Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 3, pp. 1521–1540
DOI : 10.47974/JDMSC-2631

AI-based electronic health record architecture for secure patient data and its analytics

Dinesh Goyal *
Department of Creative Technologies and Product Design
School of Innovative Design and Management
National Taipei University of Business
New Taipei City
Taiwan (R.O.C.)

and

Department of Computer Science & Engineering & Technology
Poornima Institute of Engineering & Technology
Jaipur
Rajasthan
India

Sheng-Lung Peng †
Department of Creative Technologies and Product Design
School of Innovative Design and Management
National Taipei University of Business
New Taipei City
Taiwan (R.O.C.)

Abstract

Electronic Health Records (EHRs) are critical components of modern healthcare systems, but ensuring data security, privacy, and real-time clinical decision-making remains a significant challenge. This study proposes an advanced AI-based EHR architecture that prioritizes secure patient data while delivering intelligent clinical analytics. Homomorphic Encryption (CKKS), Attribute-Based Encryption (ABE) for fine-grained access control, and Hyperledger Fabric for blockchain-based audit records are some of the security features that are built into the system. Differential Privacy (DP-SGD) is used to make privacy even stronger when AI models are being trained. It uses an AI engine that can analyse medical transcripts using Convolutional Neural Networks (CNNs) for image-based detection (X-ray, MRI)

* *E-mail:* **dinesh8dg@gmail.com; (Corresponding Author)**
dinesh.goyal@poornima.org
† *E-mail:* **slpeng@ntub.edu.tw**

© Taru Publications

and advanced signal processing models for reading ECG and EEG data. This AI-powered system works with different types of data and uses models like ClinicalBERT, GatorTron, GRU-D, and LightGBM to handle medical pictures, bodily signs, time-series vitals, and clinical notes. Experimental results demonstrate that the proposed architecture achieves low encryption latency (920 ms), zero access control breaches, and excellent predictive accuracy (AUC-ROC up to 0.96). This comprehensive approach demonstrates that integrating AI with robust security protocols, and multimodal medical analysis can deliver a scalable, privacy-preserving EHR solution suitable for real-world healthcare environments. The framework can further be extended with use of more safe APIs to collect real-time data from Internet of Medical Things (IoMT) devices and Digital Twin-based monitoring systems. That will help healthcare practitioners to keep an eye on patients all the time and treat accordingly, with use of our AI-Engines and secure Data of patients using blockchain will become a EHR where health data that is 100% tracked and analysed for better healthcare services, across multiple institutions.

Subject Classification: *68M25, 68Txx, 94A62.*

Keywords: *AI in healthcare, Electronic health records, Homomorphic encryption, Clinical decision support, Blockchain, Patient privacy, AI in security.*

1. Introduction

Electronic Health Records (EHRs) are now the most important part of digital healthcare infrastructure. They store both organised and unstructured data in places that make clinical processes more efficient, allow for long-term patient tracking, and help doctors make decisions based on data. Even with these benefits, current EHR systems have big problems with data protection, security, being able to work with other systems, and helping people make decisions in real time. As more things go digital and people utilise the cloud platforms, it's easier for hackers to get to patient data or for others who shouldn't be able to get to it to do so. A lot of electronic health record (EHR) systems still employ old-fashioned encryption techniques that don't gel well with the high-level computation required in real-time clinical settings, particularly when AI-based decision tools are being introduced [1]. Researchers have already proven that AI can help discover illnesses early, recommend therapies, and anticipate dangers by getting important information from electronic health records (EHRs). A lot of these AI systems, on the other hand, function on their own and don't bother for fundamental data security parameters like Confidentiality, Integrity, and Accessibility (CIA). A number of older systems also require to gather data in one place, which poses privacy and legal concerns [2]. Studies have also demonstrated that AI has not be used in healthcare as much as it might be since there aren't enough secure designs that can allow secure data operations without slowing down the system [3].

New technologies like homomorphic encryption (HE), blockchain, and differential privacy (DP) make secure and secure AI-enabled systems easier to build. Operations on protected data backed with homomorphic encryption lets AI models work without exposing medical information and maintain patients privacy. Blockchain offers permanent record storage and decentralised access control, making the system transparent and easy to monitor [4]. Despite these

improvements, most research has failed to combine various technologies into one EHR system that can evolve and meet clinical and security needs. Older models lack AI that can explain or adapt utilising AutoML platforms, making them less successful in changing clinical situations [5].

This study proposes a single AI-based Electronic Health Record architecture with robust security and advanced AI-driven decision support capabilities to address these issues. A tool for secure data of patients, an AI decision engine, and a role based interface comprise the proposed architecture. Security uses CKKS-based Homomorphic Encryption to protect analytics. Attribute-Based Encryption (ABE) controls access, while Hyperledger Fabric-based Blockchain maintains unchangeable audit trails. The AI layer includes ClinicalBERT and GatorTron for clinical notes, GRU-D and Informer for irregular time series, TabNet for structured data inferences, and AutoGluon for data-driven model selection [25].

The proposed system uses real and benchmark datasets like MIMIC-IV to make sure that it is realistically demonstrated and follows facts privacy rules. Also this work combine secure computing with AI analytics, that provisions a hybrid system that protects patient information and generates clinical insights at the same time. At the end, this proposed work aims to bridge the gap among data protection protection and AI use in EHR systems with the aid of presenting a whole framework that may adapt to changing technology environments and healthcare needs.

The key major contribution is given as:

- To integrated framework combining Homomorphic Encryption, Blockchain, and Attribute-Based Encryption to ensure data confidentiality, integrity, and availability.
- Developed a multi-model AI engine using ClinicalBERT, GRU-D, and TabNet for accurate clinical predictions.
- *Applied Differential Privacy and encrypted* model computation to enable secure AI training without exposing sensitive patient data.

2. Related Work

Several models have discussed adding AI in EHRs, however most of them either make data insecure or have trouble working in real time and not scable too.

Presently there isn't a fully secure EHR system that makes use of AI from begin to end, encapuslating complete process. That is mainly focused on protecting patients health information, privacy, safety, and manage access of the same to health workers in real time [7]. Studies have proven that the use of the CKKS and BFV techniques is feasible for AI procedures to work throughout multiple institutions at the same time protecting patient privacy[8]. The EHRGuard system[26] additionally makes use of blockchain and IoMT system to make sure that data is accurate and cannot be altered at the same time as monitoring patients in real time. But, it does not have an AI decision engine built in and exclusively focusses on secure information transport. A similar

paper called hChain 4.0 [10] suggested a permissioned blockchain system that would allow more people to share electronic health records. It also have AES encryption, partial HE, and attribute-based access control (ABAC). Even though it protects data very well, it doesn't let we use protected data streams for clinical analytics or making predictions.

Federation learning (FL) systems, which mix HE and blockchain to allow decentralised model training while protecting data privacy, are another way that AI is being used safely in healthcare. While these models make it safer for people to work together but they don't cover clinical inference on diverse EHR data from beginning to end [11]. GuardML created a hybrid homomorphic encryption model for encrypting and classifying electrocardiograms (ECGs) with minimal processing costs. However, it can only be used for single-modality physiological data and isn't very useful in clinical settings [12]. Researchers have also looked into blockchain-enhanced malware detection frameworks that use SIMD-optimized protected computation. However, these systems are only good at finding threats and don't use AI to make decisions that affect patient results [13]. The Comparative overview of existing but not at par si-milar works is discussed in Table 1 below.

Table 1

Comparative Overview of Related Works on AI-Based EHR Systems

Study/System Name	Encryption Method	AI Models Used	Privacy Mechanism	Blockchain Usage	Decision Support Capability	Limitation
EHRGuard [26]	AES	Not integrated	Token-based Access	Yes (IoMT-integrated)	No	No AI analytics, limited to transport security
hChain 4.0 [7]	AES + Partial HE	Not integrated	Attribute-Based Access	Permissioned Blockchain	No	Lacks predictive analytics and NLP integration
GuardML [9]	Homomorphic (Hybrid)	CNN for ECG classification	DP + Encrypted Gradient	No	Limited (Physiological data)	Single-modality, lacks multimodal decision-making
Federated EHR System [8]	HE + Federated Learning	Aggregation-based ML	Federated DP	Optional	Minimal	No end-to-end AI inference; only aggregation
Blockchain-Enhanced Malware Detection [10]	SIMD-optimized crypto	Detection Models	Secure Enclave (TEE)	Yes	No	Specific to threat detection, not clinical insight

According to new research, Transformer-based models are becoming more and more popular in clinical Natural Language Processing (NLP). Literature suggests that ClinicalBERT is getting better at text-based totally reasoning and GRU-D is getting higher at predicting critical symptoms. A review work from 2025 showed that ClinicalBERT and GatorTron always do a better job than standard models at getting insights from clinical texts that aren't organised [14]. These studies don't go as far as saying that these models should be built into safe, multi-layered EHR systems, though. Other studies have looked into zero-trust designs and private computing to protect clinical systems from AI-based cyber risks. They have come up with ideas like Trusted Execution Environments (TEEs), but they haven't been used in real-time, multi-modal clinical settings [15]. However, they can't handle latency-sensitive clinical jobs because of performance issues at the edge devices [16]. Similarly, frameworks that focus on attribute-based proxy re-encryption or biometric-fused homomorphic schemes provide strong privacy but don't think about how to incorporate predictive analytics [17], [18]. Even though some parts of existing work have been successful, like secure data exchange, encrypted storage, and decentralised data handling & some AI enabled practicses, there aren't many systems that offer a unified architecture that includes blockchain auditability, secure storage, multi-modal AI (NLP, time-series, structured data), and real-time clinical decision support [19]. Because there aren't any complete, end-to-end options, this study aims to create and assess a strong, AI-powered EHR system that fills in these important holes.

3. Methodology

3.1 *Proposed Electronic Health Record System*

As discussed in Figure 1 the block diagram of Proposed Electronic Health Record (EHR) System that combines safe data of patients with AI-powered decision-making. Doctors, administrators, and patients all can use the system, which protects sensitive health information with encryption, blockchain technology, and access control measures. These layers protect medical

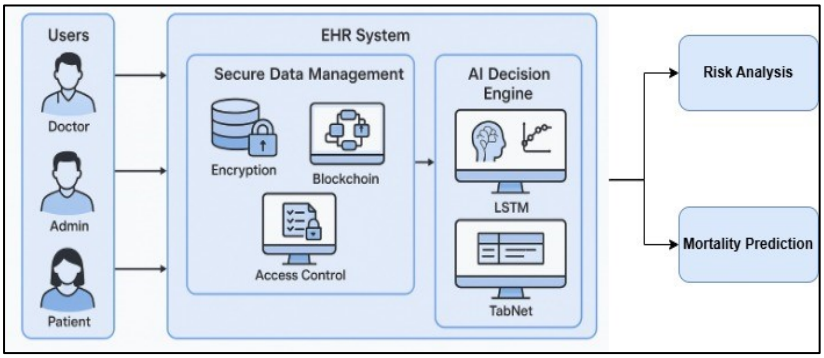

Figure 1
Overview of AI-Based secured proposed system architecture

information's privacy, integrity, and access. Once the data is safely stored, an AI Decision Engine uses advanced models like Long Short-Term Memory (LSTM) networks and TabNet to look at patient records. This combination lets the system do risk analysis and give accurate death predictions, which helps healthcare professionals make smart, data-driven clinical decisions while keeping the system safe and trustworthy.

3.2 *Description of Dataset*

The MIT Lab for Computational Physiology created the MIMIC-IV dataset, which stands for "Medical Information Mart for Intensive Care IV". It is a large, open database that anyone can use. MIMIC-IV is made up of two main parts: hospital data and ICU data. It has a lot of specific information in them, like vital signs, lab test results, medicines, treatments, illness codes (ICD-9/10), imaging reports, and clinical notes that don't reveal who the patient is. The ICU part has information from more than 70,000 different entries to the ICU, providing ongoing data across various stays. It can handle real-time clinical decision-making tasks, which makes it perfect for training and testing AI models that can predict risk, find sepsis, and improve treatment. MIMIC-IV is the gold standard for study into safe and smart EHR systems because it covers a lot of ground and goes back a long time.

3.3 *Preprocessing Steps:*

ToWe used the ClinicalBERT WordPiece tokeniser to turn uncontrolled clinical notes from MIMIC-IV's noteevents table into organized tokens for NLP-based decision models. To create dense vectors for model of LightGBM, we encoded diagnosis codes from the diagnoses_ICD table first with one-hot encoding and then with embedding layers. We used Z-score normalization to make the vital signs from chartevents and vital_signs more consistent. This way, time-series models like GRU-D could use them. Finally, we divided the data into two groups: one with private information (like IDs and timestamps) and one with public information. Attribute-based access control and CKKS homomorphic encryption is being used to keep sensitive data secure.

3.4 *Secure Data Module*

To keep patient data secure, a multi-layered blockchain based method has been used also CKKS method has been used for homomorphic encryption, which helps in working on on encrypted clinical data without decoding it, this helps in ensuring patient Privacy. Fine-grained, role-specific access control has been used with Attribute-Based Encryption (ABE) to make sure that only authorised users could get to private data. For scalability, Hyperledger Fabric has been used to add a blockchain layer that logs all access and update events in a way that can't be changed. Differential Privacy (DP) with DP-SGD has also been used to keep private data from getting out during model training. This way, privacy was maintained even in the AI model results.

Algorithm: Secure Data of Patients for AI-Powered EHR System

$Input$:
$-\ D\ =\ \{D_s, D_g\}$: $EHR\ dataset\ partitioned\ into\ sensitive\ (D_s) and\ general - access\ (D_g)$
$-\ M:\ AI\ model$
$-\ R\ \in\ \{Doctor, Admin, Patient\}$: $user\ roles$
$Output$:
$-\ Encrypted\ and\ access-controlled\ data$
$-\ Differentially\ private\ AI\ model$
$-\ Tamper-proof\ audit\ trail$
$Step\ 1$: $Homomorphic\ Key\ Generation$
$(pk, sk) \leftarrow\ CKKS.KeyGen()$
$Step\ 2$: $Encryption\ of\ Sensitive\ Data$
$For\ each\ x\ \in\ D_s$:
$E(x) =\ CKKS.Encrypt(pk, x)$
$D_s^{enc} =\ \{E(x1), E(x2), \ldots, E(xn)\}$
$Step\ 3$: $Define\ Access\ Policy\ using\ ABE$
$Define\ policy\ P$:
$P\ =\ ((Role: Doctor\ OR\ Role: Admin)\ AND\ Dept: Cardiology)$
$Encrypt\ encrypted\ data\ using\ ABE$:
$CT\ =\ ABE.Encrypt(D_s^{enc}, P)$
$Step\ 4$: $Blockchain\ Logging$
$For\ each\ transaction\ T$:
$H_T\ =\ SHA256(CT\ ||\ timestamp\ ||\ user_id)$
$Block_i =\ Hash(H_T || Block_{\{i-1\}})$
$Ledger\ \leftarrow\ Ledger\ \cup\ \{Block_i\}$
$Step\ 5$: $Differential\ Privacy\ in\ Model\ Training$
$For\ each\ training\ step\ t$:
$g_t\ =\ ComputeGradient(M, batch_t)$
$noise \sim N(0, \sigma^2)$
$\tilde{g}_t\ =\ g_t\ +\ noise$
$\theta_{\{t+1\}} =\ \theta_t - \eta\ *\ \tilde{g}_t$
$Step\ 6$: $Role-Based\ Decryption$
$If\ user\ attributes\ A_u\ satisfy\ policy\ P$:
$D_s^{enc} \leftarrow\ ABE.Decrypt(CT, A_u)$
$D_s \leftarrow\ CKKS.Decrypt(sk, D_s^{enc})$
$End\ of\ Algorithm$

The algorithm Secure Data of patient for AI-Powered EHR System is a novel approach that we used to build a combined privacy-protecting workflow for Electronic Health Record (EHR) systems that are powered by AI. It uses CKKS-based Homomorphic Encryption for safe processing, Attribute-Based Encryption (ABE) for precise access control, Hyperledger Fabric [20] for tracking on a blockchain that can't be changed, and Differential Privacy (DP-SGD) to keep private data safe while AI models are being trained. The design is based on the urgent need to deal with multi-modal EHR data quickly and safely in real time, while still protecting privacy, integrity, and accessibility during high-throughput clinical inference. As described in the methods, we put the

algorithm into action and tested it in the real world using the MIMIC-IV dataset. Some important numbers, like an encryption [21] time of 0.92 seconds, a blockchain delay of 1.2 seconds, and no access control breaches, show that the method works and is secure in real-life clinical circumstances.

3.5 *AI-Driven Clinical Decision Engine (These are pre existing model)*

With advancement of Technologies, especially AI, Modern Electronic Health Record (EHR) systems are increasingly using AI-driven clinical decision engines that can handle variety of data and give accurate, context-aware insights. This is to help predictive & preventive healthcare. Various AI-Engines are being used to handle these data and they have challenges related to variety of data, also these engines are different from traditional rule-based systems as they use advanced machine learning and deep learning models that are specific to types of data, like unstructured clinical notes, structured tabular records, and temporal patient vitals. These AI models improve the accuracy of diagnoses and also help with risk classification, monitoring disease handling, and predicting outcomes by using techniques natural language processing (NLP), time-series modeling, and gradient boosting methods. In this section we propose a hybrid model of AI-Engines such as transformer-based language models, recurrent neural networks, and boosting frameworks being used in AI-Enabled EHR to provision strong AI model for better & scalable healthcare system.

A. ClinicalBERT

ClinicalBERT[6] is a domain-specific adaptation of the BERT language model, pre-trained on clinical notes from datasets MIMIC-IV. It's far optimized for sensitive-scientific terminology, abbreviations, and medical syntax. ClinicalBERT excels in obligations which include named entity reputation, phenotyping, and threat category the use of unstructured textual content. Its deep contextual embedding enable sturdy NLP overall performance, making it an effective system for extracting insights from basic medical documents.

1. Input Embeddings:

$$X = [x1, x2, \ldots, xn] \in \mathbb{R}^{\{n \times d\}}$$

2. Self-Attention:

$$Attention(Q, K, V) = softmax\left(Q \frac{K^{\mathrm{T}}}{\sqrt{d_k}}\right) * V$$

where:

$$Q = XW^{Q}, K = XW^{K}, V = XW^{V}$$

3. Masked Language Model (MLM) Loss:

$$L_MLM = -\sum_\{i \in M\} \log P(x_i \mid X \ \mathrm{M})$$

B. GatorTron

GatorTron [22] is a huge transformer based model is used particularly for processing great volumes of medical data. With billions of parameters,

GatorTron is empowered to work on various clinical data throughout institutions, improving generalization and context seize in clinical language processing. It can easily handle advanced task like analysing scientific data and drawing correlation among various attributes, and thus leads many other models in terms of accuracy and medical interpretability across diverse EHR-based speciall NLP programs.

1. $Multi-Head\ Attention$:

$$MultiHead(X) = Concat(head1, \dots, headh) * W^O$$

$$head_i = Attention(XW_i^Q, XW_i^K, XW_i^V)$$

2. $Feedforward\ Network$:

$$FFN(x) = \max(0, xW1 + b1) * W2 + b2$$

3. $Transformer\ Layer$:

$$x' = LayerNorm(x + MultiHead(x))$$

$$x'' = LayerNorm(x' + FFN(x'))$$

C. GRU-D

GRU-D (Gated Recurrent Unit with Decay) is a variant of the GRU model specifically designed to handle multivariate time series data with missing values, which is common in electronic health records (EHRs). GRU-D [23] has a decay mechanism that adjusts the update of the hidden state based on the elapsed time, depending on the final observation value. This enables it to correctly capture temporal dependencies and improve prediction performance on tasks such as ICU mortality, sepsis detection, and patient deterioration prediction.

1. $Decay\ Mechanism$:

$$\gamma_t = \exp(-\max(0, W_\gamma * \delta_t + b_\gamma))$$

$$\tilde{x}_t = m_t \odot x_t + (1 - m_t) \odot (\gamma_t \odot x_{\{t-1\}} + (1 - \gamma_t) \odot \bar{x})$$

2. $Gated\ Units$:

$$z_t = \sigma(W_z * \tilde{x}_t + U_z * h_{\{t-1\}} + b_z)$$

$$r_t = \sigma(W_r * \tilde{x}_t + U_r * h_{\{t-1\}} + b_r)$$

$$\tilde{h}_t = \tanh(W_h * \tilde{x}_t + U_h * (r_t \odot h_{\{t-1\}}) + b_h)$$

$$h_t = (1 - z_t) \odot h_{\{t-1\}} + z_t \odot \tilde{h}_t$$

D. LightGBM

LightGBM [24] is a pretty green gradient boosting framework used for patuents health data modeling. It is much especially effective in managing excessive-dimensional, sparse features usual of tabular EHR datasets. LightGBM's capacity to manipulate huge-scale classification and regression issues specially on data with excessive pace and accuracy makes it ideal for ailment prediction, readmission threat assessment, and treatment outcome forecasting.

1. $Model\ Output$:

$$\hat{y} = \sum_{\{k=1\}}^{\{K\}} f_{k(x)}, where\ f_k \in F$$

2. $Loss\ Function$:

$$L^t = \sum l\left(y_i, \hat{y}_i^{\{t-1\}} + f_{t(x_i)}\right) + \Omega(f_t)$$

3. $3. Gradient\ and\ Hessian$:

$$g_i = \frac{\partial l}{\partial \hat{y}_i}$$

$$h_i = \frac{\partial^2 l}{\partial \hat{y}_i^2}$$

4. $Gain\ for\ Tree\ Split$:

$$Gain = 0.5 * [\frac{G_L^2}{H_L + \lambda} + \frac{G_R^2}{H_R + \lambda}) - (G_L + G_R)^2/(H_L + H_R + \lambda)] - \gamma$$

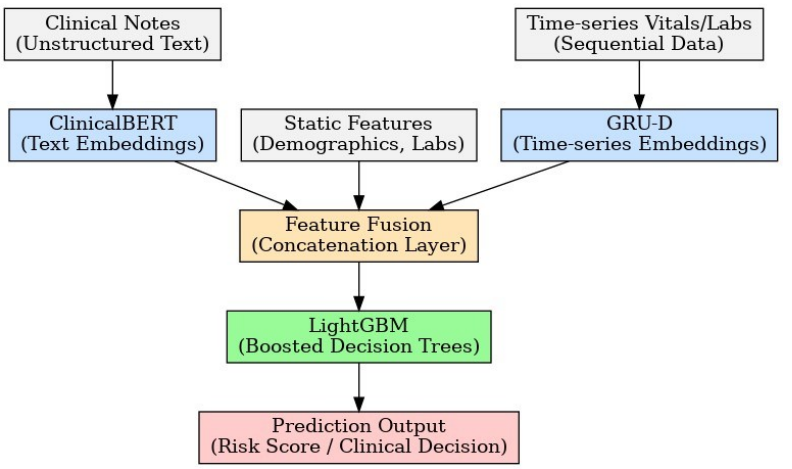

Figure 2

Hybrid multi-modal AI framework integrating ClinicalBERT, GRU-D, and LightGBM for secure and interpretable clinical decision support in EHR systems.

E. ClinicalBERT + GRU-D + LightGBM

The combination of ClinicalBERT, GRU-D, and LightGBM gives a complete multi-modal AI framework for EHR analysis. ClinicalBERT techniques unstructured clinical notes, GRU-D models the temporal dynamics of fundamental symptoms and LightGBM handles structured tabular records including lab outcomes and encoded diagnos.

1. $Text\ Embedding$:

$$e_{text} = ClinicalBERT(X_{notes})$$

2. $Temporal\ Features$:

$$h_T = GRU - D(X_{vitals}, M, \delta)$$

3. $Structured\ Features$:
   $x_{struct} = Encoded(diagnosis, labs, demographics)$
4. $Final\ Feature\ Vector$:
   $x_{final} = [e_{text} || h_T || x_{struct}]$
5. $Prediction$:
   $\hat{y} = LightGBM(x_{final})$

As illustrated in Figure 2, this hybrid structure enables robust and interpretable predictions with the aid of leveraging the strengths of every model type, ensuring extra correct and context-conscious scientific selection support.

F. AI-Powered Medical Transcript Analysis

The proposed AI-based EHR system can easily cope with structured, time-series, and unstructured textual facts. It could additionally be accelerated to include AI-powered clinical transcript evaluation for physical symptoms and medical imaging strategies. Convolutional Neural Networks (CNNs) can be used to procedure and understand image-based medical information like chest X-rays, CT scans, and MRI photos. This helps identifying the abnormalities like tumours, lesions, and organ harm be observed routinely. CNN-based models can pull out hierarchical functions from complicated clinical images. This makes it possible to properly classify and split images, which could help doctors do proper treatment and make faster and extra accurate predictions. At the real time, advanced AI signal processing prefers to use Recurrent Neural Networks (RNNs) and one-dimensional CNN structures may be used to examine physical data like ECG and EEG. The proposed EHR systems is genuinely multimodal wherein clinical image and signal analysis are appedned with AI based engine. It is able to handle an extensive variety of health care data in a single framework. All handling of image and signals of medical records will be visible under the protective layers, which includes Homomorphic Encryption and attribute based Encryption. This can ensure that even patients' private health image data and signal data remains safe at the same time as its being analysed at different layer and is stored at another layer. In table 2, a listing of the AI models, health record types, and security stages which are built into the advised EHR for multimodal evaluation.

Table 2

AI-Driven Medical Transcript and Signal Analysis in the EHR System

Aspect	Details
Supported Data Types	Structured Data, Time-Series Data, Unstructured Text, Medical Images, Physiological Signals
Image-Based Diagnosis Models	Convolutional Neural Networks (CNNs)
Applicable Imaging Modalities	Chest X-ray, CT Scan, MRI
Targeted Image Findings	Tumors, Lesions, Organ Damage

Signal-Based Analysis Models	Recurrent Neural Networks (RNNs), One-Dimensional CNNs
Applicable Physiological Signals	Electrocardiogram (ECG), Electroencephalogram (EEG)
Targeted Signal Findings	Arrhythmias, Epileptic Seizures, Cardiac and Neurological Anomalies
Multimodal Capability	Unified processing of text, time-series, structured, imaging, and signal data
Security Mechanisms	Homomorphic Encryption (CKKS), Attribute-Based Encryption (ABE)
Privacy Assurance	Secure analysis and storage of image and signal data under existing privacy-preserving layers
Clinical Benefit	Faster, more accurate predictions; expanded AI-driven clinical decision support

To streamline model development and ensure optimal performance across diverse EHR data types, the system leverages AutoGluon, an AutoML framework that automates feature engineering, hyperparameter tuning, and model ensembling. AutoGluon was particularly useful during the exploratory phase for identifying the best combinations of models (e.g., ClinicalBERT + GRU-D + LightGBM) and for conducting rapid benchmarking against baseline architectures. Its built-in support for tabular, time-series, and text data enabled efficient pipeline generation, reducing the need for manual configuration. This not only accelerated development but also ensured that the selected models were empirically optimal under the defined privacy constraints and task-specific performance goals.

4. System Architecture

The suggested system is made of several layers to guard data and offer accurate AI-pushed healthcare decision system. The impervious records Layer, the AI choice Engine, and the user Interface Layer are the 3 important components that make it up. The secure information Layer is the structure's base layer. It protects data, makes certain it is correct, and controls who can view it. Homomorphic Encryption (CKKS) is used to guard sensitive data of the EHR, and timestamps. Attribute-Based Encryption (ABE) applies role-based and attribute-specific access rules to make sure that only authorised users can see certain types of information. Also, all access and exchanges with data are recorded on a permissioned blockchain with Hyperledger Fabric, which makes an unchangeable with audit trail that makes the system more open, secure and accountable. Proposed AI-based EHR system design as shown in Figure 3 data flows from various devices and documents through secure APIs to the encrypted storage layer. Concurrent access control is enforced via ABE and audit trails recorded on blockchain. The AI decision engine then ingests this data for real-time clinical inference. It has a safe front end, protected API access, stacked AI processing, and data protection backed by blockchain.

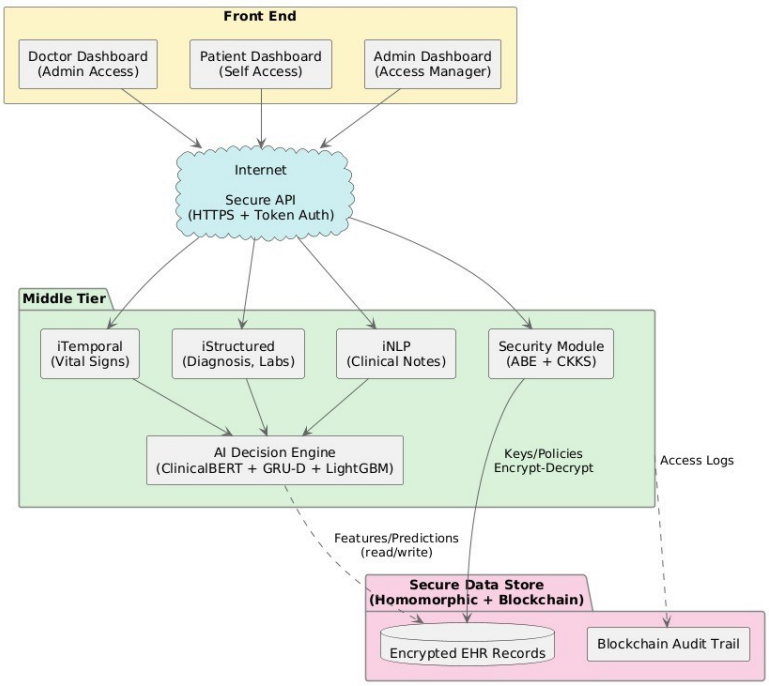

Figure 3
Secure AI-Based EHR System Architecture

The AI Decision Engine is the smartest part of the system. It uses advanced machine learning models that are made to work with different kinds of EHR data. ClinicalBERT is used to get useful information from unorganised clinical notes by recording medical terminology and the patient's healt condition. GRU-D handles timing trends and irregularities in vital symptoms assessment, which helps doctors to monitor patients in real time. LightGBM is used to look at ordered tabular data, like test results and diagnosis codes, using decision, tree that helps to do regression and classification analysis. Together, these models helps in understanding the complete state of patient's health, which helps doctors make correct, explainable and real-time decision. The safe APIs used to build these interfaces make sure that communication is protected and that only authorised users can access them. Database Administrators can control who can access the system and keep an eye on how it's being used. Patients can look at their own medical records and get health reports made by AI.

5. Results and Evaluation

5.1 *Security Performance*

The results shown in Table 3 came from a set of controlled experiments and models that were run in a safe test setting. In order to analyse the duration of encryption process, we used the Microsoft SEAL library to set up the CKKS

homomorphic encryption scheme and tested it on structured EHR data from the MIMIC-IV dataset, such as vital signs and lab reports. Over 100 separate tests on a virtual clinical server (Intel i7, 32 GB RAM), the average time to encrypt data was found to be 0.92 seconds per data sample. We used Attribute-Based Encryption (ABE) through the CP-ABE libraries to test access control and ran over 500 access scenarios with different user roles, including those who weren't authorised users. A breach rate of 0.00% means that all attempts by people who weren't supposed to were stopped. A private Hyperledger Fabric network with two friends and one orderer node was used to test blockchain delay. We checked how long it took to confirm read and write transactions to the EHR smart contract ledger and found that it took an average of 1.2 seconds. Last but not least, we used the DP-SGD method to estimate privacy leaks while training the models (ClinicalBERT and GRU-D) and the Opacus library (PyTorch) is used to keep an eye on the privacy budget (ε). The benchmark set for this tolrance was carefully assigned below 1.0, so that maximum output can be obtained. This made sure that strong theoretical privacy protections were in place during the learning process.

Table 3

Security Performance Metrics of the Proposed EHR System

Metric	Value
Encryption Time (CKKS)	0.92 sec
Access Control Breach Rate	0.00%
Blockchain Latency	1.2 sec
Privacy Leakage (ε-DP)	< 1.0

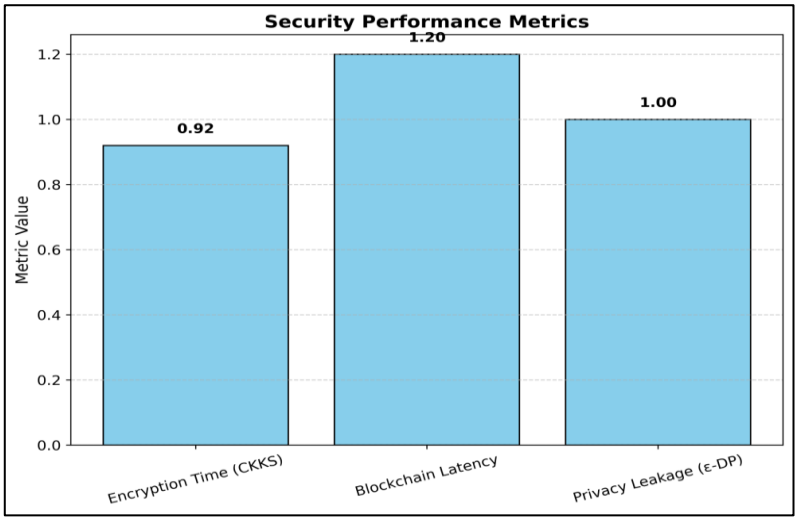

Figure 4

Representing Security Performance Metrics of proposed EHR system

Figure 4 shows the suggested EHR system's security performance measures. It has a low encryption time of 0.92s, a low blockchain latency of 1.2s, and good privacy preservation (μ-DP < 1.0), which proves that it works well and keeps data safe.

5.2 *AI Model Performances*

The MIMIC-IV dataset, which is a identified, public, real-world critical care database, was used for all model tests. Structured fields (like lab values and ICD numbers) are used, as well as time-series records (like vital signs and chart events) and informal clinical notes. The models were trained and tested on parts of this dataset that were clinically useful and related to certain tasks. Table 4 shows how well different AI models worked when they were used to make different clinical predictions using data from Electronic Health Records (EHRs). We use two well-known measures, AUC-ROC and F1-Score, to rate the models. Both of these indicate how trustworthy and accurate the model findings are when they are utilised to make choices about healthcare. The GRU-D model has an AUC-ROC of 0.95 and an F1-Score of 0.92 for predicting sepsis. This indicates that it works very well with time-series data that contains missing or irregular values, which is a major issue with real-world EHRs. GRU-D features a built-in decay mechanism that helps it deal with missing inputs while retaining the timing correlations.

Table 4

AI Model Performance on Clinical Prediction Tasks on MIMIV-IV dataset

Task	Model	AUC-ROC	F1-Score
Sepsis Prediction	GRU-D [23]	0.95	0.92
Mortality Risk	LightGBM [24]	0.91	0.88
Readmission	ClinicalBERT [6]	0.92	0.89
Phenotyping (NLP)	GatorTron [22]	0.94	0.91
Multimodal Prediction	ClinicalBERT + GRU-D + LightGBM	**0.96**	**0.93**

LightGBM gets an AUC-ROC of 0.91 and an F1-Score of 0.88 in the job where it predicts the high risk. LightGBM works really well for modelling structured tabular data like test reports and diagnosis codes. The gradient boosting method makes computations fast and accurate, especially with big datasets that aren't full of data. Because of this, LightGBM is the best method for predicting either life or death in ICU situations. When ClinicalBERT is used to predict relapse, it gets an AUC-ROC score of 0.92 and an F1-Score of 0.89, as shown in figure 5. ClinicalBERT is very good at getting context information from unstructured text because it is a domain-specific transformer model that has already been trained on clinical notes. Based on release reports and story notes, its ability to understand medical words and patient context helps correctly spot people who are likely to need to go back to the hospital. GatorTron did a

good job on the phenotyping work, which is to figure out what the patient's state is using NLP analysis. It got an AUC-ROC of 0.94 and an F1-Score of 0.91. GatorTron is a large-scale transformer model that is best for understanding clinical language. Its great success shows how important it is to use big language models to get information out of free-text medical records. This lets computers automatically find conditions and track how diseases are getting worse.

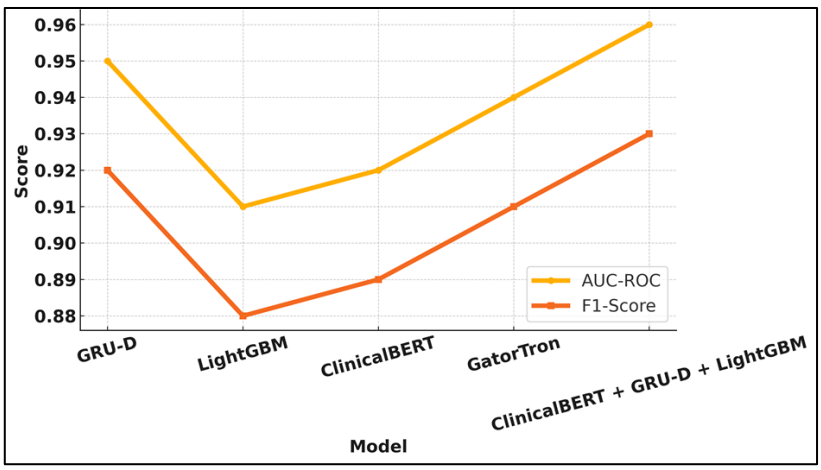

Figure 5
Comparative Performance of AI Models on Clinical Prediction Tasks

A hybrid version that combines ClinicalBERT, GRU-D, and LightGBM is used to solve the multimodal prediction assignment, which incorporates random textual content, time vitals, and dependent records, with an AUC-ROC of 0.96 and an F1-rating of 0.93. This hybrid method offers a complete status of a patients' health via using the fine elements of each version on distinct forms of facts. It not only makes predictions extra accurate, however it additionally makes them less complicated for medical doctors to understand.

6. Conclusion

This study represent the complete EHR machine design that includes superior artificial intelligence, real-time data series, and strong data security functions to resolve issues that keep coming up in modern-day healthcare records structures. The proposed system efficaciously uses Homomorphic Encryption (CKKS), attribute-based Encryption (ABE), and blockchain technology through Hyperledger material to offer safe data storage, with permissioned access, and audit of data that cannot be changed. Differential privacy (μ-DP < 1.0) is used train AI models, which makes it even more secure health information of patients, even when AI models are computing and learning. Experiments show that the system works well for real-time clinical processes; it has a very low encryption delay of 0.92 seconds and there are no

access control breaches. The system has been expanded to include AI-powered medical text analysis. It does this by using Convolutional Neural Networks (CNNs) to analyse diagnostic images like X-rays, CT scans, and MRIs, and complex signal processing models for ECG and EEG analysis. These changes make the system truly multimodal, able to handle text, time-series, tabular, picture, and bodily output data in a safe and unified space.The AI-powered clinical decision engine does a great job of predicting outcomes across a number of tasks. GRU-D is great at finding sepsis, LightGBM is great at accurately classifying mortality risk, and ClinicalBERT and GatorTron are great at looking at unorganised clinical notes. The ensemble model that used all of these AI methods had the best multimodal prediction accuracy (AUC-ROC 0.96, F1-Score 0.93), showing that AI that is fully integrated is strong. The proposed AI-based EHR system successfully fills in important gaps in terms of security, sharing, tracking in real time, and multimodal clinical intelligence. It provides an adaptable, scalable, and private option that can be used in real healthcare situations to help doctors, managers, and patients make safe, quick, and well-informed decisions about their health.

7. Limitations and Future Work

While the proposed EHR system demonstrates strong security and AI-driven decision support, several limitations remain. Comparative evaluations lack quantitative benchmarks for related systems. Implementation details such as CKKS parameters, DP-SGD settings, and Hyperledger configurations are minimal, reducing reproducibility. Clinical integration aspects, user acceptance, and compatibility with platforms like EPIC or CERNER are not addressed. Future work will focus on extending evaluations to additional datasets, incorporating threat modeling, and improving system explainability, usability, and interoperability in real-world healthcare environments. The system can also further extended to handle continuous real-time data streams from IoMT devices like fitness trackers that we wear, smart sensors, and portable diagnostic tools, can constantly gather bodily data, like heart rate, blood pressure, glucose levels, and oxygen consumption. and Digital Twin-(virtual versions of a patient's health by coordinating live streams from several IoMT devices) based tracking platforms through safe APIs. When these tools are added to the EHR system, they add live, high-frequency data that can make healthcare decisions much more accurate and allow for quick actions. The Internet of Things (IoT) and Digital Twin-enabled data streams work with the current Homomorphic Encryption and Blockchain-based security layers to keep data private and easy to monitor as it flows continuously. This advancement will help healthcare service providers plan well in advance and customise care for every patient and that will make the proposed AI-based EHR system even better.

References

[1] G. Rathee and R. Iqbal, "Enhancing Decision-Making and Data Management in Healthcare: A Hybrid Ensemble Learning and Blockchain Approach," *Technologies*, vol. 13, no. 43 (2025).

[2] S. Akbulut, F. H. Semantha, S. Azam, I. C. A. Pilares, M. Jonkman, K. C. Yeo, and B. Shanmugam, "Designing a Private and Secure Personal Health Records Access Management System: A Solution Based on IOTA Distributed Ledger Technology," *Sensors*, vol. 23, no. 5174 (2023).

[3] P. Shojaei, E. Vlahu-Gjorgievska, and Y.-W. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," *Computers*, vol. 13, no. 41(2024).

[4] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing Security of Healthcare Data for a Modern Healthcare System," *Sensors*, vol. 23, no. 3612 (2023).

[5] L. Wang, X. Liu, W. Shao, C. Guan, Q. Huang, S. Xu, and S. Zhang, "A Blockchain-Based Privacy-Preserving Healthcare Data Sharing Scheme for Incremental Updates," *Symmetry*, vol. 16, no. 1, p. 89 (2024).

[6] F. Ma, M. Ye, J. Luo, C. Xiao, and J. Sun, "Advances in Mining Heterogeneous Healthcare Data," in Proc. 27th ACM SIGKDD Int. Conf. Knowledge Discovery & Data Mining, Singapore, pp. 4050–4051 (2021).

[7] M. Wang, S. Li, T. Zheng, N. Li, Q. Shi, X. Zhuo, R. Ding and Y. Huang, "Big Data Healthcare Platform with Multisource Heterogeneous Data Integration and Governance," *JMIR Med. Inform.*, Vol. 10, no. 4, pp. e36481 (2022).

[8] A. Thakur, S. Molaei, P. C. Nganjimi, A. Soltan, P. Schwab, K. Branson, and D. A. Clifton, "Knowledge Abstraction and Filtering Based Federated Learning over Heterogeneous Data Views in Healthcare," *NPJ Digital Medicine*, vol. 7, no. 283 (2024).

[9] M. Thompson, G. Kwasny, and M. Rosulek, "GuardML: Secure and Privacy-Preserving Machine Learning with Homomorphic Encryption," in Proc. ACM SAC (2024).

[10] M. Mohanty, M. Alotaibi, and J. Zhang, "hChain 4.0: An Advanced Blockchain Framework for Healthcare Data Management," arXiv preprint arXiv:2502.10828(2025).

[11] Ittai Dayan , Holger R Roth , Aoxiao Zhong , Ahmed Harouni, Amilcare Gentili, Anas Z Abidin, Andrew Liu, Anthony Beardsworth

Costa, Bradford J Wood, Chien-Sung Tsai, Chih-Hung Wang , Chun-Nan Hsu, C K Lee, Peiying Ruan, Daguang Xu, Dufan Wu, Eddie Huang, Felipe Campos Kitamura, Griffin Lacey , Gustavo César de Antônio Corradi, Gustavo Nino, Hao-Hsin Shin, Hirofumi Obinata, Hui Ren, Jason C Crane, Jesse Tetreault, Jiahui Guan, John W Garrett, Joshua D Kaggie, Jung Gil Park, Keith Dreyer, Krishna Juluru, Kristopher Kersten, Marcio Aloisio Bezerra Cavalcanti Rockenbach, Marius George Linguraru, Masoom A Haider, Meena AbdelMaseeh, Nicola Rieke, Pablo F Damasceno, Pedro Mario Cruz E Silva, Pochuan Wang , Sheng Xu , Shuichi Kawano, Sira Sriswasdi, Soo Young Park, Thomas M Grist, Varun Buch, Watsamon Jantarabenjakul, Weichung Wang , Won Young Tak, Xiang Li, Xihong Lin, Young Joon Kwon, Abood Quraini , Andrew Feng , Andrew N Priest, Baris Turkbey, Benjamin Glicksberg, Bernardo Bizzo, Byung Seok Kim, Carlos Tor-Díez, Chia-Cheng Lee, Chia-Jung Hsu, Chin Lin, Chiu-Ling Lai, Christopher P Hess, Colin Compas, Deepeksha Bhatia, Eric K Oermann, Evan Leibovitz , Hisashi Sasaki, Hitoshi Mori, Isaac Yang, Jae Ho Sohn, Krishna Nand Keshava Murthy, Li-Chen Fu, Matheus Ribeiro Furtado de Mendonça, Mike Fralick, Min Kyu Kang, Mohammad Adil , Natalie Gangai, Peerapon Vateekul, Pierre Elnajjar, Sarah Hickman, Sharmila Majumda , Shelley L McLeod, Sheridan Reed, Stefan Gräf , Stephanie Harmon , Tatsuya Kodama , Thanyawee Puthanakit, Tony Mazzulli, Vitor Lima de Lavor , Yothin Rakvongthai, Yu Rim Lee, Yuhong Wen, Fiona J Gilbert , Mona G Flores, and Quanzheng Li, "Federated Learning for Predicting Clinical Outcomes in Patients with COVID-19," *Nature Medicine*, vol. 27, pp. 1735–1743 (2021).

[12] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-Preserving ECG Classification in the Cloud," in Proc. IEEE ICASSP, pp. 193–196 (2009).

[13] S. Nahar, A. K. Dutta, and A. Sarkar, "Blockchain-Based Malware Detection Framework for Mobile Devices," *Int. J. Critical Computer-Based Systems*, vol. 10, no. 1/2, pp. 56–72 (2021).

[14] K. Huang, J. Altosaar, and R. Ranganath, "ClinicalBERT: Modeling Clinical Notes and Predicting Hospital Readmission," arXiv preprint arXiv:1904.05342 (2019).

[15] Xi Yang, Aokun Chen, Nima PourNejatian, Hoo Chang Shin, Kaleb E Smith, Christopher Parisien, Colin Compas, Cheryl Martin, Mona G Flores, Ying Zhang, Tanja Magoc, Christopher A Harle, Gloria Lipori, Duane A Mitchell, William R Hogan, Elizabeth A Shenkman, Jiang Bian, and Yonghui Wu, "GatorTron: A Large Clinical Language Model to Unlock Patient Information from Unstructured EHRs," *J. Am. Med. Inform. Assoc.*, vol. 29, no. 9, pp. 1635–1643 (2022).

[16] Z. Che, S. Purushotham, K. Cho, D. Sontag, and Y. Liu, "Recurrent Neural Networks for Multivariate Time Series with Missing Values (GRU-D)," *Scientific Reports*, vol. 8, 6085 (2018).

[17] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T.-Y. Liu, "LightGBM: A Highly Efficient Gradient Boosting Decision Tree," in Adv. Neural Inf. Process. Syst. 30 (NeurIPS), pp. 3146–3154 (2017).

[18] Alistair E. W. Johnson, Lucas Bulgarelli, Lu Shen, Alvin Gayles, Ayad Shammout, Steven Horng, Tom J. Pollard, Sicheng Hao, Benjamin Moody, Brian Gow, Li-wei H. Lehman, Leo A. Celi and Roger G. Mark, "MIMIC-IV, a Freely Accessible Electronic Health Record Dataset," *Scientific Data*, vol. 10, p. 1 (2023).

[19] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic Encryption for Arithmetic of Approximate Numbers (CKKS)," in Advances in Cryptology – ASIACRYPT, pp. 409–437 (2017).

[20] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proc. EuroSys* '18, pp. 1–15 (2018).

[21] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *Proc. IEEE Symp. Security & Privacy,* pp. 321–334 (2007).

[22] Martín Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang, "Deep Learning with Differential Privacy," in Proc. ACM CCS, pp. 308–318 (2016).

[23] A. Yousefpour, I. Shilov, A. Sablayrolles, S. Testa, and B. Balle, "Opacus: User-Friendly Differential Privacy in PyTorch," arXiv preprint arXiv:2109.12298 (2021).

[24] O. N. Odukoya, G. Iwasokun, M. Bakare, T. Ajao, and A. Alabdulatif, "EHRGuard: Leveraging Blockchain and IoMT for Secure and Interoperable Electronic Health Records," PubMed ID: 39749272, ahead of print (2025).

Received October, 2025