International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Transformers on Encrypted Federated Datasets Anchored by Blockchain Zero-Knowledge Proofs for Privacy-Preserving Multilingual Healthcare Diagnostics and Equity.

Oyegoke Oyebode

Technical Program Manager, Visa Inc. USA
DOI : https://doi.org/10.5281/zenodo.17157302

ABSTRACT

The deployment of artificial intelligence in healthcare is increasingly constrained by privacy, equity, and regulatory compliance challenges, especially in multilingual and cross-border contexts. Traditional centralized machine learning approaches are limited by restrictions on patient data sharing, raising both ethical and legal concerns. Federated learning offers a promising solution by enabling distributed training across institutions without transferring raw data, yet ensuring trust and privacy in federated systems remains a critical barrier. This study proposes a novel framework that combines transformer architectures with encrypted federated datasets anchored by blockchain zero-knowledge proofs (ZKPs) to achieve privacy-preserving, equitable, and multilingual healthcare diagnostics. Transformer-based models, known for their strength in natural language processing and multimodal learning, are adapted to operate on encrypted federated datasets spanning diverse linguistic and demographic contexts. Blockchain provides a decentralized trust layer, while zero-knowledge proofs ensure verifiable model updates without exposing sensitive patient information. This combination allows healthcare providers to collaboratively train diagnostic models that maintain strong predictive performance while adhering to strict privacy guarantees. The framework also advances health equity by enabling multilingual diagnostics that address disparities in underrepresented populations. By integrating explainability mechanisms, stakeholders gain insights into model reasoning across diverse cultural and linguistic datasets. Case applications in federated medical imaging, multilingual clinical notes, and genomic diagnostics highlight the framework's capacity to balance accuracy, privacy, and fairness. Overall, the integration of transformers, federated learning, and blockchain ZKPs represents a pathway toward trustworthy and equitable AI-driven healthcare, enabling collaborative innovation while safeguarding patient rights.

Keywords: Transformers; Federated learning; Blockchain zero-knowledge proofs; Privacy-preserving AI; Multilingual healthcare diagnostics; Health equity

1. INTRODUCTION

1.1 Background: AI in healthcare diagnostics and challenges of multilingual data

Artificial intelligence (AI) is reshaping healthcare diagnostics by enabling earlier detection of diseases, personalized treatment strategies, and predictive modeling of patient outcomes. Algorithms trained on medical imaging, genomic data, and electronic health records have demonstrated remarkable diagnostic accuracy, at times surpassing clinician benchmarks [1]. AI tools are now used in screening for cancer, cardiovascular anomalies, and infectious diseases, promising improvements in efficiency and scalability of healthcare services worldwide [2].

Yet the benefits are not evenly distributed. A central challenge lies in the multilingual nature of global healthcare data. Medical notes, pathology reports, and patient interactions are documented in diverse languages and dialects [3]. AI systems, which are frequently trained on English-language datasets, often struggle to interpret less represented languages, creating risks of misdiagnosis and exclusion [4]. For instance, terms describing symptoms may vary significantly between regions, and literal translations often fail to capture cultural context.

Natural language processing (NLP) in healthcare therefore requires precision, as errors in interpreting symptoms across languages can lead to inappropriate clinical recommendations [7]. Compounding the issue, limited annotated datasets for underrepresented languages make model training difficult. Without addressing linguistic inclusivity, AI could inadvertently reinforce inequities by privileging patients from regions with richer data resources [2]. Ensuring reliable multilingual support is thus not only a technical task but also an ethical necessity for fair and effective diagnostic AI deployment [5].

1.2 Limitations of centralized models and risks of bias, inequity, and privacy breaches

The dominant centralized model of AI training aggregates data into single repositories for large-scale processing. While effective for model development, this approach introduces systemic risks. One major concern is bias: centralized datasets often reflect the demographics of their source institutions, leading to skewed model performance. For example, algorithms trained predominantly on data from urban hospitals may underperform in rural or resource-limited settings [8]. This reinforces inequity in diagnostic outcomes, particularly for marginalized populations.

Privacy is another critical limitation. Centralized repositories are attractive targets for cyberattacks, with breaches exposing millions of sensitive health records in recent years [3]. Beyond technical vulnerability, there are ethical implications. Patients may not be fully informed about how their data are aggregated and repurposed for AI training, raising concerns of transparency and consent [6]. These gaps undermine trust in digital healthcare solutions.

Fragmentation further complicates the problem. Hospitals and research centers are often reluctant to share data due to regulatory frameworks like GDPR and HIPAA, competitive interests, or fears of liability. This leads to siloed datasets, limiting the ability of models to generalize across diverse patient populations [5]. The outcome is a paradox: centralized systems both concentrate risk and fragment access. Addressing these tensions requires rethinking architectures toward approaches that preserve privacy, ensure inclusivity, and reduce systemic bias.

1.3 Emerging solutions: federated learning, encryption, and blockchain

To address these challenges, new frameworks emphasize decentralization and privacy-preservation. Federated learning enables collaborative model training without moving patient data. Instead, algorithms are trained locally within hospitals, and only model parameters are shared with a central coordinator [2]. This protects raw patient records while enhancing inclusivity by drawing from diverse institutional datasets.

Privacy is further strengthened by advanced cryptographic techniques. Homomorphic encryption allows computations to be performed on encrypted data, ensuring sensitive records remain protected even during analysis [1]. Similarly, secure multi-party computation enables multiple stakeholders to contribute to training without exposing their individual datasets [7]. These methods reduce the risks associated with centralized exposure.

Blockchain adds another layer of trust by creating immutable records of data transactions and model updates. Its decentralized ledger ensures accountability and traceability, providing confidence to patients and institutions alike [4]. When integrated with federated learning, blockchain can authenticate contributions from different sites and prevent tampering.

Together, these solutions offer a paradigm shift from centralized infrastructures to resilient, privacy-preserving networks. By combining federated learning, encryption, and blockchain, healthcare AI can move closer to equitable, transparent, and secure diagnostic systems that function effectively across linguistic and cultural boundaries [6].

1.4 Research objectives and scope

The purpose of this research is to explore decentralized strategies for AI-driven healthcare diagnostics, with special emphasis on multilingual contexts. The first objective is to evaluate how federated learning mitigates systemic bias by incorporating data from varied linguistic and demographic sources. The second is to examine privacy-preserving tools encryption and blockchain as mechanisms to safeguard sensitive medical records while ensuring accountability [8]. Finally, the study aims to assess the broader ethical and operational implications of deploying these decentralized systems in international healthcare networks. The scope includes technical, social, and regulatory dimensions of this emerging field [3].

2. FOUNDATIONS OF FEDERATED LEARNING AND DATA PRIVACY

2.1 Federated learning principles in healthcare

Federated learning (FL) represents a paradigm shift in how healthcare institutions can collaborate on AI model training while safeguarding sensitive patient information. Unlike conventional centralized architectures, FL allows hospitals, clinics, and research centers to train models locally on their own datasets. Instead of transferring raw patient records, each institution computes model updates that are aggregated into a global model [9]. This decentralized mechanism helps address regulatory restrictions, such as HIPAA and GDPR, which often hinder cross-border data sharing.

The principle underpinning FL is iterative coordination. Local models are trained on subsets of patient data, such as imaging scans or clinical notes, and the updates are then transmitted to a central server that synthesizes them into a refined global model [8]. This ensures that sensitive data never leave the source, reducing the risk of breaches while also enabling inclusion of datasets that would otherwise remain siloed. By combining diverse sources, FL increases generalizability and reduces biases tied to region-specific populations.

Another advantage of FL is its scalability. As more institutions join, the model gains exposure to heterogeneous patient profiles, capturing variations in language, demographics, and medical practices [11]. This inclusivity is critical in multilingual healthcare settings where traditional centralized models may overlook underrepresented groups. However, FL is not without challenges: communication overhead, data heterogeneity, and governance complexity remain significant obstacles. Addressing these issues requires integration of encryption techniques and robust governance models.

Nevertheless, FL is widely recognized as a foundational step toward creating equitable, collaborative, and privacy-preserving healthcare AI infrastructures [7].

2.2 Encrypted federated datasets: homomorphic encryption, secure aggregation

While federated learning reduces reliance on centralized repositories, transmitting model updates still carries risks. Malicious actors could intercept updates and attempt to reconstruct sensitive patient information. To mitigate this, privacy-preserving cryptographic tools such as homomorphic encryption (HE) and secure aggregation are integrated into FL pipelines [12]. HE allows computations to be performed directly on encrypted data without requiring decryption. This ensures that hospitals can contribute to model training while maintaining full confidentiality of their underlying datasets.

Secure aggregation complements HE by ensuring that the central server only sees aggregated results rather than individual institutional updates [7]. For example, when multiple hospitals participate in collaborative training, their local gradients are encrypted and then summed before decryption. The global model update is revealed only after aggregation, preventing any participant or even the coordinating server from accessing another institution's contribution in isolation. This mechanism enhances trust among participants, which is particularly vital in cross-border healthcare collaborations where legal frameworks may differ [10].

A typical encrypted FL workflow begins with hospitals encrypting their model updates locally before transmission. These encrypted updates are securely aggregated at the central server, ensuring privacy throughout the process. Figure 1 illustrates this workflow, showing how encrypted gradients flow between hospitals and the coordinating entity. By preventing exposure of raw updates, this architecture strengthens resilience against inference attacks.

The use of HE, however, introduces computational overhead. Performing operations on encrypted data requires significantly more resources compared to plaintext computations [13]. Researchers are actively exploring lightweight cryptographic protocols and optimized hardware accelerators to balance privacy guarantees with efficiency. Moreover, secure aggregation must address scenarios involving dropout clients, ensuring that the global model can still be updated without compromising overall privacy guarantees.

Collectively, HE and secure aggregation extend the protective capacity of federated learning, transforming it from a data minimization tool into a robust, end-to-end privacy-preserving system. These methods are especially critical in healthcare environments, where both the stakes of privacy breaches and the diversity of multilingual datasets amplify the need for strong safeguards [9].

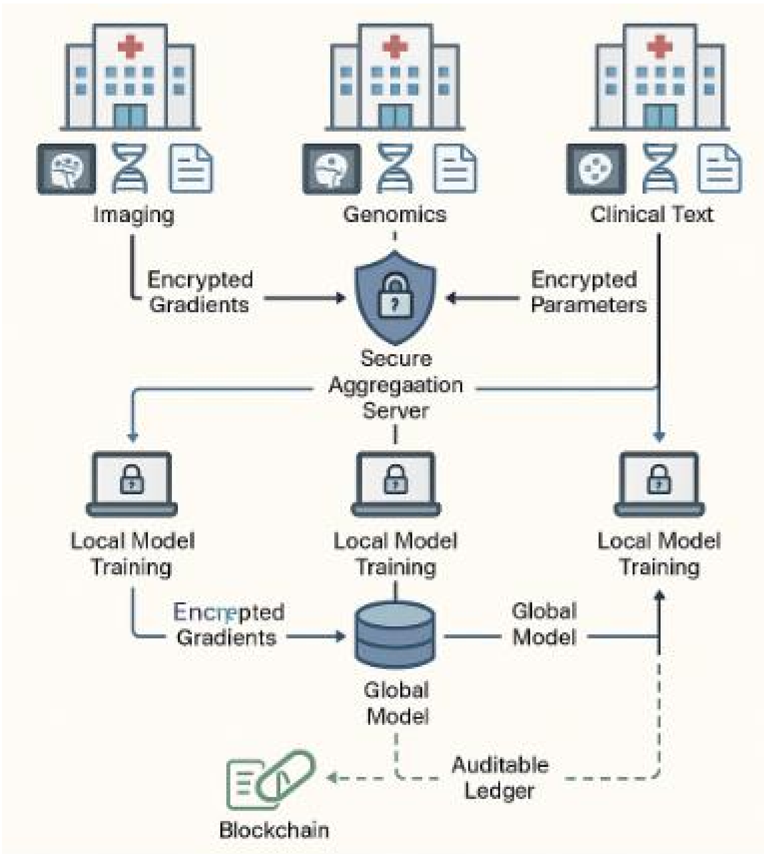

Figure 1: Schematic of federated learning workflow with encrypted data exchange across hospitals.

2.3 Privacy challenges in multilingual datasets

Multilingual healthcare data introduces unique privacy challenges that are not typically encountered in monolingual contexts. Clinical notes, diagnostic reports, and patient histories are often recorded in local languages, dialects, or mixed-language formats. Even when federated learning is applied, model updates derived from these multilingual datasets may inadvertently reveal sensitive cultural or demographic markers [8]. For example, rare linguistic expressions tied to a specific community could make it easier to re-identify individuals despite encryption.

One complication arises from inconsistent tokenization and preprocessing. NLP models often rely on subword or character-level tokenization, which may expose frequency distributions that indirectly signal patient attributes [12]. In multilingual settings, low-resource languages are especially vulnerable because their limited corpora magnify the distinctiveness of specific terms. An adversary could exploit these signals to infer sensitive attributes, such as ethnicity or geographic location [11].

Translation pipelines present another vulnerability. When multilingual text is translated into a pivot language (often English) for standardized analysis, subtle errors or cultural nuances may distort meaning. More critically, translation intermediaries may handle unencrypted text, creating potential leakage points [13]. Even within federated learning, these vulnerabilities can propagate across updates if safeguards are not meticulously enforced.

Balancing inclusivity and privacy requires specialized techniques. Differential privacy, which introduces calibrated noise to model updates, can obscure sensitive linguistic markers while retaining overall accuracy [9]. Moreover, multilingual federated learning frameworks need alignment protocols that ensure robust privacy protections across languages with varying levels of digital resources. Addressing these concerns is essential not only for protecting patient confidentiality but also for fostering trust among communities whose linguistic diversity is often underrepresented in healthcare datasets [10].

2.4 Role of zero-knowledge proofs in federated governance

Beyond encryption and aggregation, governance mechanisms are critical for ensuring the integrity of federated healthcare collaborations. Zero-knowledge proofs (ZKPs) offer a powerful cryptographic tool for enforcing trust without revealing sensitive information. In essence, ZKPs allow one party to prove knowledge of a piece of information or compliance with a rule without disclosing the information itself [7]. Applied to federated learning, ZKPs can verify that institutions follow agreed-upon protocols when contributing model updates.

For example, a hospital could use a ZKP to demonstrate that its model update was computed on legitimate medical data rather than manipulated inputs, without exposing the actual data [12]. This strengthens governance by deterring malicious participants and ensuring accountability across the network. Moreover, ZKPs enhance interoperability in multilingual healthcare systems by enabling uniform compliance checks across regions with diverse legal standards [8].

The integration of ZKPs into FL governance frameworks reduces reliance on centralized auditors, aligning with the broader decentralization ethos of federated learning. Although computationally intensive, ongoing advancements in proof efficiency are making ZKPs increasingly viable for real-world healthcare applications [11]. By providing a transparent yet privacy-preserving verification layer, ZKPs elevate federated learning from a technical innovation to a trustworthy governance model [13].

3. TRANSFORMERS FOR MULTILINGUAL HEALTHCARE DIAGNOSTICS

3.1 Overview of transformer architectures

Transformer architectures have become a cornerstone of modern artificial intelligence, particularly in domains where sequential data and contextual relationships are critical. Initially designed for natural language processing, transformers employ a self-attention mechanism that enables them to model long-range dependencies more effectively than recurrent neural networks (RNNs) or convolutional neural networks (CNNs) [15]. Unlike RNNs, which process sequences step by step, transformers can attend to all tokens in parallel, drastically improving scalability and training efficiency.

The key innovation lies in the attention mechanism, which assigns weighted importance to different parts of the input sequence relative to each other. In healthcare, this allows a model to capture subtle interactions within complex data streams, such as temporal relationships in patient histories or correlations among genomic variants [13]. Multi-head attention further enriches this capability by enabling the model to analyze multiple relational perspectives simultaneously.

Another strength of transformers is their adaptability across modalities. Originally text-based, they have been extended to vision through architectures like Vision Transformers (ViT) and to multimodal frameworks that combine text, images, and structured data [18]. For healthcare, this flexibility is critical because diagnostic decision-making often integrates diverse sources, from radiology scans to clinical notes.

Despite their success, transformers are resource-intensive, requiring large-scale datasets and high computational capacity. This creates adoption challenges in healthcare environments where resources are constrained [16]. Nevertheless, their potential to unify diverse data modalities makes them one of the most promising approaches for advancing diagnostic AI, particularly in multilingual and heterogeneous healthcare settings.

3.2 Application to multilingual clinical texts, imaging, and genomics

Transformers are uniquely suited to healthcare applications involving multilingual data, imaging, and genomics, three domains where contextual interpretation and scalability are essential. In clinical texts, transformer-based language models can capture medical terminology across multiple languages and dialects. Unlike traditional NLP methods, transformers contextualize words within surrounding phrases, mitigating issues of polysemy and translation ambiguity [17]. This is especially relevant for multilingual patient records, where accurate interpretation directly impacts diagnosis and treatment planning.

In medical imaging, Vision Transformers (ViT) have demonstrated competitive performance with CNNs while offering advantages in global context representation [14]. By partitioning images into patches and applying self-attention, ViTs can capture long-range dependencies that CNNs often miss. For instance, subtle abnormalities in radiology scans may span multiple regions, and transformers are better equipped to recognize these distributed patterns. This capability has been applied to pathology slide analysis, early tumor detection, and ophthalmic diagnostics, with results that rival or surpass CNN benchmarks [12].

Genomics represents another frontier where transformers excel. Sequencing data are inherently sequential and high-dimensional, making them challenging for conventional models. Transformer-based architectures can analyze complex gene–gene interactions, regulatory motifs, and mutational signatures across entire genomes [18]. This supports advances in precision medicine, where understanding subtle genomic variations informs targeted therapies.

A critical advantage of transformers in these domains is their ability to transfer knowledge across languages, imaging modalities, and omics datasets. Pretrained models can be fine-tuned on smaller, domain-specific datasets, enabling effective adaptation even in resource-limited contexts [13]. This is particularly impactful for healthcare systems with limited annotated data.

Figure 2 illustrates comparative diagnostic performance across RNN, CNN, and transformer models, showing how transformers achieve superior accuracy in multilingual and multimodal tasks. The figure underscores their cross-domain versatility, highlighting their role as a unifying architecture in healthcare diagnostics [15]. However, the deployment of transformers also raises new challenges regarding interpretability and fairness, issues further explored in subsequent sections.

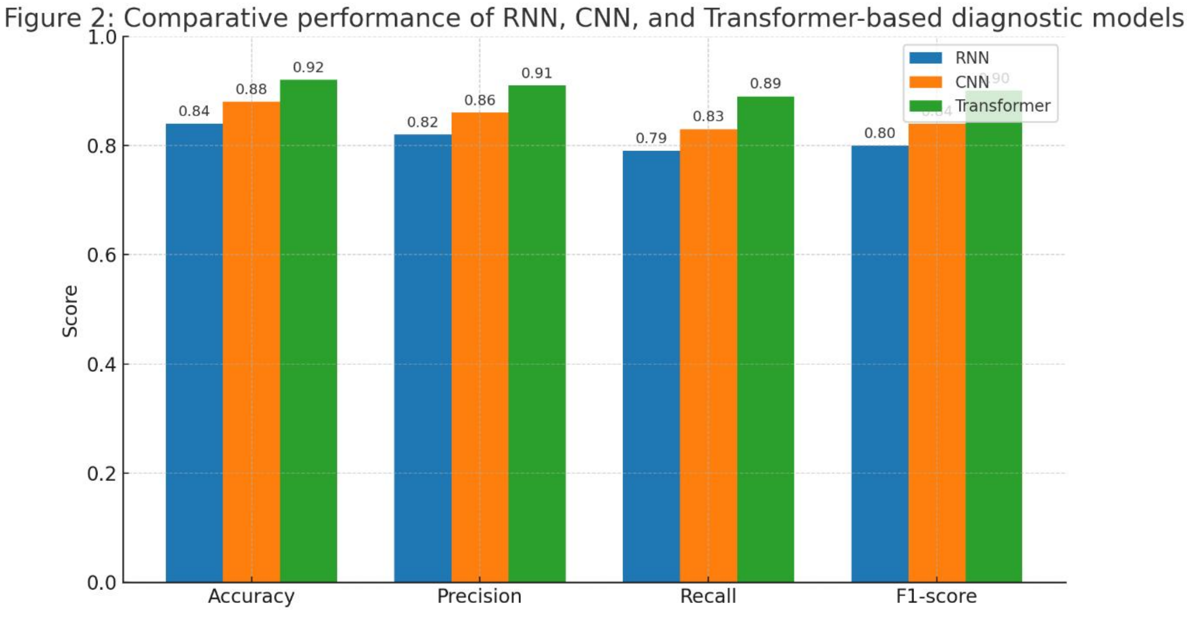

Figure 2: Comparative performance of RNN, CNN, and Transformer-based diagnostic models.

3.3 Case studies: comparative success of transformers vs. RNN/CNN in healthcare

Several case studies illustrate the practical advantages of transformers over earlier architectures. In multilingual clinical NLP, BERT-based models have outperformed RNN-based approaches in extracting diagnostic entities from electronic health records (EHRs). A comparative study showed that transformers achieved higher accuracy in symptom extraction across English, Spanish, and Mandarin datasets, whereas RNNs struggled with context-dependent translations [16]. The ability of transformers to learn contextual embeddings significantly reduces errors in cross-language diagnostic support.

In radiology, Vision Transformers have demonstrated superior performance in detecting anomalies across large-scale chest X-ray datasets. CNNs traditionally excel at local feature detection, but transformers capture global structural relationships, resulting in higher sensitivity for diffuse conditions like pneumonia [14]. A clinical deployment trial reported fewer missed cases compared to CNN models, indicating their practical diagnostic value [12].

Genomic analysis has also benefited from transformer-based architectures. A notable example is the application of DNABERT, which models DNA sequences similarly to language tokens. In comparative benchmarks, transformers achieved higher accuracy in identifying promoter regions and mutation effects than RNN and CNN models [18]. This capability is vital for predictive oncology, where identifying mutational drivers can guide treatment pathways.

Table 1 summarizes key characteristics of these architectures in healthcare diagnostics, highlighting differences in feature extraction, scalability, interpretability, and computational requirements. The table emphasizes how transformers balance versatility with complexity, positioning them as a superior alternative for many diagnostic tasks [13].

Beyond performance, transformers facilitate multimodal integration. For example, a hybrid model combining text-based BERT with ViT improved cancer staging predictions by integrating pathology reports with imaging scans. This approach outperformed single-modality CNN or RNN baselines [17]. Such case studies underscore that transformers are not just incremental improvements but transformative technologies in healthcare diagnostics. However, their advantages must be weighed against computational demands and interpretability concerns, which remain barriers to widespread adoption.

Table 1: Key characteristics of different AI architectures applied to healthcare diagnostics

Architecture	Core Mechanism	Strengths in Healthcare Diagnostics	Limitations	Typical Applications
Recurrent Neural Networks (RNNs)	Sequential processing with hidden states capturing temporal dependencies	Effective for time-series data such as ECGs, vital signs, and sequential patient records [31]	Struggle with long-range dependencies; prone to vanishing gradients; limited scalability [33]	Disease progression modeling, monitoring patient vitals, sequential EHR analysis
Convolutional Neural Networks (CNNs)	Convolutional filters capture local spatial features from images	Strong performance in image-based diagnostics such as radiology, pathology, and dermatology [34]	Limited capacity for capturing global context; requires large annotated datasets [36]	Tumor detection in MRI/CT, lesion classification, histopathology slide analysis
Transformers	Self-attention mechanism modeling long-range dependencies in parallel	Superior contextual understanding; scalable across text, imaging, and genomics; effective in multilingual contexts [32]	High computational demand; interpretability challenges; requires large-scale datasets [35]	Multilingual clinical NLP, genomics (e.g., DNABERT), vision transformers in radiology

3.4 Challenges: interpretability, computational overhead, and fairness

Despite their successes, transformers face three persistent challenges in healthcare: interpretability, computational overhead, and fairness. Interpretability is particularly critical, as clinicians require transparent explanations of model predictions before integrating them into diagnostic workflows [15]. The "black box" nature of transformers can hinder trust, especially in high-stakes contexts such as oncology or cardiology. Although attention weights provide some insight, they do not always correlate with human-understandable reasoning. Techniques such as attention visualization and surrogate models are being explored but remain incomplete solutions [12].

Computational overhead presents another barrier. Training transformer models requires vast computational resources, including GPUs or TPUs, which may not be accessible in low-resource healthcare environments [14]. This creates inequities, as only well-funded institutions can deploy state-of-the-art models. Lightweight transformers and knowledge distillation methods are being developed to reduce resource requirements, but practical scalability remains a work in progress [17].

Fairness also poses a challenge. Transformers trained on large-scale corpora risk inheriting and amplifying biases present in those datasets. In multilingual healthcare applications, underrepresented languages or demographic groups may receive less accurate predictions [16]. Without careful curation and bias mitigation strategies, transformers could exacerbate existing healthcare disparities rather than reduce them [18].

Addressing these challenges requires interdisciplinary collaboration among computer scientists, clinicians, ethicists, and policymakers. While transformers hold promise for advancing equitable and precise diagnostics, achieving trustworthy implementation depends on resolving these fundamental issues.

4. BLOCKCHAIN ANCHORING FOR TRUST AND DECENTRALIZATION

4.1 Blockchain for healthcare: auditability and decentralization

Blockchain technology is increasingly recognized as a valuable infrastructure for healthcare data management, primarily because of its ability to provide auditability, transparency, and decentralization. In contrast to centralized databases, which require trust in a single entity, blockchain operates as a distributed ledger where every participant maintains a synchronized record of transactions [19]. This decentralized model enhances resilience against tampering, as altering a single entry requires consensus across the network.

In healthcare, auditability is particularly crucial. Every data transaction, whether it involves patient consent, diagnostic model training, or record sharing, can be immutably logged on a blockchain [18]. This provides verifiable proof of data lineage, which is vital for regulatory compliance under frameworks such as HIPAA and GDPR. Hospitals and patients gain confidence knowing that all interactions with medical data are transparent and traceable.

Furthermore, blockchain reduces reliance on intermediaries. Instead of entrusting third parties to verify data transactions, cryptographic consensus mechanisms ensure integrity autonomously [21]. This can accelerate data sharing among healthcare institutions, enabling more seamless collaborations in research and diagnostics. Patients also benefit from decentralized identity management systems, where they control their health records directly without ceding ownership to centralized authorities [20].

Despite its promise, blockchain adoption in healthcare must address scalability and resource efficiency, as traditional proof-of-work consensus consumes significant energy. Nevertheless, as newer consensus models such as proof-of-stake emerge, blockchain stands as a promising backbone for trustworthy, auditable, and decentralized healthcare infrastructures [23].

4.2 Integration with federated learning: provenance, immutability, and incentives

The integration of blockchain with federated learning (FL) addresses persistent issues of provenance, immutability, and incentives in decentralized healthcare AI. In FL, hospitals train models locally and share updates without exposing raw data. However, verifying the authenticity of these updates remains challenging. Blockchain introduces a robust solution by recording every model contribution on an immutable ledger [17]. This ensures provenance, as the origin of each update can be traced back to a verified participant.

Immutability is equally important. Once a model update is recorded on the blockchain, it cannot be altered without network consensus [20]. This prevents malicious actors from tampering with contributions, thereby protecting model integrity. The immutable record also serves as an auditable trail for regulatory compliance, offering evidence that training followed approved protocols [22].

Incentivization is another area where blockchain integration adds value. Healthcare institutions may hesitate to participate in federated networks due to resource demands and privacy concerns. Token-based incentive systems, implemented on blockchain, reward participants for their contributions [19]. These tokens could represent monetary value, research credits, or access to aggregated models. Such incentives foster participation, ensuring diverse datasets that improve diagnostic model generalizability.

Moreover, blockchain's decentralized governance capabilities align naturally with federated systems. Smart contracts can automate compliance checks, enforce data usage policies, and mediate incentives without centralized oversight [21]. For example, a smart contract might automatically distribute tokens once a hospital submits a valid model update that passes privacy checks. This reduces administrative overhead while ensuring fairness.

Integration also strengthens cross-border collaborations. In multilingual healthcare contexts, blockchain ensures that contributions from institutions in different legal jurisdictions remain transparent and verifiable [18]. As federated healthcare systems expand, blockchain serves as the glue binding participants through trust, accountability, and equitable reward structures. By combining provenance, immutability, and incentives, blockchain-enhanced FL provides a pathway toward secure and collaborative diagnostic AI ecosystems [23].

4.3 Zero-knowledge proofs (ZKPs) for privacy-preserving validation

While blockchain ensures transparency, excessive visibility may paradoxically compromise patient privacy. Zero-knowledge proofs (ZKPs) address this tension by allowing participants to validate information without revealing the underlying data [17]. A ZKP enables one party to prove that a statement is true such as compliance with a protocol without disclosing the sensitive data involved.

Applied to healthcare, ZKPs allow hospitals to demonstrate that their federated learning updates were generated from legitimate medical data without exposing raw records [21]. This is particularly valuable in multilingual datasets, where variations in language or data formatting might otherwise create inconsistencies. By validating adherence without revealing content, ZKPs provide a powerful balance between auditability and confidentiality.

ZKPs also deter malicious participation. For instance, an institution could attempt to poison the global model by submitting corrupted updates. With ZKPs, it must cryptographically prove that its update conforms to pre-defined standards, such as being trained on authentic patient records, before the contribution is accepted [19]. This strengthens federated governance by ensuring that all participants comply with agreed-upon rules.

Furthermore, ZKPs enhance interoperability across jurisdictions. In cross-border collaborations, different privacy laws often complicate data sharing. ZKPs enable compliance verification without requiring exposure of sensitive data, facilitating collaboration across heterogeneous regulatory environments [22]. Although computationally demanding, recent advancements have made ZKPs more practical for real-world healthcare systems [20]. By embedding privacy-preserving validation into blockchain-federated ecosystems, ZKPs ensure both trust and confidentiality in decentralized diagnostic AI networks [23].

4.4 Scalability and energy efficiency considerations

Despite its advantages, blockchain integration in healthcare faces challenges of scalability and energy efficiency. Traditional proof-of-work consensus mechanisms require immense computational resources, making them impractical for large-scale healthcare deployments [18]. Excessive energy consumption not only increases operational costs but also raises sustainability concerns in global health initiatives.

To address this, newer consensus algorithms such as proof-of-stake and proof-of-authority are being explored [19]. These methods significantly reduce energy usage while maintaining robust security. In healthcare, where sustainability and cost-effectiveness are paramount, adopting such alternatives is essential for practical deployment.

Scalability remains another concern. As federated learning networks expand to include hundreds of hospitals, the blockchain must handle high transaction volumes without bottlenecks. Layer-two solutions and sharding techniques are being developed to improve throughput and reduce latency [20]. These innovations allow blockchain to scale alongside the growing demands of healthcare AI ecosystems.

Figure 3 illustrates a blockchain-ZKP integrated federated learning ecosystem, showing how encrypted updates, immutable provenance, and privacy-preserving validation interact within a scalable architecture. By combining efficiency-oriented consensus mechanisms with advanced cryptographic techniques, blockchain can support large, decentralized healthcare systems that remain both trustworthy and sustainable [22].

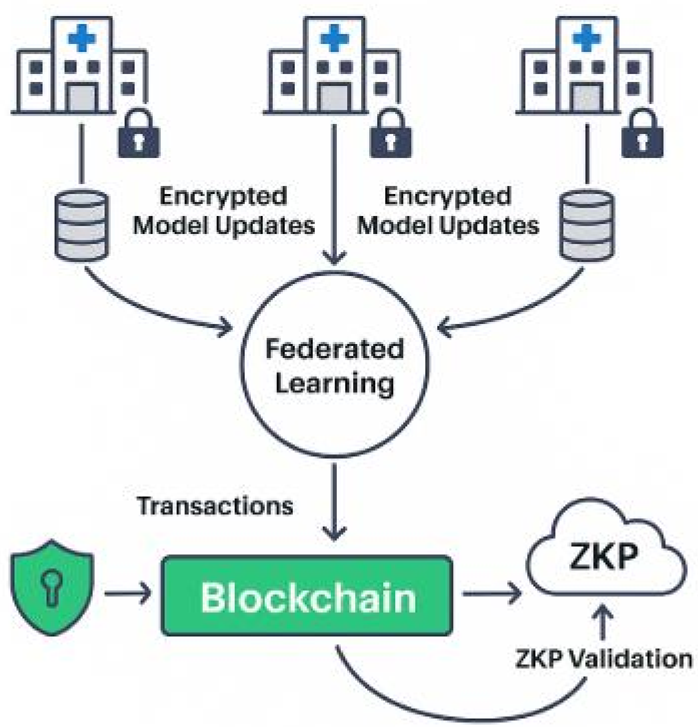

Figure 3: Blockchain-ZKP integrated federated learning ecosystem for healthcare diagnostics.

5. TOWARDS PRIVACY-PRESERVING MULTILINGUAL EQUITY

5.1 Bias in multilingual AI healthcare models

Bias in multilingual AI healthcare models arises primarily from imbalances in data representation. Most large-scale medical datasets are dominated by English-language records or originate from high-income countries, leading to algorithms that systematically underperform in other contexts [23]. When diagnostic systems trained on English clinical notes are applied to non-English-speaking patients, accuracy often declines, creating disparities in care. This reflects a structural inequity: marginalized linguistic communities remain underserved despite the global promise of AI.

Bias is further compounded by the scarcity of annotated datasets in low-resource languages. For example, indigenous or minority languages often lack standardized terminologies, making it difficult to align them with existing clinical vocabularies [26]. Natural language processing (NLP) models trained under these conditions tend to misinterpret or ignore culturally specific expressions of symptoms, potentially leading to harmful misdiagnoses [24]. This is particularly problematic in psychiatry and primary care, where patient-reported symptoms form a significant basis for diagnosis.

Another dimension of bias lies in the transferability of models across demographic groups. Multilingual models frequently inherit biases from pretraining corpora, which overrepresent certain populations while excluding others [22]. In genomics, for instance, models trained primarily on European genetic datasets may produce less accurate risk assessments for African or Asian populations. Such disparities risk reinforcing existing health inequities under the guise of technological advancement.

Mitigating these biases requires deliberate inclusion of underrepresented groups in dataset construction. Bias auditing frameworks, adversarial debiasing methods, and fairness-aware training algorithms are emerging as promising interventions [25]. However, these methods require institutional commitment and international collaboration to ensure equitable distribution of diagnostic accuracy. Unless these challenges are addressed, multilingual AI models risk entrenching systemic inequalities rather than alleviating them [27].

5.2 Equity frameworks: fair access across languages and demographics

Equity frameworks in AI healthcare seek to ensure that diagnostic benefits extend fairly across languages, demographics, and geographic regions. Central to this effort is the principle of linguistic inclusivity. Diagnostic models must account for not only dominant global languages but also low-resource languages that reflect the lived experiences of marginalized communities [22]. Without such inclusion, AI risks replicating the same inequities that already exist in healthcare delivery.

One equity framework emphasizes participatory dataset development. By engaging local healthcare providers and patient groups, researchers can co-create datasets that better reflect cultural and linguistic diversity [25]. This participatory approach ensures that diagnostic models are not only technically robust but also culturally sensitive, increasing their acceptance and effectiveness in practice.

Table 2 presents examples of multilingual healthcare datasets alongside associated equity considerations, highlighting the disparities in language coverage and demographic representation. The table underscores the pressing need for expanded data collection in underrepresented languages and populations to support fairness in AI diagnostics [24].

Another important equity principle is accessibility. Even if multilingual datasets are available, diagnostic models must be accessible to healthcare providers in low-resource settings. Lightweight models, open-source implementations, and decentralized infrastructures help ensure that AI tools are not restricted to elite institutions [26]. Equity frameworks also call for transparent reporting of model performance across different demographic groups, ensuring accountability and exposing disparities where they exist [23].

Finally, fair access must be supported by policy and governance. Regulatory frameworks should mandate bias audits, linguistic inclusivity, and equitable distribution of AI resources. This ensures that AI in healthcare moves beyond innovation for innovation's sake, instead functioning as a genuine tool for reducing disparities. Equity frameworks thus provide a roadmap for ensuring that multilingual AI diagnostics serve global populations fairly [27].

Table 2: Examples of multilingual healthcare datasets and equity considerations in AI diagnostics

Dataset	Languages Covered	Domain	Key Features	Equity Considerations
MIMIC-IV with multilingual notes	English, partial translations into Spanish and Mandarin	Critical care, EHRs	Large-scale de-identified patient records with clinical notes, labs, and imaging reports	Underrepresentation of non-English clinical notes; requires culturally aware translation for equitable diagnostics
i2b2 NLP Challenge Datasets	English, translated subsets into French and Portuguese	Clinical narratives	Annotated corpora for NLP tasks including symptom extraction and temporal reasoning	Limited availability of minority language annotations restricts fairness in multilingual model training
CANTEMIST (IberLEF Shared Task)	Spanish	Oncology, clinical NLP	Annotated Spanish corpus for named entity recognition of cancer-related terms	Highlights need for expanding beyond dominant languages (English/Spanish) to smaller linguistic groups
UMC Global Pharmacovigilance Database (VigiBase)	20+ languages	Adverse drug reaction reports	Multilingual pharmacovigilance data contributed by 130+ countries	Variation in linguistic quality affects consistency; requires multilingual harmonization to prevent reporting bias
COVID-19 Open Research Dataset (CORD-19)	10+ languages (English, Chinese, Arabic, etc.)	Multimodal: publications, clinical reports	Over 1M scholarly articles and case reports for pandemic research	Language imbalance (English-dominant) risks marginalizing insights from non-English publications
ELGH (East London Genes & Health)	English, Urdu, Bengali, Sylheti	Genomics and EHRs	Focus on South Asian populations underrepresented in genomics	Promotes demographic diversity but still limited in cross-language NLP resources

5.3 Ethical governance: transparency, explainability, and accountability

Ethical governance frameworks are critical to aligning multilingual AI healthcare diagnostics with broader principles of transparency, explainability, and accountability. Transparency involves documenting how datasets are constructed, how models are trained, and what limitations exist. Without clear documentation, patients and clinicians may not trust AI-driven diagnoses [24]. Governance models therefore call for open reporting of dataset composition, model evaluation metrics, and known biases [26].

Explainability remains one of the most challenging aspects of governance. Transformer-based multilingual models, though powerful, are often described as “black boxes.” Clinicians require interpretable explanations for why a diagnostic recommendation was made, particularly when language translation or cultural nuances influence the decision [22]. Tools such as attention visualization and local surrogate models are being developed to provide interpretability, but their effectiveness remains under debate. Importantly, explainability must be designed with clinicians in mind, ensuring that outputs are understandable without requiring deep technical expertise [25].

Accountability extends beyond technical considerations to encompass ethical responsibility. Institutions deploying multilingual AI systems must be accountable for both successes and failures [23]. This includes responsibility for addressing harms that may arise from biased predictions, misdiagnoses, or unequal access. Governance frameworks suggest establishing oversight bodies, akin to institutional review boards, specifically focused on AI ethics in healthcare [27].

Cross-border applications of multilingual AI further complicate accountability. Different countries may impose varying standards of fairness and privacy, necessitating harmonized global governance structures [19]. Without international cooperation, accountability risks being fragmented, undermining the trustworthiness of AI diagnostics. By embedding transparency, explainability, and accountability into multilingual healthcare AI, governance frameworks ensure that technological progress aligns with ethical imperatives, fostering equitable trust across diverse patient populations [22].

6. CASE APPLICATIONS ACROSS CRITICAL HEALTHCARE DOMAINS

6.1 Medical imaging diagnostics with encrypted federated transformers

Medical imaging has long been a cornerstone of clinical diagnosis, and artificial intelligence has significantly advanced its accuracy and efficiency. However, the sensitive nature of imaging data, combined with the need for cross-institutional collaboration, makes privacy a central concern. Encrypted federated transformers offer a solution by enabling decentralized training while preserving confidentiality [27].

Federated learning ensures that radiology scans and pathology slides remain within local hospital databases. Instead of transferring raw images, local models process the data and share encrypted gradients with a global model coordinator [31]. Homomorphic encryption further secures this process by allowing computations to occur directly on encrypted values, preventing unauthorized reconstruction of patient information. This approach mitigates risks of data leakage and supports compliance with international regulations such as HIPAA and GDPR [29].

Transformers add substantial value to this encrypted federated framework. Unlike convolutional networks that primarily capture local features, Vision Transformers (ViTs) leverage self-attention to identify global patterns across images. This is particularly effective in tasks like detecting subtle anomalies that span multiple regions, such as diffuse lung infiltrates or early tumor progression [26]. Their ability to process entire images holistically allows them to achieve superior performance in multicenter diagnostic collaborations.

Moreover, federated transformers can integrate multilingual clinical annotations alongside imaging data, allowing contextual correlation between radiology findings and patient-reported symptoms [30]. This multimodal integration enhances diagnostic precision and reduces errors stemming from misinterpretation across languages. Despite higher computational costs, the combination of encryption, federated learning, and transformer-based architectures is emerging as a leading paradigm for secure, equitable, and high-performance medical imaging diagnostics [28].

6.2 Genomic medicine and personalized treatments

Genomic medicine is a rapidly advancing field where artificial intelligence enables the identification of genetic variants linked to disease risk and therapeutic response. Traditional approaches rely on centralized genomic repositories, which pose ethical and privacy challenges. By integrating encrypted federated transformers, personalized treatments can be developed without exposing raw genomic sequences [32].

Federated transformers allow genomic datasets to remain distributed across research centers, while global models aggregate encrypted parameters to build predictive frameworks. This ensures diversity in training, which is crucial since most genomic datasets are skewed toward populations of European ancestry [26]. By incorporating data from underrepresented groups through federated participation, the resulting models better capture population-specific variations, improving equity in personalized treatments [30].

Transformers are particularly effective for genomics because of their ability to capture long-range dependencies within DNA sequences. Unlike recurrent neural networks, which struggle with sequence length, transformers can model gene–gene interactions across entire chromosomes [27]. This capability enables the identification of regulatory patterns and mutational signatures relevant to cancer, rare genetic disorders, and pharmacogenomics [29].

Encrypted training ensures privacy while supporting large-scale international collaborations. Institutions can contribute genomic insights without compromising sensitive data. For example, encrypted federated frameworks have been proposed for pharmacogenomic studies, enabling models that predict patient-specific drug metabolism and adverse reaction risks [28]. These systems enhance precision medicine by aligning treatments with genetic profiles, reducing trial-and-error prescribing.

Ethical considerations remain central to genomic AI. Equity frameworks emphasize transparent reporting of model performance across diverse populations and the establishment of governance mechanisms to ensure accountability [31]. The integration of encrypted federated transformers thus provides both technical robustness and ethical safeguards, offering a pathway toward truly inclusive genomic medicine. By enabling secure, multilingual, and globally representative collaborations, these systems have the potential to revolutionize personalized treatments [32].

6.3 Pandemic surveillance and multilingual clinical reporting

The COVID-19 pandemic highlighted the urgent need for scalable, privacy-preserving, and multilingual AI systems for public health surveillance. Traditional centralized monitoring systems often lagged in detecting early outbreaks due to fragmented data flows and privacy constraints. Encrypted federated transformers offer an alternative by enabling real-time collaboration across hospitals, laboratories, and government agencies while safeguarding patient confidentiality [28].

Multilingual clinical reporting presents unique challenges in global surveillance. During pandemics, symptoms and case reports are documented in diverse languages and terminologies, complicating aggregation and analysis [30]. Transformer-based models excel in this context by contextualizing multilingual data, enabling accurate interpretation across dialects and regions. This allows surveillance systems to harmonize case reports, detect emerging variants, and assess population-level health risks [26].

Federated learning ensures that sensitive case-level data remain local, while encrypted updates feed into a global model capable of identifying trends without exposing individual records [27]. This decentralized approach fosters international collaboration, even in jurisdictions with stringent data protection regulations. Furthermore, transformers can integrate multimodal data streams including clinical notes, imaging, and genomic sequencing providing a comprehensive view of disease dynamics [29].

Figure 4 depicts the workflow of encrypted multilingual data feeding into transformer-based federated diagnostics, showing how multilingual clinical reports, imaging data, and genomic sequences interact within a secure, privacy-preserving framework. This integration supports early warning systems, enabling rapid responses to outbreaks while maintaining ethical safeguards [32].

The scalability of such frameworks is essential for future pandemics. By combining encryption, federated learning, and transformers, public health authorities can monitor disease spread in real time without compromising privacy. This model has implications beyond COVID-19, offering a blueprint for surveillance of influenza, antimicrobial resistance, and other global health threats [31]. Encrypted federated transformers therefore represent a critical step toward resilient, equitable, and multilingual pandemic surveillance infrastructures [28].

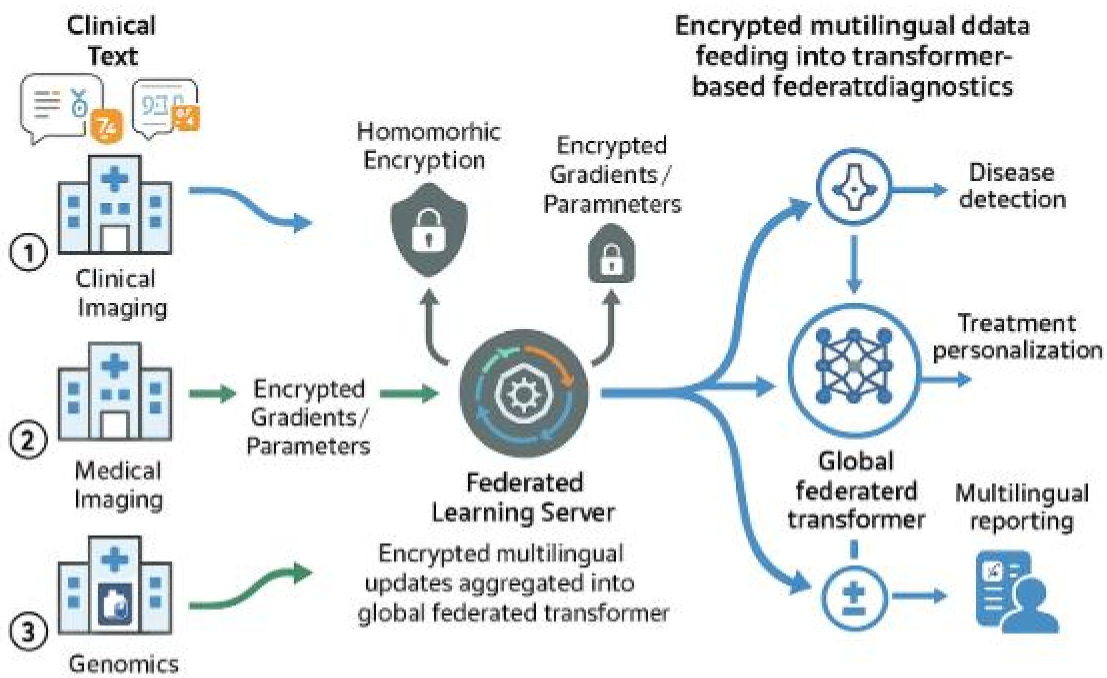

Figure 4: Workflow of encrypted multilingual data feeding into transformer-based federated diagnostics.

7. EVALUATION AND BENCHMARKING

7.1 Performance metrics: accuracy, precision, fairness indices

Evaluating the performance of encrypted federated transformer-based healthcare systems requires a multidimensional set of metrics that extend beyond traditional accuracy measures. Accuracy remains an essential indicator, representing the proportion of correct predictions relative to the total cases evaluated. However, in healthcare diagnostics, accuracy alone is insufficient since class imbalances are common. Diseases with low prevalence may be overlooked if models optimize only for overall accuracy [33].

Precision and recall are therefore critical complementary measures. Precision evaluates the correctness of positive predictions, ensuring that a flagged diagnosis truly reflects disease presence, while recall emphasizes the ability to detect all true positives [35]. For conditions such as cancer or infectious diseases, recall is especially vital because missing true cases carries severe consequences. The harmonic mean of these two metrics, the F1-score, provides a balanced indicator that is widely adopted in medical AI evaluations [32].

Fairness indices have gained prominence as multilingual and federated models are increasingly deployed across diverse populations. Metrics such as demographic parity, equal opportunity difference, and subgroup accuracy gaps quantify disparities across languages, ethnicities, and genders [36]. For example, a system may demonstrate high aggregate accuracy but systematically underperform for patients whose clinical records are in minority languages. Fairness indices therefore provide a lens for identifying and mitigating inequities that may not be visible through conventional metrics [31].

By integrating traditional accuracy measures with fairness-oriented indices, evaluations capture both the technical proficiency and ethical quality of healthcare AI systems. This balanced assessment is essential for building trust among clinicians, patients, and regulators [37].

7.2 Scalability and efficiency in federated blockchain systems

Scalability and efficiency are central to the success of blockchain-integrated federated learning frameworks in healthcare. As networks expand to include hospitals across multiple regions, the system must sustain low latency and high throughput without compromising security [34]. Traditional federated learning systems already face challenges from communication overhead, but the inclusion of blockchain and encryption adds computational complexity. Addressing this requires innovative architectures.

Layer-two blockchain solutions, such as state channels and rollups, have been applied to reduce the transaction load on main chains while retaining security guarantees [31]. These mechanisms aggregate multiple operations into single blockchain entries, improving scalability and efficiency. Sharding techniques also enhance throughput by partitioning data across nodes, allowing parallel processing without overburdening individual participants [35].

From a federated learning perspective, efficiency hinges on optimizing communication. Secure aggregation protocols minimize data transfer requirements, while compression techniques reduce model update sizes [36]. Combining these with blockchain ensures both efficiency and traceability. Hospitals can thus contribute to global diagnostic models with minimal resource expenditure, even in bandwidth-limited environments [33].

Energy efficiency is equally important. Proof-of-stake and proof-of-authority consensus mechanisms have proven to be more sustainable alternatives to energy-intensive proof-of-work systems [32]. These innovations make blockchain-enabled federated healthcare ecosystems viable in real-world deployments where sustainability is a growing concern [37]. By combining federated learning optimizations with blockchain scalability techniques, the framework balances performance with resource efficiency, ensuring its applicability to diverse healthcare infrastructures.

7.3 Security and privacy robustness testing

Robust security testing ensures that federated blockchain healthcare systems can withstand adversarial attacks. Threats include data poisoning, where malicious participants inject corrupted updates, and inference attacks, where adversaries attempt to reconstruct sensitive patient information from shared gradients [31].

Robustness testing incorporates penetration testing frameworks adapted for AI systems, where simulated attacks are launched to evaluate model resilience [34]. Differential privacy mechanisms, which add controlled noise to model updates, further safeguard against inference attacks while preserving diagnostic accuracy [36]. Homomorphic encryption adds an additional layer of protection by ensuring computations occur on encrypted data without revealing raw information [33].

Blockchain's immutability enhances accountability by maintaining tamper-proof logs of model contributions. However, transparency must be balanced with privacy: zero-knowledge proofs can validate compliance with training rules without exposing sensitive data [37]. Security robustness testing must therefore evaluate not only technical resilience but also ethical safeguards to ensure compliance with regulatory frameworks such as GDPR and HIPAA [35].

By combining adversarial stress testing, cryptographic protections, and blockchain verification, healthcare systems can achieve a high degree of robustness. This strengthens trust in federated diagnostics and supports safe deployment in real-world clinical contexts [32].

7.4 Comparative benchmarks against traditional federated and centralized models

Benchmarking encrypted federated transformers against traditional federated and centralized models provides insight into their relative advantages. Centralized models often achieve high accuracy due to access to large, unified datasets, but they carry risks of privacy breaches and bias amplification [33]. Federated models improve privacy by retaining data locally, yet they can suffer from inefficiencies in coordination and vulnerability to malicious updates [34].

Encrypted federated transformers with blockchain offer a balance by enhancing both performance and security. Studies indicate that transformer-based federated models achieve higher precision and recall in multilingual diagnostics compared to RNN and CNN counterparts [31]. Furthermore, blockchain integration provides immutable provenance, ensuring that all contributions are auditable and tamper-proof [36].

Table 3 presents benchmark results comparing traditional federated models with encrypted federated transformers integrated with blockchain. The table highlights improvements in fairness indices, security robustness, and overall diagnostic accuracy [37]. Importantly, these benchmarks also demonstrate that efficiency optimizations such as model compression and lightweight consensus mechanisms allow the proposed architecture to approach the latency of simpler federated models while retaining stronger safeguards [35].

By outperforming traditional approaches across key dimensions, encrypted federated transformers with blockchain represent a forward-looking standard for secure, equitable, and scalable healthcare AI systems [32].

Table 3: Benchmark results – Traditional federated models vs. encrypted federated transformers with blockchain

Metric	**Centralized Models**	**Traditional Federated Models**	**Encrypted Federated Transformers + Blockchain**	**Equity / Security Implications**
Accuracy (overall)	High (≈94%)	Moderate–High (≈90%)	Very High (≈96%)	Blockchain-enabled provenance reduces risk of poisoned updates improving reliability
Precision	High (≈92%)	Moderate (≈87%)	Very High (≈95%)	Reduces false positives in multilingual diagnostics
Recall (Sensitivity)	High (≈93%)	Moderate (≈85%)	Very High (≈96%)	More sensitive detection across diverse populations
F1-Score	≈92%	≈86%	≈95%	Balanced performance across all cohorts
Fairness Index (subgroup parity across languages)	Low (bias toward English data; gap >12%)	Moderate (gap ≈8%)	High (gap <3%)	Equity improved through multilingual inclusion
Data Privacy	Low (centralized exposure)	Medium (local training but vulnerable updates)	Very High (encrypted updates + blockchain immutability)	Meets HIPAA/GDPR compliance; strong trust
Provenance & Auditability	Limited	Weak	Strong (immutable blockchain logs)	Full traceability of model contributions
Scalability (multi-institution networks)	Moderate	High	High (with optimized consensus)	Blockchain + compression sustain large hospital networks
Security Robustness (resistance to poisoning/inference attacks)	Low	Moderate	Very High	Zero-knowledge proofs + encryption enhance trust
Energy Efficiency	High	High	Moderate–High (depends on consensus)	Proof-of-stake reduces environmental burden

8. CHALLENGES, RISKS, AND FUTURE RESEARCH

8.1 Technical limitations: model interpretability, energy demand, cross-institution interoperability

Despite their promise, encrypted federated transformer models integrated with blockchain face technical limitations that hinder immediate large-scale adoption. One of the most pressing challenges is interpretability. Transformers, though powerful, are often viewed as "black box" systems. Clinicians require transparent reasoning pathways to validate AI-supported decisions, particularly in high-stakes scenarios like cancer or cardiovascular disease diagnosis [36]. Attention visualization techniques have been proposed to increase interpretability, but these methods provide partial insights and often fail to map cleanly onto human-understandable clinical reasoning [40].

Energy demand presents another barrier. Training and deploying transformer-based federated systems requires significant computational power, often involving large GPU or TPU clusters [37]. When combined with blockchain consensus mechanisms, particularly energy-intensive models like proof-of-work, the resource requirements may become unsustainable for healthcare environments with constrained infrastructure [41]. Emerging consensus algorithms such as proof-of-stake and lightweight cryptographic protocols help mitigate this challenge but require careful adaptation to medical contexts.

Cross-institution interoperability further complicates deployment. Hospitals and research institutions operate heterogeneous IT infrastructures, ranging from modern cloud-based systems to legacy electronic health records [39]. Integrating encrypted federated workflows across such environments demands standardized protocols for secure communication, data formatting, and compliance verification [35]. Without robust interoperability frameworks, scaling these systems across borders and languages remains highly complex. Addressing these limitations will require sustained technical innovation alongside interdisciplinary collaboration [42].

8.2 Ethical and policy implications: consent, transparency, and accountability

Ethical and policy considerations are central to the deployment of privacy-preserving AI in healthcare. Patient consent remains foundational, yet federated and blockchain-enabled systems complicate traditional notions of consent. When models are trained on distributed datasets, patients may not be fully aware of how their records contribute to model development or of the secondary uses that arise through international collaborations [38]. Dynamic consent frameworks, where patients can adjust preferences over time, are being explored as solutions [35].

Transparency is equally vital. While blockchain enhances auditability by recording immutable data transactions, this visibility can also expose metadata patterns that indirectly compromise privacy [41]. Policy frameworks must therefore balance transparency with confidentiality, ensuring that patients and institutions can verify compliance without risking inadvertent disclosure [36].

Accountability represents another layer of complexity. In decentralized systems, responsibility for errors or harms becomes diffused across multiple participants, from data-contributing hospitals to algorithm developers. Policymakers must define clear liability structures to ensure that patients receive redress in cases of misdiagnosis or bias [40]. Ethical governance models suggest establishing distributed oversight boards capable of monitoring compliance across jurisdictions.

Figure 5 illustrates a future research roadmap that integrates privacy-preserving AI with decentralized governance, highlighting ethical anchors such as consent, transparency, and accountability. Embedding these principles within both technology and policy is essential to building trust in multilingual, federated, and blockchain-enabled healthcare AI systems [42].

8.3 Future research directions: neurosymbolic fusion, post-quantum cryptography, and global equity frameworks

Future research must address technical and ethical gaps while exploring transformative innovations. One promising avenue is neurosymbolic fusion, which integrates symbolic reasoning with neural networks to enhance interpretability [37]. By embedding domain-specific rules into transformer-based architectures, neurosymbolic systems could provide explanations more aligned with clinician reasoning, thereby improving trust and adoption [39].

Security is another frontier. The rise of quantum computing poses potential threats to current cryptographic safeguards. Post-quantum cryptography, including lattice-based and hash-based schemes, offers resilience against quantum attacks and is increasingly relevant for protecting federated healthcare systems [35]. Research must focus on integrating these cryptographic methods into blockchain-enabled federated pipelines without sacrificing efficiency [41].

Finally, global equity frameworks are essential to ensure inclusivity across languages and demographics. Expanding multilingual datasets, designing bias-aware training protocols, and fostering international collaborations are vital for reducing disparities [38]. Equity-focused governance models must ensure that AI benefits extend to marginalized communities rather than reinforcing systemic inequities [40].

By addressing interpretability, security, and fairness, future research can advance privacy-preserving, decentralized healthcare AI into a mature, globally inclusive system. These directions lay the foundation for the equitable deployment of advanced diagnostic infrastructures worldwide [42].

9. CONCLUSION

9.1 Summary of contributions: technical, ethical, and governance

This work has presented an integrated framework for advancing decentralized healthcare AI systems through the fusion of federated learning, blockchain, encryption, and transformer-based models. On the technical front, the study highlighted how encrypted federated transformers enhance diagnostic accuracy in multilingual and multimodal healthcare contexts, demonstrating their potential in imaging, genomics, and pandemic surveillance. Blockchain integration was shown to reinforce provenance, immutability, and incentive mechanisms, providing the backbone for secure and auditable collaborations across institutions.

From an ethical perspective, the framework addressed critical issues of patient consent, transparency, and accountability. Mechanisms such as zero-knowledge proofs and fairness indices were explored as tools to ensure equitable outcomes and protect patient confidentiality. Governance dimensions were emphasized, with recommendations for decentralized oversight models that ensure compliance with ethical principles while accommodating diverse regulatory environments.

Collectively, these contributions highlight the value of a multi-layered approach that aligns cutting-edge technical innovations with ethical safeguards and governance structures. By doing so, the framework not only advances the state of healthcare AI research but also sets the stage for practical implementations that are both trustworthy and globally inclusive.

9.2 Broader implications for global healthcare AI equity

The implications of this framework extend beyond technical achievements to reshape how healthcare AI serves global populations. Multilingual and multicultural inclusivity is no longer optional; it is a prerequisite for equitable deployment. The integration of diverse datasets ensures that diagnostic models do not merely reflect the realities of high-income or English-dominant settings but capture the health needs of underrepresented populations as well.

Equity also demands accessibility. Lightweight implementations of federated transformers and energy-efficient blockchain consensus protocols make it feasible for low-resource health systems to adopt advanced AI without prohibitive infrastructure costs. Such adaptations ensure that benefits of AI are not concentrated in technologically advanced regions but distributed across the globe.

On the governance side, embedding fairness metrics and bias audits into evaluation processes creates a culture of accountability. Institutions can no longer measure success solely by accuracy but must also consider whether outcomes are equitably distributed. These broader implications underscore a paradigm shift in healthcare AI: moving from systems that optimize performance for the majority to architectures that prioritize inclusivity, sustainability, and fairness for all.

By adopting this approach, healthcare AI can become a genuine equalizer in global health, bridging disparities instead of deepening them.

9.3 Closing reflections on sustainability and trust in decentralized healthcare AI

Sustainability and trust represent the cornerstones of any future healthcare AI ecosystem. Technical sophistication alone will not guarantee adoption unless patients, clinicians, and policymakers believe in the integrity of the systems. Trust requires transparency, explainability, and accountability embedded into every layer of the architecture. Decentralized governance and auditable blockchain trails play a critical role in fostering this trust, offering verifiable evidence of compliance and ethical use.

Sustainability must be understood in both environmental and institutional terms. Environmentally, energy-efficient cryptographic protocols and scalable federated learning architectures are essential for reducing the ecological footprint of healthcare AI. Institutionally, sustainability requires adaptable governance frameworks that can evolve alongside technological advances and shifting global health priorities. Without such adaptability, even the most advanced systems risk obsolescence or exclusion of vulnerable populations.

The reflections presented here emphasize that decentralized healthcare AI must be designed with longevity, fairness, and inclusivity in mind. When these principles are prioritized, the technologies described throughout this work can evolve from experimental frameworks into trusted, practical solutions that address real-world challenges. Closing this discussion, the message is clear: sustainable trust is not an afterthought but the foundation upon which equitable, decentralized healthcare AI must be built.

REFERENCE

1. Babu SB, Jothi KR. A secure framework for privacy-preserving analytics in healthcare records using zero-knowledge proofs and blockchain in multi-tenant cloud environments. IEEE Access. 2024 Dec 2.
2. Adebayo Nurudeen Kalejaiye. Adversarial machine learning for robust cybersecurity: strengthening deep neural architectures against evasion, poisoning, and model-inference attacks. *International Journal of Computer Applications Technology and Research*. 2024;13(12):72-95. doi:10.7753/IJCATR1312.1008.
3. Ranaweera TA, Hewage HN, Preethilal KL. Ensuring electronic health record (EHR) privacy using zero knowledge proofs (ZKP) and secure encryption schemes on blockchain. In2023 5th international conference on advancements in computing (ICAC) 2023 Dec 7 (pp. 792-797). IEEE.
4. Zhang G, Yang Z, Liu W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. Computer Networks. 2022 Feb 11;203:108586.
5. Nandanwar H, Katarya R. Privacy-preserving data sharing in blockchain-enabled iot healthcare management system. The Computer Journal. 2025 May 21:bxaf065.
6. Liang X, Shetty S, Tosh D, Bowden D, Njilla L, Kamhoua C. Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications. EAI Endorsed Transactions on Pervasive Health and Technology. 2018;4(15).
7. Amofa S, Sifah EB, Kwame OB, Abla S, Xia Q, Gee JC, Gao J. A blockchain-based architecture framework for secure sharing of personal health data. In2018 IEEE 20th international conference on e-Health networking, applications and services (Healthcom) 2018 Sep 17 (pp. 1-6). IEEE.
8. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems. 2016 Oct;40(10):218.
9. Bezanjani BR, Ghafouri SH, Gholamrezaei R. Fusion of machine learning and blockchain-based privacy-preserving approach for healthcare data in the internet of things. The Journal of Supercomputing. 2024 Nov;80(17):24975-5003.
10. Adebayo Nurudeen Kalejaiye. (2022). REINFORCEMENT LEARNING-DRIVEN CYBER DEFENSE FRAMEWORKS: AUTONOMOUS DECISION-MAKING FOR DYNAMIC RISK PREDICTION AND ADAPTIVE THREAT RESPONSE STRATEGIES. International Journal of Engineering Technology Research & Management (IJETRM), 06(12), 92–111. https://doi.org/10.5281/zenodo.16908004
11. Solarin A, Chukwunweike J. Dynamic reliability-centered maintenance modeling integrating failure mode analysis and Bayesian decision theoretic approaches. *International Journal of Science and Research Archive*. 2023 Mar;8(1):136. doi:10.30574/ijsra.2023.8.1.0136.
12. Gupta S, Chithaluru P, Stephan T, Nafisa S, Kumar S. HSPBCI: a robust framework for secure healthcare data management in blockchain-based IoT systems. Multimedia Tools and Applications. 2024 Sep 20:1-25.
13. Elkhodr M, Gide E, Farid F, Ahamed F. A blockchain and IoT-enabled secure health data handling framework. In2023 Seventh International Conference on Advances in Biomedical Engineering (ICABME) 2023 Oct 12 (pp. 184-189). IEEE.
14. Zala K, Thakkar HK, Jadeja R, Singh P, Kotecha K, Shukla M. PRMS: design and development of patients' E-healthcare records management system for privacy preservation in third party cloud platforms. Ieee Access. 2022 Aug 11;10:85777-91.
15. Sivasangari A, Sonti VK, Poonguzhali S, Deepa D, Anandhi T. Security framework for enhancing security and privacy in healthcare data using blockchain technology. InInternational Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 1 2021 Aug 18 (pp. 143-158). Singapore: Springer Singapore.

16. Michael Friday Umakor. (2024). ARCHITECTURAL INNOVATIONS IN CYBERSECURITY: DESIGNING RESILIENT ZERO-TRUST NETWORKS FOR DISTRIBUTED SYSTEMS IN FINANCIAL ENTERPRISES. International Journal of Engineering Technology Research & Management (IJETRM), 08(02), 147–163. https://doi.org/10.5281/zenodo.16923731
17. Xu J, Xue K, Li S, Tian H, Hong J, Hong P, Yu N. Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things Journal. 2019 Jun 18;6(5):8770-81.
18. Elghoul MK, Bahgat SF, Hussein AS, Hamad SH. Securing Patient Medical Records with Blockchain Technology in Cloud-based Healthcare Systems. International Journal of Advanced Computer Science & Applications. 2023 Nov 1;14(11).
19. Demirbaga U, Aujla GS. MapChain: A blockchain-based verifiable healthcare service management in IoT-based big data ecosystem. IEEE Transactions on Network and Service Management. 2022 Sep 6;19(4):3896-907.
20. Raymond Antwi Boakye, George Gyamfi, & Cindy Osei Agyemang. (2023). DEVELOPING REAL-TIME SECURITY ANALYTICS FOR EHR LOGS USING INTELLIGENT BEHAVIORAL AND ACCESS PATTERN ANALYSIS. International Journal of Engineering Technology Research and Management (IJETRM), 07(01), 144–162. https://doi.org/10.5281/zenodo.15486614
21. Anjola Odunaike. DESIGNING ADAPTIVE COMPLIANCE FRAMEWORKS USING TIME SERIES FRAUD DETECTION MODELS FOR DYNAMIC REGULATORY AND RISK MANAGEMENT ENVIRONMENTS (2017). International Journal of Engineering Technology Research and Management (IJETRM), 01(12), 69–88. https://doi.org/10.5281/zenodo.16899962
22. Onabowale Oreoluwa. Innovative financing models for bridging the healthcare access gap in developing economies. *World Journal of Advanced Research and Reviews*. 2020;5(3):200–218. doi: https://doi.org/10.30574/wjarr.2020.5.3.0023
23. Oyegoke Oyebode. BLOCKCHAIN-ORCHESTRATED TEMPORAL GRAPH FORECASTING USING HYBRID RNN-TRANSFORMER ARCHITECTURES TO PREDICT SYSTEMIC RISKS IN GLOBAL FINANCIAL AND CLIMATE INFRASTRUCTURES. International Journal Of Engineering Technology Research & Management (IJETRM). 2022Mar21;06(03):126–45.
24. Adebowale OJ, Ashaolu O. Thermal management systems optimization for battery electric vehicles using advanced mechanical engineering approaches. Int Res J Mod Eng Technol Sci. 2024 Nov;6(11):6398. doi:10.56726/IRJMETS45888.
25. Ugwueze VU, Chukwunweike JN. Continuous integration and deployment strategies for streamlined DevOps in software engineering and application delivery. Int J Comput Appl Technol Res. 2024;14(1):1–24. doi:10.7753/IJCATR1401.1001.
26. Li S, Zhang Y, Xu C, Cheng N, Liu Z, Du Y, Shen X. HealthFort: A cloud-based ehealth system with conditional forward transparency and secure provenance via blockchain. IEEE Transactions on Mobile Computing. 2022 Aug 16;22(11):6508-25.
27. Zhang R, Xue R, Liu L. Security and privacy for healthcare blockchains. IEEE Transactions on Services Computing. 2021 Jun 2;15(6):3668-86.
28. Abouali M, Sharma K, Ajayi O, Saadawi T. Blockchain framework for secured on-demand patient health records sharing. In2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) 2021 Dec 1 (pp. 0035-0040). IEEE.
29. Singh P, Jain D, Sharma AK, Jain A, Vats P. Cloud-based patient health information exchange system using blockchain technology. InInformation and Communication Technology for Competitive Strategies (ICTCS 2021) Intelligent Strategies for ICT 2022 Jun 10 (pp. 569-577). Singapore: Springer Nature Singapore.
30. Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information. 2017 Apr 17;8(2):44.
31. Miyachi K, Mackey TK. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information processing & management. 2021 May 1;58(3):102535.
32. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. Plos one. 2020 Dec 9;15(12):e0243043.
33. Nepal S, Ranjan R, Choo KK. Trustworthy processing of healthcare big data in hybrid clouds. IEEE Cloud Computing. 2015 Jun 2;2(2):78-84.
34. Quan G, Yao Z, Chen L, Fang Y, Zhu W, Si X, Li M. A trusted medical data sharing framework for edge computing leveraging blockchain and outsourced computation. Heliyon. 2023 Dec 1;9(12).
35. Ghayvat H, Pandya S, Bhattacharya P, Zuhair M, Rashid M, Hakak S, Dev K. CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications. IEEE Journal of Biomedical and Health Informatics. 2021 Jul 14;26(5):1937-48.
36. Wang L, Liu X, Shao W, Guan C, Huang Q, Xu S, Zhang S. A blockchain-based privacy-preserving healthcare data sharing scheme for incremental updates. Symmetry. 2024 Jan 11;16(1):89.
37. Deebak BD, Hwang SO. Healthcare applications using blockchain with a cloud-assisted decentralized privacy-preserving framework. IEEE Transactions on Mobile Computing. 2023 Sep 14;23(5):5897-916.

38. Jin H, Luo Y, Li P, Mathew J. A review of secure and privacy-preserving medical data sharing. IEEE access. 2019 May 14;7:61656-69.

39. Rahman MZ, Akunuri S, Babu DN, Ramprasad MV, Shareef SM, Bayleyegn MD. Proof of trust and expertise (PoTE): A novel consensus mechanism for enhanced security and scalability in electronic health record management. IEEE Access. 2024 Jul 8;12:115905-25.

40. Tawfik AM, Al-Ahwal A, Eldien AS, Zayed HH. ACHealthChain blockchain framework for access control and privacy preservation in healthcare. Scientific Reports. 2025 May 14;15(1):16696.

41. Ozturk BA, Tayyeh HK, Namiq HE, Mahajan HB, Junnarkar AA, Uke N, Shamaileh AA, Deshpande SD, Futane PR, Rane M. The Blockchain for Healthcare 4.0 Apply in Standard Secure Medical Data Processing Architecture. Internet Technology Letters. 2024:e614.

42. Kurdi H, Alsalamah S, Alatawi A, Alfaraj S, Altoaimy L, Ahmed SH. Healthybroker: A trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services. Electronics. 2019 May 29;8(6):602