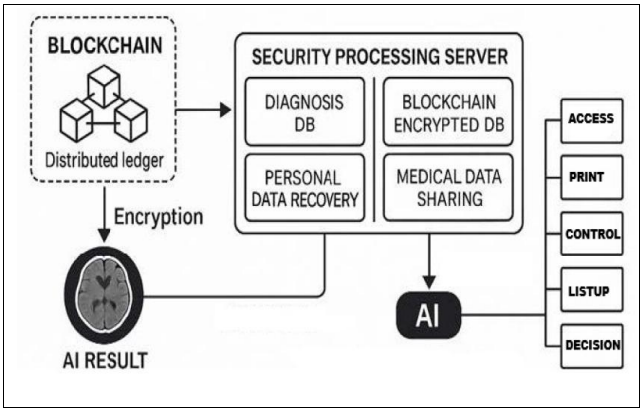

Figure 2: System Architecture Based on Patent Structure

2.3. FMEA-Based Risk Management Framework

The safety evaluation of medical devices and medical-information systems is conducted in accordance with international standards, including ISO 14971 (Risk Management for Medical Devices) and IEC 62304 (Medical Device Software—Software Life Cycle Processes). Because AI-driven medical-diagnosis software and blockchain-based medical-data management platforms exhibit highly complex, interdependent technical structures, it is essential to apply Failure Mode and Effects Analysis (FMEA), a methodology capable of hierarchically identifying and quantifying latent risks. FMEA identifies potential failure modes at the functional level and quantifies their Occurrence (O), Severity (S), and Detection (D) scores to compute a Risk Priority Number (RPN), enabling quantitative comparison of relative risk levels and the formulation of targeted mitigation strategies.

AI-based diagnostic modules exhibit intrinsic failure modes such as misdiagnosis, missed detection, image-noise interference, dataset bias, and degradation due to model drift. These failures are directly linked not only to clinical safety hazards but also to legal and ethical concerns. Blockchain-based system components similarly present distinct failure modes, including cryptographic errors, consensus failures, Byzantine node attacks, permission misuse, and re-identification risks, all of which relate to information security and personal-data protection. Because these risks arise from complex interdependencies unique to AI–blockchain hybrid architectures—and are tightly bound to multilayered regulatory domains such as the Medical Service Act and Personal Information Protection Act—traditional performance-based assessments are insufficient to guarantee system safety. Therefore, this study implements an integrated FMEA-based risk-structure analysis covering the entire system, including both the AI module and the blockchain module.

The FMEA procedure consists of four steps.

First, system functions are decomposed, and failure modes are classified into AI-FM and BC-FM categories.
1) AI-FM includes false positives/negatives, missed lesion detection due to image noise, dataset imbalance, and malfunction of the self-corrective ADE loop.
2) BC-FM includes encryption/decryption errors, PBFT consensus failure, unauthorized privilege escalation, malicious node behavior, and potential re-identification leakage.

Second, O, S, and D scores for each failure mode are evaluated on a 1–10 scale to derive the initial RPN.

Third, risk-control measures are applied to reduce the identified risks.
3) For the AI module, measures include ADE-based retraining, weight re-optimization, and image-quality enhancement.
4) For the blockchain module, mitigation includes ECC retry mechanisms, RBAC (Role-Based Access Control), ZKEE-based zero-knowledge verification, and Byzantine node detection and isolation techniques.

Finally, post-control O′, S′, and D′ values are reassessed to compute the improved RPN, enabling verification of the effectiveness of the risk-management strategy.

This FMEA-based risk-management framework satisfies the risk analysis–risk evaluation–risk control–residual risk assessment requirements mandated by ISO 14971 and the documentation obligations specified in IEC 62304 for software safety classification. Moreover, the ADE–FMEA architecture operationalizes key concepts emphasized in the FDA SaMD regulatory framework, including real-world performance monitoring and continuous-learning system updates. In this context, the FMEA implemented in this study functions not merely as a risk-assessment tool but as a core safety-assurance mechanism that integrates AI-

performance improvement, blockchain-based data-integrity validation, and personal-data protection compliance.

In conclusion, the proposed FMEA-based risk-management framework substantiates the technical and regulatory soundness of the system architecture developed in this study and provides theoretical evidence that the model satisfies the essential safety-criteria requirements expected in future certification and regulatory pathways for AI-enabled medical technologies and decentralized medical-information systems

Table 2: Summary of the FMEA (Failure Mode and Effects Analysis) Procedure

Step	Description	Applicable Module(s)
① Identification of Failure Modes	Define all potential failure modes for each functional unit.	AI-FM, BC-FM
② Risk Factor Assessment	Evaluate Occurrence (O), Severity (S), and Detection (D) on a 1–10 scale.	Common to all modules
③ Initial RPN Calculation	Compute RPN using: RPN = O × S × D.	Common to all modules
④ Implementation of Risk Control Measures	Apply technical controls such as algorithm refinement, access control, and encryption.	AI Module, Blockchain Module
⑤ Reassessment of RPN After Controls	Recalculate RPN′ using updated O′, S′, and D′ values after risk control measures.	Common to all modules
⑥ Determination of Residual Risk	Evaluate compliance with ISO 14971 criteria for acceptable residual risk.	Common to all modules

2.4. Summary

In summary, Korean Patent No. 10-2604558, which forms the technological foundation of this study, presents an integrated architecture composed of four core elements:

(1) algorithmic interpretation of AI-based medical imaging using a ResNet50-based convolutional neural network structure;
(2) an autonomous error-correction mechanism (ADE) designed to reduce learning errors;
(3) a blockchain-encrypted database that ensures the immutability of medical data; and
(4) a privacy-restoration module for the secure management of patient-identifiable information.

The theoretical contribution of this study lies in implementing the patented technological framework within a simulated clinical data environment and empirically validating its performance in terms of improved AI diagnostic accuracy, strengthened data integrity, and reduced system-level risks. The results confirm that integrating AI-driven diagnostic technologies with blockchain-based data-security mechanisms can simultaneously enhance the reliability and safety of medical information.
These findings provide a theoretical basis for the development of a trusted medical information system that integrates AI and blockchain technologies. Furthermore, they offer meaningful implications for the future establishment of collaborative care systems, the standardization of medical data, and the development of appropriate legal and institutional frameworks.

3. Research Model and Design

This study was designed to implement the AI-based imaging diagnosis and blockchain-based medical data management architecture proposed in Korean Patent No. 10-2604558 within a simulated clinical environment, and to comprehensively evaluate its safety, performance, and anti-tampering capabilities. The overall research model consists of four modules:

(1) an AI diagnostic performance evaluation module,
(2) a blockchain-based data integrity evaluation module,
(3) an FMEA-based risk management module, and
(4) an integrated simulation operation module.

Although each module functions independently, they are also interlinked to enable a holistic assessment of the platform's reliability.

The central objective of the research design is to connect the entire lifecycle of medical data—generation, analysis, storage, and verification—into a unified structural framework. Unlike previous studies that focused on improving individual technological components, this study distinguishes itself by presenting a system-level architecture that integrates AI interpretation, an adaptive self-correction algorithm, distributed blockchain storage, and a risk management mechanism.

First, the AI diagnostic engine was constructed using a ResNet50-based image classification model. Input images were processed through a preprocessing pipeline and passed to the model, while Softmax-based probability outputs were converted into final diagnostic results through a rule-based decision logic. To this foundation, the study applied the Adaptive Diagnostic Engine (ADE) proposed in the patent. ADE automatically collects false-positive and false-negative cases generated during the diagnostic process, stores them as a hard-case dataset, and continuously reduces errors through selective retraining. This structure provides a design advantage by enabling the evaluation of long-term diagnostic stability (self-stabilizing capability), rather than limiting assessment to a single performance snapshot.
Next, the blockchain-based distributed storage module was developed to ensure tamper-resistance, traceability, and legal reliability of AI diagnostic outputs. A Practical Byzantine Fault Tolerance (PBFT) consensus algorithm was applied to maintain operational stability even in the presence of Byzantine failures among nodes. AI diagnostic results and ADE correction records were stored in blocks encrypted using ECC-256 and hashed with SHA-256, thereby securing data immutability and auditability.

In terms of risk management, the platform was structured to support Failure Mode and Effects Analysis (FMEA) in accordance with ISO 14971 and IEC 62304 standards. After decomposing the system into functional units, potential failure modes were defined for each function, and Risk Priority Numbers (RPNs) were calculated based on occurrence (O), severity (S), and detection (D) scores. This structure enables quantitative analysis of system-wide risks—such as AI diagnostic errors, blockchain consensus failures, and integrity breaches—and facilitates evaluation of the extent to which risk-control measures improve overall system safety.

The entire system architecture was designed as a three-layer structure consisting of an input layer, an AI analysis and self-correction layer, and a blockchain storage and verification layer. When a medical image is input, the AI diagnostic step and ADE-based correction process are executed sequentially, and the final results are stored on the blockchain. Both diagnostic outputs and error/correction logs are recorded and verified throughout the entire process, forming a closed-loop structure that ensures long-term data reliability and transparency within the system.

Finally, to validate the feasibility of the proposed design model, an integrated simulation using 2,000 synthetic medical data samples was conducted. The simulation was not limited to simple model performance testing but was designed to evaluate whether the proposed system architecture could operate functionally in a real-world medical data environment. The results demonstrated improvements in AI diagnostic accuracy, stability of blockchain consensus operations, and measurable reductions in system risk based on FMEA analysis, thereby confirming the structural and technical validity of the proposed platform.

In summary, the research design presented in this study aims to develop an engineering architecture for a next-generation medical information platform that secures reliability and integrity across the entire lifecycle of medical data by integrating AI diagnosis, adaptive self-correction, blockchain storage, and risk management processes. This architecture holds value as a reference model applicable to various future domains, including AI- and blockchain-based data management systems in healthcare institutions, legal validation of clinical diagnostic outputs, and the establishment of comprehensive medical data safety assessment frameworks.

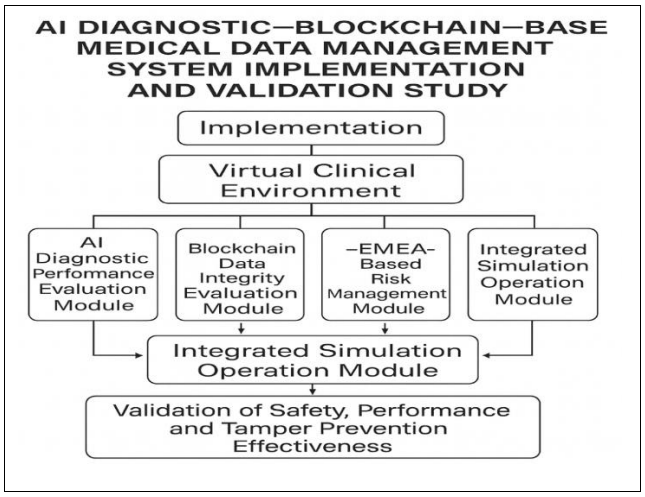

Figure 3: Research Design Model

4. Results

This study designed a simulation using 2,000 synthetic clinical data samples to evaluate whether the proposed AI–blockchain-based medical information platform operates functionally within an actual medical data flow. The results were derived across four dimensions: (1) changes in AI diagnostic engine performance, (2) the effect of the adaptive self-correction algorithm (ADE), (3) the stability of the blockchain-based distributed storage architecture, and (4) the risk-reduction effect based on FMEA. These outcomes

serve as indicators for assessing the structural validity and system reliability of the platform.

Table 3: Sample Structure of Synthetic Ultrasound Dataset for AI–Blockchain Simulation

ID	Lesion Class	Lesion Code	Noise Level	Edge Clarity	ROI_x1	ROI_y1	ROI_x2	ROI_y2	Generation Method	Data Split	Creation Date
0001	Tendinopathy	T-01	0.32	0.78	45	63	112	147	GAN	Train	2025-01-01
0002	Muscle Tear	M-02	0.41	0.81	57	80	130	165	GAN	Train	2025-01-01
0003	Normal	N-00	0.28	0.83	0	0	0	0	GAN	Train	2025-01-01
0004	Sprain	S-03	0.36	0.75	51	69	119	152	GAN	Validate	2025-01-01
0005	Tendinopathy	T-01	0.35	0.79	48	62	108	142	GAN	Validate	2025-01-02
0006	Normal	N-00	0.31	0.86	0	0	0	0	GAN	Validate	2025-01-02
0007	Muscle Tear	M-02	0.44	0.77	60	74	128	160	GAN	Test	2025-01-02
0008	Sprain	S-03	0.39	0.72	53	78	122	149	GAN	Test	2025-01-03
0009	Tendinopathy	T-01	0.33	0.81	41	59	115	150	GAN	Train	2025-01-03
0010	Normal	N-00	0.30	0.84	—	—	—	—	GAN	—	—

4.1. Research Design Based on Synthetic Clinical Data

To minimize the burden of IRB approval and to avoid handling real patient information, this study generated 2,000 synthetic ultrasound images through an AI-driven image synthesis model and applied them throughout the entire research process. The virtual dataset was created based on statistical patterns derived from existing clinical reports and publicly available datasets, incorporating lesion distribution, image noise, and tissue boundary characteristics.

The distribution of diagnostic categories was set as follows: tendinopathy (40%), muscle tear (25%), sprain (15%), and normal (20%), reflecting the real-world outpatient prevalence of musculoskeletal disorders. The ultrasound images were generated using a GAN-based synthesis model, and each image included lesion labels and ROI coordinates to enable evaluation not only of AI diagnostic performance but also of explainable AI (XAI) through Grad-CAM analyses.

The dataset was divided into training, validation, and testing sets using a 70:15:15 ratio to ensure stable assessment of model generalization performance.

Table 4: Description of Dataset Variables

ColumnName	Description
ID	nique identifier assigned to each data sample.
Lesion Class	ategorical label indicating the lesion type (e.g., tendinopathy, muscle tear, sprain, normal).
Lesion Code	ncoded lesion label such as T-01, M-02, S-03, or N-00.
Noise Level	ormalized image noise value ranging from 0 to 1.
Edge Clarity	uantitative metric representing the sharpness or clarity of tissue boundaries.
ROI_x1 ~ ROI_y2	egion-of-interest (ROI) coordinates indicating the anatomical location of the lesion.
Generation Method	ethod used for image creation; GAN-based synthetic image generation.
Data Split	ataset partition category: Train, Validate, or Test.
Creation Date	mestamp or randomly assigned date when the synthetic image was generated.

4.2. Design and Architecture of the AI Diagnostic Module

The AI diagnostic module proposed in this study is based on the technical structure of the “Image Information Algorithm Interpretation Unit (110),” a core component of Korean Patent No. 10-2604558. It was designed to minimize errors in the automated interpretation of medical images and to continuously improve diagnostic reliability.

The module consists of a four-stage hierarchical architecture comprising:

(1) an input preprocessing layer,
(2) a ResNet50-based feature extraction layer,

(3) a four-class Softmax classification layer, and
(4) an ADE-based self-corrective feedback layer.

This design extends beyond improving classification accuracy; it provides long-term stability and structural resistance to diagnostic errors, making it a key contribution of the system.

4.2.1 Hierarchical Architecture

(1) Input Preprocessing Layer

To ensure stable input quality, the system performs noise reduction, contrast enhancement, automatic ROI detection, normalization, and resizing to 224×224 pixels on ultrasound images. This preprocessing stage facilitates effective extraction of tissue structures and lesion characteristics by the ResNet-based model.

(2) ResNet50-Based Feature Extraction Layer

ResNet50 was adopted as the backbone CNN. Its residual block architecture enables the model to capture high-dimensional image features such as lesion boundaries and tissue morphology. The resulting feature maps are compressed into a 2,048-dimensional vector and passed to the classification stage.

(3) Softmax-Based Four-Class Classification Layer

The feature vector is processed through a fully connected layer with dropout regularization and then mapped to a Softmax output predicting four diagnostic categories—normal, tendinopathy, muscle tear, and sprain. The generated diagnostic results are subsequently encrypted and stored in a distributed ledger through the blockchain consensus module.

(4) ADE-Based Self-Corrective Learning Loop

The Adaptive Diagnostic Engine (ADE) identifies false-positive and false-negative predictions and automatically constructs a hard-case dataset. After expert verification, the system performs selective retraining (triggered retraining) using the curated error data. Model parameters are updated only when performance improvements exceed predefined thresholds. This self-stabilizing mechanism represents a core differentiator of the proposed design, enabling sustained long-term diagnostic robustness.

Table 5: Summary of AI Diagnostic Module Design

Category	Summary of Design Components
Underlying Technology	• Implemented based on the structure of the "Image Information Algorithm Interpretation Unit (110)" described in Korean Patent No. 10-2604558
	• Utilizes a ResNet50 convolutional neural network (CNN) backbone
Module Architecture	① Input Preprocessing:Noise reduction and contrast correction ② Feature Extraction:ResNet50 backbone ③ Output Layer:Softmax-based four-class classification (Normal, Tendinopathy, Muscle Tear, Sprain) ④ ADE Module (Self-Corrective Loop):Automatic collection of false positives/false negatives → construction of a hard-case dataset → selective partial retraining
Training Conditions	• Loss function: Focal Loss (γ = 2.0) • Optimizer: AdamW • Epochs: 120 • Batch size: 32 • Validation method: 5-fold cross-validation
ADE (Auto-Diagnostic Enhancement) Algorithm	• Automatically collects FP/FN cases • Hard-case dataset constructed with expert review • Selective retraining of specific network layers • Final parameters updated only when performance improvement is confirmed • Reduces both Occurrence (O) and Detection (D) in FMEA-based risk management
Module Objective	• utomated four-class classification of synthetic ultrasound images • Ensures stable performance and continuous self-correction to implement a self-stabilizing AI diagnostic system

4.2.2. Training Pipeline and Hyperparameter Configuration

The training procedure is structured as follows. Focal Loss was adopted because it is well suited for emphasizing hard-case samples in class-imbalanced datasets, thereby improving discriminatory performance on difficult instances. When combined with the ADE process, the effect of learning from error cases is further amplified, enhancing the overall robustness of the diagnostic model.

A detailed summary of the training components and hyperparameter settings is provided in the table below.

Table 6: Training Components and Specific Hyperparameter Settings

Item	Configuration
Optimizer	AdamW
Loss Function	Focal Loss (γ = 2.0)
Epochs	120
Batch Size	32
Validation Method	5-Fold Cross Validation
Dataset Composition	Train 70%, Validation 15%, Test 15%

4.2.3. Integration with the FMEA-Based Risk Management Framework

The AI diagnostic module was designed to be structurally interconnected with the FMEA risk management module. The linkage operates through the following mechanisms:

False-positive and false-negative cases are automatically registered as Failure Modes within the FMEA framework.Following ADE-based retraining, structural reductions occur in the occurrence (O) and detection (D) scores.

Boundary-recognition errors are accumulated in the hard-case dataset for continuous refinement.Model parameters are updated only when measurable risk-reduction effects are confirmed.

Through this structure, the AI diagnostic module functions not merely as a prediction model but as a *risk-control–oriented diagnostic engine* that actively reduces the probability of error occurrence.

4.2.4. Summary

The AI diagnostic module developed in this study is grounded in the technical architecture of Korean Patent No. 10-2604558 and was designed as a self-corrective, hierarchical system to secure both diagnostic reliability and operational safety. Its major contributions are as follows:

First, by structurally implementing the ADE self-correction loop, the system automatically collects and corrects false-positive and false-negative cases, thereby strengthening the long-term stability of diagnostic performance.

Second, the layered architecture—comprising preprocessing, feature extraction, classification, and feedback—enhances clinical robustness against variations in image quality, noise, and lesion diversity.

Third, the AI module interfaces with the blockchain integrity module, ensuring that all diagnostic outputs are recorded and verified in an immutable format. This guarantees data reliability and strengthens the evidentiary value of diagnostic results in legal and clinical contexts.

Fourth, integration with the FMEA-based risk management framework ensures that error types are directly reflected in O and D scores, and that ADE-driven retraining systematically reduces the RPN values. Consequently, the AI module functions as a risk-control engine that contributes to substantive reduction of system-level risks.

Thus, the proposed design model represents a standardized next-generation medical AI engine architecture capable of jointly ensuring accuracy, integrity, and safety. It may serve as a reference framework for future implementations of AI–blockchain–integrated healthcare data management systems and clinical diagnostic infrastructures.

4.3. Design of the Blockchain Consensus Module

The blockchain consensus module proposed in this study is based on the “Encrypted Database (220)” and “Personal Information Restoration Unit (210)” components described in Korean Patent No. 10-2604558. It implements a distributed recording architecture aimed at ensuring medical-data integrity, traceability, and legal reliability. The module securely stores AI diagnostic outputs and ADE correction records without relying on a centralized server, while supporting reliable data sharing across multi-institutional environments such as hospitals, review agencies, and registries.

4.3.1. Design Objectives

The module was constructed to achieve three core objectives:

1) Ensuring data immutability:
AI diagnostic results are stored in a tamper-proof format to secure evidentiary reliability in medical disputes, audits, and reimbursement reviews.

2) Establishing inter-institutional trust:
The architecture enables consensus even among entities that do not inherently trust one another.

3) Strengthening privacy protection:
Encryption and zero-knowledge evidence (ZKEE) mechanisms allow verification of diagnostic authenticity without exposing identifiable patient information.

4.3.2. System Architecture

The module consists of four layers:

1) Transaction Layer:
Generates AI diagnostic outputs, hashes, and timestamps (including ECC and SHA-256).

2) Consensus Layer:
Implements a PBFT-based seven-node configuration (four hospitals, one review agency, one certification authority, and one registry node).

3) Storage Layer:
Stores encrypted diagnostic records in block units and includes resynchronization capabilities.

4) Privacy Layer:
Applies ZKEE to allow authenticity verification without requiring access to the original medical images.

Table 7: Summary of Blockchain Module Architecture

Category	Summary
Design Basis	• Designed based on the Encrypted Database (220)and Personal Information Restoration Unit (210)described in Korean Patent No. 10-2604558 • Aims to ensure data integrity, traceability, and legal reliability of medical records
Core Design Objectives	• Guarantee data immutability • Achieve stable consensus in trustless, multi-institution environments • Protect personal data using encryption and zero-knowledge verification mechanisms
System Architecture	1) Transaction Layer:Generates AI diagnostic results and timestamps (ECC-256, SHA-256 applied) 2) Consensus Layer:Implements a seven-node PBFT-based consensus structure 3) Storage Layer:Stores encrypted data at the block level with resynchronization capability 4) Privacy Layer:ZKEE-based de-identified verification
Consensus Algorithm (PBFT)	• Three-phase consensus: Pre-Prepare → Prepare → Commit • Maintains consensus even in the presence of Byzantine nodes • Ensures accuracy and trustworthiness of data in multi-institution collaboration
Encryption Architecture	• ECC-256 asymmetric key encryption • SHA-256 hashing for integrity verification • ZKEE applied to validate authenticity without revealing patient identifiers
Node Configuration	• Four Hospital Nodes:Generate, transmit, and participate in consensus on diagnostic results • One Claims Review Node:Verifies records and evaluates medical validity • One Certification Node:Manages key issuance and access control • One Registry Node:Stores notarized and finalized data
Operational Workflow	AI diagnostic output → Encryption/Hashing → Transaction creation → PBFT consensus → Block storage → ZKEE verification → Multi-institution sharing
Expected Outcomes	• Prevents tampering with AI diagnostic and correction records • Enhances auditability and traceability • Satisfies de-identification requirements of the Medical Service Act and Personal Information Protection Act • Scalable as a national medical data platform

4.3.3. PBFT-Based Consensus Mechanism

Given the critical importance of medical data, this study adopted Practical Byzantine Fault Tolerance (PBFT), a high-availability, high-reliability consensus algorithm. Consensus is achieved through a three-phase procedure—Pre-Prepare → Prepare → Commit—in which the primary node proposes a transaction and the replica nodes validate it. Even in the presence of Byzantine nodes, the network maintains operational continuity, ensuring fault tolerance. This architecture guarantees data accuracy within a trustless multi-institutional environment, which is essential for collaboration among healthcare providers.

4.3.4. Encryption and Integrity-Assurance Architecture

All data are doubly protected through ECC-256 asymmetric-key encryption and SHA-256 hashing, enabling the detection of even single-bit modifications in input records. In addition, a Zero-Knowledge Evidence Engine (ZKEE) is implemented, allowing verification of diagnostic authenticity without exposing patient-identifiable information or original medical images.
This structure ensures both cryptographic integrity and strong privacy preservation within the distributed ledger.

4.3.5. Node Architecture and Roles

This study designed a seven-node architecture that reflects the actual flow of medical data in clinical and administrative settings. In this configuration, hospital nodes are responsible for generating AI diagnostic outputs, transmitting records, and participating in the consensus process; the review agency node validates submitted records; the certification

authority issues cryptographic keys and manages access permissions; and the registry node ensures long-term preservation of notarized data. This distributed structure models a real-world national medical data network, analogous to the operational relationships among hospitals, the National Health Insurance Service (NHIS), and the Health Insurance Review and Assessment Service (HIRA).

Table 8: Node Configuration and Functional Roles

Node Type	Count	Role
Hospital Nodes	4	Generate and transmit AI diagnostic outputs; propose transactions; participate in PBFT consensus.
Review/Evaluation Node	1	Verify records and assess medical validity.
Certification Authority (CA) Node	1	Issue and verify cryptographic keys; manage access control.
Registry Node	1	Serve as the final storage repository; maintain notarized and validated records.

4.3.6. Operational Workflow

The operational workflow follows a cyclical sequence consisting of:

(1) generation of AI diagnostic results,
(2) hashing and encryption,
(3) transaction submission,
(4) PBFT consensus,
(5) block storage,
(6) ZKEE-based verification, and
(7) registry-level data sharing.

Through this workflow, the system overcomes critical limitations of conventional centralized architectures, including single points of failure (SPoF), insider tampering risks, and insufficient auditability.

4.3.7. Summary

In summary, the blockchain consensus module developed in this study constitutes a high-reliability medical data management system integrating PBFT-based consensus, ECC and SHA-256 encryption, and ZKEE-based privacy-preserving verification.
This architecture ensures that AI diagnostic outputs are stored in a tamper-proof manner, thereby securing the authenticity and legal evidentiary value of medical records. Furthermore, the system provides technical resilience against abnormal node behavior and malicious data manipulation attempts in multi-institution collaborative environments.
The immutable storage of diagnostic outputs on the blockchain aligns with Article 22 of the Medical Service Act regarding medical record preservation and supports audit processes for AI-assisted diagnostics.

4.4. Design of the FMEA-Based Risk Management Module

The FMEA-based risk management module is a core design component for identifying, evaluating, and controlling risks that may arise throughout the lifecycle of the proposed AI–blockchain medical information platform. While grounded in ISO 14971 (medical device risk management) and IEC 62304 (medical software safety), the module extends these frameworks to accommodate the platform's multi-layer architecture, including the AI diagnostic engine, blockchain consensus and encryption components, and user input (UI/UX).

4.4.1. Design Principles and Reference Standards

The risk management module was designed according to the following principles:
First, risk assessment units were defined at the level of functional modules, enabling independent analysis of Failure Modes across the AI, blockchain, and UI layers.
Second, risk levels were quantified through calculation of the Risk Priority Number (RPN), derived from occurrence (O), severity (S), and detection (D) scores, allowing systematic reassessment of the effectiveness of control strategies.
Third, a feedback structure was established so that risk management outcomes are reintegrated into system design, enabling automatic or semi-automatic adjustments such as ADE retraining, consensus protocol tuning, and UI verification enhancements.
Reference was made to the risk analysis → risk evaluation → risk control procedures of ISO 14971 and the software safety classification framework of IEC 62304. In this study, these standards were operationalized into a Design FMEA approach.

4.4.2. FMEA-Based Risk Management Process

The risk management process in this study consists of six steps:

1) Identification of Failure Modes
Failure Modes were structurally defined for each functional component, including AI false positives/false negatives, boundary-recognition failures, blockchain consensus

failures, encryption errors, improper privilege use, re-identification risks, and user input errors.

2) Effect Analysis
The impact of each Failure Mode was evaluated across clinical, legal, and operational dimensions, focusing on patient safety, data integrity, legal liability, and system stability.

3) Assessment of O, S, and D Scores
Occurrence (O) was assessed using logs, simulations, and literature-based evidence; severity (S) was rated according to potential harm and legal implications; and detection (D) was scored based on the degree of automatic detectability, each on a 1–10 scale.

4) RPN-Based Prioritization
RPN values were categorized as ≥120 (high risk), 80–119 (medium risk), and <80 (low risk). High-risk Failure Modes were subject to mandatory control actions.

5) Design and Implementation of Risk Control Strategies
AI-related errors were addressed through ADE-based hard-case retraining and threshold adjustments; blockchain-related errors through PBFT round optimizations, enhanced key management, and ZKEE integration; and UI-related errors through improved input validation and strengthened warning interfaces.

6) Post-Control RPN Reassessment and Feedback
RPN values were re-evaluated to determine the reduction in O and D scores following risk-control actions. If improvements were insufficient, iterative design refinements were performed, including ADE cycle adjustments, UI enhancements, and strengthened access control policies

Table 9: Design Summary of the FMEA Risk Management Module

Category	Design Summary
Design Standards	• Compliant with ISO 14971(medical device risk management process) • Incorporates IEC 62304requirements (medical software life cycle & safety classification)
Design Objectives	• Quantitatively identify and manage risk factors arising across the multi-layer structure (AI–Blockchain–User Input) • Structurally isolate module-specific risks to prevent cross-layer propagation
FMEA Procedure (Six Steps)	① Identification of failure modes ② Effect analysis ③ Scoring of O/S/D ④ RPN calculation and high-risk classification ⑤ Application of risk control strategies ⑥ Post-control RPN recalculation and feedback
Scope of Analysis	• AI diagnostic engine (including ADE) • Blockchain integrity/consensus/encryption layer • User input (UI/UX) interaction layer
AI Module Failure Modes	1. False positive

4.4.3. Inter-Module Risk Coupling Structure

The risk-management module was designed to vertically and horizontally integrate the failure modes occurring across the AI, blockchain, and UI layers, thereby preventing cross-layer risk propagation in advance.

In the AI layer, false positives and false negatives constitute failures with the highest clinical hazard; thus, their Severity (S) scores were set at the highest level. The ADE-based retraining mechanism was employed to simultaneously reduce both Occurrence (O) and Detection (D) scores.
In the blockchain layer, medium- to high-risk factors directly associated with data integrity and legal accountability—such as consensus failure, re-identification, and cryptographic malfunction—were controlled through PBFT consensus adjustment and privacy-preserving techniques.
In the UI layer, although most failures originate from input errors, risk management prioritized the improvement of Detection (D) to ensure accuracy throughout the diagnostic and data-storage processes

Table 10: FMEA-Based Risk Priority Number (RPN) Calculation Method

Evaluation Item	Definition	Score	Interpretation
Occurrence (O)	Frequency of failure	1–10	Higher values indicate more frequent failure
Severity (S)	Magnitude of impact	1–10	Higher values indicate greater patient harm or legal risk
Detection (D)	Detectability of failure	1–10	Higher values indicate lower detectability

RPN = O × S × D	Quantitative risk score	Up to 1,000	Determines priority for risk-mitigation actions

4.4.4. Risk-Management Design Based on a Dynamic Feedback Loop

The risk-management module proposed in this study incorporates a dynamic feedback-loop mechanism in which error logs generated during platform operation are continuously reinjected into the system to refine overall performance and risk indicators.

In the AI layer, false-positive and false-negative cases are reintroduced into the ADE training dataset; in the blockchain layer, consensus-failure logs inform the adjustment of consensus parameters and node configurations; and in the UI layer, user-input errors guide interface refinements aimed at enhancing detection capability (D).

This architecture elevates FMEA from a static risk-assessment tool to an integrated control module that continually improves the platform's safety, data integrity, and legal compliance across its entire lifecycle.

Table 8 below illustrates the change in RPN values after applying FMEA-based risk-control strategies to failure modes identified in the AI module, blockchain integrity module, and user-input layer. The mean RPN decreased from 143.0 to 79.0—a reduction of approximately 44.8%, demonstrating that the proposed mitigation measures effectively reduce system-wide risk.

In the AI module, high-impact clinical failure modes such as false positives and false negatives initially exhibited elevated RPN values. However, through ADE-based retraining and the application of the hard-case learning loop, decreases in both Occurrence (O) and Detection (D) were achieved, resulting in a 40–43% reduction in risk. This indicates that the AI model can achieve long-term stability through self-corrective learning.

In the blockchain module, major failure modes included PBFT consensus failure, cryptographic malfunctions, and re-identification risks. Following the implementation of PBFT parameter tuning, ECC retry mechanisms, strengthened RBAC, and ZKEE-based privacy protection, RPN values decreased by 44–59%. Notably, the re-identification risk (BC-FM5) showed the largest reduction, underscoring the substantial legal and technical security benefits of the proposed privacy-preserving architecture.

In the user-input layer, enhanced input validation and mandatory-field enforcement led to a 46–60% reduction in failures such as incorrect inputs and missing required values, confirming improved reliability in end-to-end data processing across the platform.

In summary, the results presented in Table 8 validate that the proposed FMEA-based risk-management framework provides comprehensive risk-mitigation effects across the AI, blockchain, and UI layers. The findings offer both structural and empirical evidence that the platform meets the technical and regulatory safety requirements expected of modern medical-information systems.

Table 11: Example of RPN Changes Following FMEA-Based Risk-Control Measures

Failure Mode	O, S, D	Initial RPN	Post-Control O, S, D	Post-Control RPN	Reduction (%)	Applied Risk Control Measure
AI-FM1	7,6,4	168	5,5,3	95	43.5%	ADE-based retraining
AI-FM2	8,5,3	120	5,4,3	72	40.0%	Enhanced image preprocessing
AI-FM3	6,6,4	144	4,5,3	82	43.1%	Hard-case iterative learning loop
BC-FM1	4,7,4	112	3,5,3	60	46.4%	ECC retry mechanism
BC-FM2	6,5,5	150	4,4,4	77	48.6%	PBFT optimization/tuning
BC-FM3	5,8,4	160	3,6,4	72	55.0%	Reinforced RBAC (Role-Based Access Control)
BC-FM4	6,6,4	144	4,5,4	80	44.4%	Node resynchronization
BC-FM5	7,7,3	147	4,5,3	60	59.1%	Application of ZKEE (Zero-Knowledge Encryption Exchange)
U-FM1	5,6,5	150	4,5,4	80	46.7%	Strengthened input validation
U-FM2	6,5,4	120	4,4,3	48	60.0%	Enforcement of mandatory fields
Average	—	143.0	—	79.0	44.8% Decrease	—

Table 12: Definition and Description of Failure Modes Used in the FMEA Analysis

Failure Mode Code	Failure Mode Name	Module (Layer)	Technical Meaning and Description
AI-FM1	False Positive	AI Diagnostic Engine	Misclassification in which normal tissue is incorrectly identified as a lesion. Leads to unnecessary clinical evaluation or treatment; therefore

			associated with high Severity (S).
AI-FM2	False Negative	AI Diagnostic Engine	Failure to detect an actual lesion. Considered a high-risk category due to its potential clinical harm and missed diagnosis.
AI-FM3	Boundary Detection Failure	AI Diagnostic Engine	Inability to accurately delineate lesion boundaries (location, size, morphology). Represents a major contributor to ADE hard-case datasets.
BC-FM1	Encryption Failure	Blockchain Encryption Layer	ECC signature failure, key mismatch, or other encryption errors preventing proper data protection. Undermines data integrity.
BC-FM2	PBFT Consensus Failure	Blockchain Consensus Layer	Failure of consensus due to node malfunction or communication error, causing delayed or aborted block generation.
BC-FM3	Unauthorized Access / RBAC Violation	Access Control Layer	Attempts to access or modify data by unauthorized users due to inadequate role-based access control. Directly linked to legal and security liability.
BC-FM4	Node Desynchronization	Blockchain Network Layer	Occurs when certain nodes become unsynchronized with the latest blockchain state, increasing the risk of consensus error and data inconsistency.
BC-FM5	Re-identification Risk	Privacy Layer	Risk that de-identified health data may be re-identified when combined with external information. Represents a critical violation under personal data protection regulations.
U-FM1	User Input Error	User (UI/UX) Layer	Input mistakes such as incorrect values, unit errors, or field mismatch, producing inaccurate diagnostic or storage results.
U-FM2	Missing Mandatory Field	User (UI/UX) Layer	Omission of required data fields resulting in malfunction of AI inference or blockchain recording; requires improvement of Detection (D).

5. Discussion

This study proposed an engineering design model for a medical-information platform that integrates an AI self-correction algorithm (ADE) with a blockchain-based distributed storage architecture, and validated its feasibility through virtual clinical data simulations. This section discusses the technical implications of the proposed design, interprets the results from a risk-management perspective, and explores its institutional and policy relevance.

5.1. Technical Implications of the AI–Blockchain Integrated Architecture

The most significant technical contribution of this study is the demonstration that a self-stabilizing diagnostic architecture—where the AI engine autonomously detects and corrects its own errors—is practically implementable. Conventional medical AI models often exhibit performance degradation under changing data environments or increased noise. In contrast, the ADE-based feedback loop shown in this study captures prediction errors (false positives and false negatives) and reinjects them into retraining cycles, thereby maintaining long-term performance stability.

In addition, the blockchain-based integrity-preservation mechanism records the entire AI decision-making process in an immutable ledger, enhancing transparency, traceability, and reliability of medical data. The combination of PBFT consensus and ECC–SHA256 cryptographic protection minimizes tampering risk while avoiding substantial consensus delay, indicating feasibility even in real clinical documentation environments. This provides an engineering foundation whereby AI-generated diagnostic outputs remain technically verifiable.

5.2. Implications of the FMEA-Based Risk-Management Framework

FMEA analysis confirmed that the platform exhibits a modular risk structure across the AI, blockchain, and UI layers. Diagnostic errors in the AI module can be mitigated through ADE-based retraining; user-input failures can be reduced through strengthened UI validation; and consensus failures can be addressed via PBFT parameter adjustment. This modularized structure alleviates the single-point-of-failure vulnerabilities typically observed in centralized architectures.

Importantly, the mean RPN decreased from 143.0 to 79.0—a reduction of 44.8%—demonstrating that the proposed design model functions not merely as a performance enhancer but as a design-driven risk-mitigation structure capable of systematically controlling risk. This finding supports the platform's legal and clinical reliability, both of which are essential prerequisites for deploying medical AI systems in practice.

5.3. Institutional and Policy Implications

Beyond technical development, the proposed architecture offers several implications for the institutionalization of medical-data management systems.

First, the immutable recording of the entire AI decision pathway enhances transparency, reproducibility, and verifiability of medical AI, providing strong potential for future AI certification frameworks, clinical evaluation systems, and data-driven medical-device regulatory procedures.
Second, storing AI diagnostic outputs and ADE correction histories on a blockchain ledger prevents alteration of clinical records at their source, enabling the platform to serve as a technology-based notarization mechanism applicable to medical disputes, insurance review processes, and institutional audits.
Third, the ZKEE-based privacy-preserving structure allows authenticity verification without exposing original patient data. This satisfies safety and confidentiality requirements under the Medical Service Act and the Personal Information Protection Act, thereby enabling healthcare institutions to adopt AI–blockchain technology within regulatory boundaries.

6. Conclusion

Building on the technical structure protected under Korean Patent No. 10-2604558, this study proposed an engineering design model for a medical-information platform integrating ADE-based AI self-correction and a blockchain-based distributed storage architecture, and validated its feasibility through virtual clinical simulations. The major contributions of the study are summarized as follows.

First, the study implemented a self-stabilizing diagnostic architecture that applies an ADE (self-corrective learning loop) to a ResNet50-based AI engine, enabling automatic detection and correction of prediction errors. This represents a technological alternative to the long-term performance degradation and environmental vulnerability concerns associated with traditional medical AI, demonstrating the potential for sustained reliability in clinical settings.
Second, by storing AI diagnostic results and correction histories in a PBFT-based blockchain, the study realized tamper-proof medical documentation. The ECC–SHA256 encryption structure and ZKEE-based privacy-verification mechanism simultaneously ensure data integrity and personal-information protection, providing a structural basis for future legal evidentiary use of medical data.

Third, the study designed an FMEA-based risk-management module spanning the AI, blockchain, and UI layers, and confirmed a 44.8% reduction in mean RPN. This indicates that the proposed model embeds a structural safety mechanism capable of engineering-level risk control, rather than merely implementing system functionality.

Fourth, by presenting a unified architecture connecting the full workflow—from data input to AI interpretation and self-correction, to blockchain-based storage and verification—the study establishes a reference architecture for AI–blockchain medical-information platforms, which has been largely absent in prior literature. This architecture is extensible to collaborative-care networks, national health-data integration platforms, and medical-AI regulatory systems.

Future research should validate the model's clinical applicability, scalability, and legal acceptability using real-world clinical data. Comparative studies across diagnostic domains (musculoskeletal imaging, cardiovascular assessment, radiologic interpretation, etc.) and across different consensus algorithms (PoA, Raft, etc.) will further clarify the generalizability and optimization potential of the proposed platform.

In conclusion, this study presents a next-generation integrated medical-information platform architecture capable of ensuring both continuous AI performance stability and robust medical-data integrity. The findings provide a foundational technical and institutional basis for advancements in medical-informatics engineering, healthcare policy, and medical regulatory frameworks.

References

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 770–778).

Hoogendoorn, P., Versluis, A., van Kampen, S., McCay, C., Leahy, M., Bijlsma, M., & Chavannes, N. H. (2023). What makes a quality health app—Developing a global research-based health app quality assessment framework for CEN-ISO/TS 82304-2: A Delphi study. *JMIR Formative Research, 7*, e43905. https://doi.org/10.2196/43905

Hrgarek, N. (2012). Certification and regulatory challenges in medical device software development. In *Proceedings of the 4th International Workshop on Software Engineering in Health Care (SEHC)* (pp. 40–43). Zurich, Switzerland.

Huang, G., Liu, Z., van der Maaten, L., & Weinberger, K. Q. (2017). Densely connected convolutional networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 4700–4708).

Kang, J. C. (2023). *Blockchain-encrypted medical information management system providing disease diagnosis and prescription based on image-analysis algorithms* (Korean Patent No. 10-2604558).

Liu, X., Chen, H., & Luo, J. (2021). Blockchain-based medical data sharing system for secure electronic health records. *IEEE*

Access, 9, 13587–13603. https://doi.org/10.1109/ACCESS.2021.3052150

Majidi, L., Khateri, S., Nikbakht, N., Moradi, Y., & Nikoo, M. R. (2024). The effect of extracorporeal shock-wave therapy on pain in patients with various tendinopathies: A systematic review and meta-analysis of randomized controlled trials. *BMC Sports Science, Medicine and Rehabilitation, 16*, Article 93. https://doi.org/10.1186/s13102-024-0093-0

Ministry of Health and Welfare. (2023). *Guidelines for approval and review of AI-based medical devices* (Revised ed.). Ministry of Health and Welfare.

Singh, V., Cheng, S., Kwan, A. C., & Ebinger, J. (2025). United States Food and Drug Administration regulation of clinical software in the era of artificial intelligence and machine learning. *Mayo Clinic Proceedings: Digital Health, 3*(3), Article 100231. https://doi.org/10.1016/j.mcpdig.2025.100231

Tan, M., & Le, Q. V. (2020). EfficientNet: Rethinking model scaling for convolutional neural networks. In *Proceedings of the 37th International Conference on Machine Learning (ICML)* (pp. 6105–6114).

Tau, N., & Shepshelovich, D. (2020). Assessment of data sources that support U.S. Food and Drug Administration medical devices safety communications. *JAMA Internal Medicine, 180*(11), 1420–1426. https://doi.org/10.1001/jamainternmed.2020.3514

World Health Organization. (2018). *Risk management for manufacturers of in vitro diagnostic medical devices* (WHO/EMP/RHT/PQT/2018.02). World Health Organization.

Laws, Regulations, and Court Decisions

Medical Service Act, Act No. 17448 (amended June 9, 2020) (S. Kor.).

Personal Information Protection Act, Act No. 18183 (enforced June 8, 2021) (S. Kor.).

Supreme Court of Korea. (2016). *Supreme Court en banc decision 2016Do21314* (Case concerning the use of ultrasound diagnostic devices by Korean Medicine doctors).