High-Level Design Report

1. Introduction

1.1 Purpose of the system

The purpose of this system is to develop a web-based medical support platform that leverages artificial intelligence to assist healthcare professionals and patients in the diagnostic process. The system aims to enhance diagnostic accuracy, accelerate clinical decision-making, and enable early detection of critical diseases. It achieves this through AI-driven image analysis for physicians and natural language processing for patient symptom interpretation. While supporting both user types, the system maintains a strict ethical framework emphasizing that final medical decisions rest solely with licensed professionals.

1.2 Design goals

- Accuracy and Reliability: Achieve diagnostic accuracy above 90% and maintain a False Negative Rate below 5% for critical illnesses.
- Ethical and Legal Compliance: Ensure full compliance with GDPR, KVKK, and HIPAA regulations. Guarantee 100% disclaimer coverage for all patient-facing outputs.
- Performance and Responsiveness: Deliver medical image results within 10 seconds and patient symptom-based outputs within 5 seconds.
- Data Privacy and Security: Implement encryption for all stored data, apply role-based access control, and ensure secure API communication.
- Usability and Accessibility: Provide intuitive, role-specific dashboards for doctors and patients with bilingual (Turkish and English) support.
- System Availability: Maintain at least 99.5% uptime through cloud-based deployment with continuous monitoring.
- Ethical AI Interaction: Filter anxiety-inducing or misleading content in patient interactions with a moderation accuracy of at least 95%.

1.3 Definitions, acronyms, and abbreviations

- AI: Artificial Intelligence
- LLM: Large Language Model
- CNN: Convolutional Neural Network
- FNR: False Negative Rate
- FPR: False Positive Rate
- GDPR: General Data Protection Regulation

- KVKK: Kişisel Verilerin Korunması Kanunu (Turkish Personal Data Protection Law)
- HIPAA: Health Insurance Portability and Accountability Act
- RBAC: Role-Based Access Control
- UI: User Interface
- NLP: Natural Language Processing
- REST API: Representational State Transfer Application Programming Interface

1.4 Overview

The proposed system is a hybrid AI-based medical support platform integrating computer vision and natural language processing to assist doctors and patients. Doctors can upload and analyze medical images, view AI-supported results, and access patient histories, while patients can describe symptoms in natural language and receive simplified, safe, and ethically filtered feedback.

The platform operates as a decision-support system—not as an autonomous diagnostic tool—to ensure ethical and professional use. It is deployed on cloud infrastructure with GPU acceleration to handle deep learning inference efficiently. Overall, the system bridges the gap between AI-driven diagnostics and responsible clinical practice.

2. Current software architecture (if any)

At the current stage of development, no fully implemented software architecture exists. The system is still in the design and planning phase, where architectural components, module boundaries, and technology selections are being defined.

3. Proposed software architecture

3.1 Overview

The system adopts a multi-tier architecture consisting of three primary layers:

1. Frontend Layer: Provides distinct interfaces for doctors and patients. Developed using modern web technologies, it communicates securely with backend services through RESTful APIs.
2. Backend Layer: Handles authentication, business logic, data processing, and model orchestration. It acts as a bridge between the frontend, databases, and AI inference services.

3. AI Inference Layer: Hosts machine learning models for both image-based and text-based analysis. This layer includes separate models for each diagnostic task and integrates with external APIs for LLM-based reasoning.
4. Database Layer: Stores encrypted user data, image metadata, interaction logs, and feedback reports. It supports auditing, uptime monitoring, and model traceability.

All layers communicate through secure HTTPS channels and incorporate logging and monitoring mechanisms to ensure traceability, reliability, and compliance with medical data protection laws.

3.2 Subsystem decomposition

1. User Management Subsystem
    - Handles authentication, role-based access, and session control.
    - Differentiates privileges between doctors and patients.

2. Image Processing Subsystem
    - Manages upload, preprocessing, and inference of medical images (X-ray, CT, MRI, ultrasound).
    - Integrates with deep learning models trained on specific datasets (e.g., lung, brain, general X-ray).

3. Symptom Analysis Subsystem
    - Utilizes LLMs for processing natural language symptom inputs.
    - Generates simplified, safe, and ethically constrained health suggestions.

4. Data Security and Compliance Subsystem
    - Encrypts all stored and transmitted data.
    - Ensures GDPR, KVKK, and HIPAA compliance through anonymization and secure key management.

5. Feedback and Moderation Subsystem
    - Allows doctors to provide structured feedback on AI outputs.
    - Applies content moderation to detect and filter misleading or inappropriate model outputs.

6. Monitoring and Logging Subsystem
    - Records all user activities, AI inferences, and feedback actions for traceability.
    - Provides dashboards for uptime monitoring and performance analytics.

7. Localization and UI Subsystem

- Manages multilingual text content and ensures full translation coverage.
- Tailors the interface layout and accessibility for different user roles.

3.3 Hardware/software mapping

The AI Health System is designed to operate on a cloud-based infrastructure that supports scalable computation, secure data handling, and high availability. The mapping between hardware resources and software components is structured to ensure efficient execution of AI workloads while maintaining compliance with healthcare data protection requirements.

The frontend layer runs entirely on client-side hardware, requiring only a modern web browser on desktop, tablet, or mobile devices. No specialized hardware or local installation is required for end users. All computationally intensive tasks are offloaded to backend and AI inference services to ensure usability for patients and doctors regardless of device capabilities.

The backend services are deployed on cloud-based virtual machines or container orchestration platforms. These services handle authentication, role-based access control, business logic, request orchestration, and secure communication with databases and AI services. Backend instances are hosted on CPU-based nodes with autoscaling enabled to support concurrent users and maintain system responsiveness.

The AI inference layer is mapped to GPU-enabled cloud instances to support deep learning workloads efficiently. Image-based diagnostic models (CNNs for X-ray, CT, MRI, and ultrasound analysis) run on dedicated GPU resources to meet strict performance requirements (≤10 seconds inference time). NLP and LLM-based symptom analysis may run on either GPU or optimized CPU instances depending on model size and latency constraints, with external API integration where applicable.

The database layer is deployed on managed cloud database services. Relational databases are mapped to persistent storage volumes optimized for transactional integrity, while NoSQL databases are mapped to scalable storage for chatbot sessions, logs, and feedback data. All storage resources are encrypted at rest and replicated to ensure fault tolerance.

This hardware/software mapping ensures separation of concerns, scalability, and reliable performance while supporting secure medical data processing and AI-assisted diagnostics.

3.4 Persistent data management

Persistent data management in the AI Health System is designed to ensure data integrity, security, traceability, and compliance with medical data protection regulations such as

GDPR, KVKK, and HIPAA. The system adopts a layered data storage strategy tailored to different data types and access patterns.

Medical imaging data is stored in secure cloud object storage systems. Images are stored in standardized formats along with associated metadata such as acquisition time, modality type, and anonymized patient identifiers. Access to raw images is restricted to authorized doctor accounts, and all retrieval operations are logged for auditing purposes.

Structured application data, including user profiles, roles, access permissions, diagnosis summaries, and report metadata, is stored in a relational database. This ensures strong consistency, referential integrity, and reliable transaction management. All sensitive fields are encrypted, and personally identifiable information (PII) is minimized and anonymized where possible.

Unstructured and semi-structured data, such as chatbot interactions, symptom descriptions, user feedback, and moderation logs, are stored in a NoSQL database. This approach supports flexible schemas and efficient handling of multi-turn conversational data while maintaining scalability and performance.

To ensure data durability and recoverability, regular automated backups are performed, and versioning mechanisms are applied to critical datasets and model-related metadata. Audit logs capturing data access, AI inference requests, and administrative actions are retained for traceability and compliance verification.

Data lifecycle management policies define retention periods, archival rules, and secure deletion procedures in accordance with legal and ethical requirements. By separating storage concerns and enforcing strict access control, the system ensures that persistent data remains secure, consistent, and usable throughout the system's operational lifecycle.

3.5 Access control and security

The system enforces strict access control mechanisms to ensure that sensitive medical data is only accessible to authorized users. A role-based access control (RBAC) model is implemented, separating system privileges between doctors and patients. Doctors are granted access to detailed diagnostic outputs, medical images, and explainability features, while patients are restricted to simplified and non-alarming information.

Secure authentication mechanisms are used to prevent unauthorized access, including strong password policies and optional multi-factor authentication for medical professionals. All access to patient data and AI-generated outputs is logged for audit and traceability purposes. In addition, all stored and transmitted data is protected using industry-standard encryption techniques to ensure confidentiality, integrity, and compliance with healthcare data protection regulations.

3.6 Global software control

The AI Health System follows a centralized software control approach managed by the backend application layer. All user interactions, including image uploads and symptom submissions, are first processed by this central controller, which is responsible for authentication, role verification, input validation, and request routing. Subsystems do not communicate directly with each other; instead, all coordination is performed through the backend to ensure controlled execution and system consistency.

During operation, the central control mechanism manages the sequence of AI inference, confidence evaluation, ethical filtering, and result presentation. Outputs are generated according to predefined safety rules and user roles, ensuring that patient-facing information remains simplified while doctor-facing information provides detailed analytical support. This global control structure guarantees predictable behavior, traceability, and safe integration of artificial intelligence within the healthcare environment.

3.7 Boundary conditions

Boundary conditions define how the system behaves under exceptional, startup, shutdown, and failure-related situations. These conditions are critical to ensure system stability, safety, and predictable operation, especially in a healthcare-oriented environment.

3.7.1 System Startup

When the system starts, the following conditions apply:

- Core backend services shall initialize before user access is permitted.
- Security and authentication services shall be activated prior to any data interaction.
- AI inference services shall be registered and health-checked before accepting analysis requests.
- If any critical service is unavailable during startup, the system shall remain in restricted mode until recovery.

3.7.2 System Shutdown

During planned or unplanned shutdowns:

- Active user sessions shall be terminated safely.
- Ongoing AI inference requests shall be completed if possible or gracefully canceled.

- No partial or inconsistent data shall be stored.
- Users shall be informed if services become unavailable.

3.7.3 Invalid Input Conditions

The system shall handle invalid or incomplete inputs safely:

- Unsupported image formats shall be rejected.
- Empty or ambiguous symptom descriptions shall trigger clarification requests.
- Input validation shall occur before any AI inference is initiated.

3.7.4 AI Service Unavailability

If AI inference services are unavailable due to system load, network failure, or maintenance:

- The system shall not attempt to generate speculative outputs.
- Users shall receive a clear notification indicating temporary unavailability.
- No cached or outdated AI results shall be reused.
- Core system access shall remain functional.

3.7.5 Low Confidence or Uncertain Results

When AI model confidence falls below predefined thresholds:

- Results shall be suppressed or marked as inconclusive.
- Patient-facing outputs shall avoid medical interpretation.
- Doctors shall be informed of uncertainty through confidence indicators.
- The system shall recommend professional evaluation without suggesting diagnoses.

3.7.6 Network and Connectivity Failures

In case of network interruption:

- User actions shall not result in data corruption.
- Partial uploads shall be discarded safely.
- The system shall prompt users to retry once connectivity is restored.
- No sensitive data shall be transmitted without secure connection validation.

3.7.7 Security-Related Boundary Conditions

If unauthorized access or suspicious activity is detected:

- The system shall immediately restrict access.
- Relevant sessions shall be terminated.
- Events shall be recorded in audit logs.

3.7.8 Emergency and Safety Constraints

Under all boundary conditions:

- The system shall prioritize patient safety.
- No autonomous medical decisions shall be produced.
- The system shall consistently emphasize that AI outputs are supportive only.
- Final responsibility shall always remain with licensed healthcare professionals.

4. Subsystem services

This section describes the major subsystems of the AI Health System and the services each subsystem provides. The purpose is to define responsibilities and interactions at a high level, without specifying implementation details.

4.1 User Interface Subsystem

The User Interface Subsystem provides all interaction mechanisms between users and the system.

Provided services:

- Role-specific interfaces for doctors and patients
- Secure login and session handling
- Medical image upload interfaces for doctors
- Symptom input forms for patients
- Visualization of AI-generated results
- Display of confidence information and disclaimers
- Language selection between Turkish and English

This subsystem focuses on usability, clarity, and safe presentation of medical information.

4.2 Authentication and Authorization Subsystem

This subsystem manages identity verification and access control.

Provided services:

- User authentication
- Role-based access control enforcement
- Session validation and expiration handling
- Prevention of unauthorized data access

It ensures that users can only access system functions and information appropriate to their assigned role.

4.3 AI Inference Subsystem

The AI Inference Subsystem is responsible for executing artificial intelligence models.

Provided services:

- Medical image analysis using deep learning models
- Symptom interpretation using NLP-based models
- Confidence score generation
- Model selection based on input type
- Safe handling of low-confidence predictions

This subsystem operates strictly as a decision-support mechanism.

4.4 Data Management Subsystem

The Data Management Subsystem handles storage and retrieval of system data.

Provided services:

- Secure storage of uploaded medical images
- Management of analysis results and metadata
- Storage of user interaction history

All stored data follows encryption and access control policies.

4.5 Ethical Filtering and Moderation Subsystem

This subsystem ensures responsible and safe AI usage.

Provided services:

- Filtering of patient-facing outputs
- Removal of alarming or speculative medical language
- Enforcement of medical disclaimers
- Suppression of uncertain or high-risk interpretations

It plays a central role in preventing patient anxiety and misuse of AI outputs.

4.6 Logging and Audit Subsystem

The Logging and Audit Subsystem supports transparency and traceability.

Provided services:

- Recording system actions and user activities
- Logging AI inference requests and responses
- Monitoring abnormal system behavior

Logs are protected from unauthorized modification.

4.7 System Monitoring and Maintenance Subsystem

This subsystem supports operational reliability.

Provided services:

- Health monitoring of core services
- Detection of service failures
- Performance tracking
- Support for maintenance and recovery operations

It ensures continuous system availability.

4.8 Subsystem Interaction Overview

Subsystems interact through controlled and secure communication channels. User requests flow from the interface layer to backend services, AI inference modules, and data management components before returning filtered and role-appropriate outputs.

This layered interaction model supports scalability, maintainability, and safe system operation.

5. Glossary

AI Inference: Execution of AI models to generate results.

Architecture: Overall system structure and organization.

Boundary Conditions: System behavior under abnormal or exceptional cases.

Centralized Control: Control managed by a single coordinating component.

Confidence Score: Degree of certainty of AI output.

Data Management: Storage and handling of system data.

Decision-Support System: System assisting human decision-making.

Ethical Filtering: Restriction of unsafe or alarming outputs.

High-Level Design (HLD): Design phase defining system structure and responsibilities.

Medical Image: Diagnostic images such as X-ray, CT, or MRI.

Monitoring: Observation of system health and performance.

RBAC: Role-based access control.

Reliability: Ability to operate consistently.

Scalability: Ability to handle increased load.

Subsystem: Major functional component of the system.

6. References

Sommerville, I. (2020). Software Engineering (10th ed.). Pearson Education.

Pressman, R. S., & Maxim, B. R. (2020). Software Engineering: A Practitioner's Approach (9th ed.). McGraw-Hill.

Bass, L., Clements, P., & Kazman, R. (2021). Software Architecture in Practice (4th ed.). Addison-Wesley.

Gaur, L., & Bhatnagar, V. (2023). AI-enabled healthcare systems: Architecture, challenges, and design considerations. IEEE Access, 11, 23765–23780.

Microsoft Azure. (2024). Architectural best practices for cloud-based AI applications. https://learn.microsoft.com/azure/architecture/

European Parliament. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

U.S. Department of Health & Human Services. (1996). Health Insurance Portability and Accountability Act (HIPAA).

T.C. Resmî Gazete. (2016). Kişisel Verilerin Korunması Kanunu (KVKK), Kanun No: 6698.

ISO/IEC 27001:2022. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.