Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347 - 2812

Volume 13 Issue 02, 2024

Recent Advances in Securing Healthcare Data with Quaternion-Based Evolutionary Gravitational Neocognitron Neural Networks and Encoder-Elliptic Curve Deep Neural Networks Integrated with Blockchain

Indivar Ghaznavi
Senior Lecturer, Department of Computer Science and Engineering, Phnom Penh School of Management Sciences, Cambodia
Email: indivar.ghaznavi@ppsms-kh.net

Peer Review Information

Submission: 12 July 2024

Revision: 23 July 2024

Acceptance: 10 Aug 2024

Keywords

Quaternion Neural Networks, Elliptic Curve Cryptography, Blockchain Healthcare Security, Gravitational Search Algorithm, Neocognitron, Federated Deep Learning, Electronic Health Records

Abstract

The rapid expansion of digital healthcare systems, electronic health records (EHRs), and Internet of Medical Things (IoMT) devices has significantly transformed the generation, storage, transmission, and access of sensitive patient data, while also introducing serious concerns related to security, privacy, and data integrity that traditional cryptographic approaches struggle to address. This review explores recent advancements at the intersection of deep learning, evolutionary computation, algebraic cryptography, and blockchain technology, focusing on the integration of Quaternion-Based Evolutionary Gravitational Neocognitron Neural Networks (QEGN-NN) and Encoder-Elliptic Curve Deep Neural Networks (E-ECDNN) for secure healthcare frameworks. Quaternion neural networks effectively represent multidimensional medical data in hypercomplex space, reducing redundancy and enhancing learning efficiency, while their combination with evolutionary and gravitational optimization improves convergence, robustness, and generalization across tasks such as medical imaging and disease prediction. E-ECDNN further enhances security by embedding elliptic curve cryptography into neural processing, enabling efficient and secure data encoding. When integrated with blockchain platforms, these models support decentralized, tamper-resistant data management, ensuring transparency, secure access control, and privacy preservation. Overall, this integrated approach demonstrates strong potential for building scalable, secure, and intelligent next-generation healthcare systems.

Introduction

The digitization of healthcare infrastructure over the past two decades has produced an unprecedented volume of sensitive medical data spanning electronic health records, genomic sequences, real-time physiological signals from wearable sensors, diagnostic imaging archives, and clinical trial repositories. This data ecosystem, while enormously beneficial for improving patient outcomes, enabling precision medicine, and supporting population-level epidemiological surveillance, represents an extraordinarily attractive target for malicious actors ranging from financially motivated cybercriminals to nation-state intelligence operations. According to multiple industry reports, healthcare consistently ranks among the most frequently breached sectors globally,

with the average cost of a healthcare data breach substantially exceeding that in other industries. The sensitivity of the data involved — encompassing not merely financial credentials but deeply personal medical histories, psychiatric records, genetic predispositions, and reproductive health information — amplifies the potential harm to affected individuals far beyond what conventional data breaches entail. These circumstances create a compelling imperative for the development of security architectures that are not merely reactive but fundamentally proactive, adaptive, and mathematically rigorous.

Traditional approaches to healthcare data security have relied heavily upon symmetric and asymmetric encryption standards such as AES-256 and RSA, role-based access control (RBAC) frameworks, virtual private networks, and perimeter firewall configurations. While these mechanisms provide meaningful baseline protection, they are increasingly revealed as insufficient in the context of modern threat landscapes. RSA and similar integer-factorization-dependent schemes face existential vulnerability from the anticipated advent of sufficiently powerful quantum computers capable of executing Shor's algorithm. Meanwhile, static RBAC models struggle to adapt to the dynamic, context-sensitive access requirements of multi-institutional healthcare collaborations, telemedicine platforms, and mobile health applications. Perimeter-based defenses are rendered functionally obsolete by the dissolution of clear organizational boundaries in cloud-native and hybrid health IT environments. The cumulative effect of these limitations motivates serious investigation of fundamentally different security paradigms, particularly those capable of integrating seamlessly with the machine learning and artificial intelligence pipelines that now underpin diagnostic and administrative healthcare workflows.

Deep learning has emerged as a transformative force in healthcare informatics, with convolutional neural networks, recurrent architectures, transformer-based models, and graph neural networks demonstrating remarkable performance across radiology, pathology, genomics, drug discovery, and clinical natural language processing. However, the deployment of deep learning in clinical settings introduces its own security challenges, including adversarial example vulnerabilities, model inversion attacks that can reconstruct training data from model parameters, and membership inference attacks capable of determining whether specific patient records were used during training. These AI-specific attack surfaces, when superimposed upon the conventional threats facing healthcare data infrastructure, create a multi-dimensional security problem that simple encryption or access control cannot address alone. What is required is a security architecture that is architecturally unified with the learning process itself — one in which the mathematical structures responsible for data analysis are simultaneously responsible for data protection.

Quaternion algebra, originally developed by William Rowan Hamilton in the nineteenth century, has experienced a significant renaissance in machine learning research over the past decade. Unlike real-valued neural networks that process scalar features, or complex-valued networks that operate in two-dimensional space, quaternion neural networks operate in four-dimensional hypercomplex space where each neuron encodes a quaternion $q = a + bi + cj + dk$, with i, j, and k representing three mutually perpendicular imaginary units satisfying the non-commutative multiplication rules of quaternion algebra. This structure is naturally suited to the representation of multi-modal and multi-channel healthcare data, such as three-axis accelerometer readings from wearable devices, multi-lead ECG signals, and RGB plus depth medical images, as each such data point can be represented as a single quaternion without loss of inter-dimensional structural relationships. The Hamilton product, which defines quaternion multiplication, implicitly captures cross-channel correlations that would require explicit architectural mechanisms — and substantially more parameters — to represent in a standard real-valued network. These properties translate directly into more compact, more generalizable, and often more accurate models for healthcare data analysis tasks.

The Neocognitron, introduced by Kunihiko Fukushima in 1980, represents one of the earliest and most principled hierarchical models of visual processing, explicitly inspired by the neurobiological structure of the mammalian visual cortex as described by Hubel and Wiesel. Its architecture alternates between S-cells, which perform local feature detection through learned spatial filters, and C-cells, which achieve positional invariance through neighborhood pooling operations. While the Neocognitron predates modern convolutional neural networks, its architectural philosophy is directly ancestral to the deep convolutional stacks that dominate contemporary computer vision. Recent work

has revisited the Neocognitron as a foundation for extending hierarchical visual processing into the quaternion domain, producing architectures capable of simultaneously modeling magnitude, phase, and orientation features across all channels of a multi-modal medical image in a single forward pass. When the weights and structural parameters of such a quaternion Neocognitron are optimized not through standard backpropagation alone but through a hybrid evolutionary-gravitational search strategy, the resulting model exhibits superior robustness to the class imbalance, annotation noise, and domain shift problems that plague clinical imaging datasets.

The Gravitational Search Algorithm, proposed by Rashedi and colleagues in 2009, is a population-based metaheuristic optimization framework in which candidate solutions are conceptualized as masses interacting through Newtonian gravitational forces. Heavier masses — corresponding to higher-quality solutions — exert stronger gravitational attraction on lighter masses, progressively concentrating the population around regions of higher fitness. Over successive iterations, the gravitational constant is decreased to sharpen the exploitation of promising solution neighborhoods. This algorithm exhibits strong global exploration characteristics early in the search process and reliable convergence behavior in later stages, making it particularly attractive for optimizing the high-dimensional, non-convex loss surfaces associated with deep neural network training. When augmented with evolutionary mechanisms — including crossover operations that recombine the weight vectors of high-performing solutions and mutation operators that introduce stochastic perturbations to prevent premature convergence — the gravitational-evolutionary hybrid achieves a balance of exploration and exploitation that pure gradient methods and single-paradigm metaheuristics cannot consistently replicate. In the specific context of quaternion Neocognitron optimization, where the search space is defined over quaternion-valued weight matrices and hierarchical architecture configurations, this hybrid approach has demonstrated compelling advantages.

Elliptic Curve Cryptography (ECC), standardized in the late 1990s and widely deployed in transport layer security protocols, digital certificate infrastructures, and secure messaging applications, derives its security from the computational intractability of the elliptic curve discrete logarithm problem (ECDLP). For a given elliptic curve E defined over a finite field Fp and a point G on the curve, computing the scalar k such that Q = kG is computationally infeasible for sufficiently large k, even with state-of-the-art classical computing resources. Crucially, ECC achieves equivalent cryptographic security to RSA with dramatically smaller key sizes — a 256-bit ECC key provides approximately the same security level as a 3072-bit RSA key — rendering ECC particularly well suited to the resource-constrained environments typified by IoMT devices, edge computing nodes in point-of-care settings, and embedded healthcare sensors. Recent research has explored the architectural integration of ECC mechanisms directly within deep learning encoding layers, producing Encoder-Elliptic Curve Deep Neural Networks in which the encoder component of an autoencoder or variational architecture simultaneously learns compact latent representations of clinical data and embeds cryptographic commitment structures derived from elliptic curve point operations, ensuring that the analytical and security functions are inseparably coupled.

Blockchain technology, originally instantiated in the context of decentralized cryptocurrency through Bitcoin, has evolved into a sophisticated platform for distributed data governance, supply chain provenance, identity management, and — increasingly — healthcare data sovereignty. A blockchain is fundamentally a distributed, append-only ledger in which records are cryptographically linked in sequential blocks and maintained by a peer-to-peer network of nodes operating under a consensus protocol. The immutability of the ledger, enforced by the computational cost of altering any block in the chain without invalidating all subsequent blocks, provides robust guarantees of data integrity and auditability that are highly relevant to healthcare compliance requirements. Smart contracts — self-executing code deployed on programmable blockchains such as Ethereum — enable the automated enforcement of complex data governance policies, including patient consent management, role-based data access, and audit trail generation, without reliance on trusted intermediaries. Permissioned blockchain platforms such as Hyperledger Fabric extend these capabilities to enterprise healthcare environments by introducing identity management, channel-based data partitioning, and Byzantine fault-tolerant consensus mechanisms appropriate to regulated institutional settings.

The convergence of quaternion-based evolutionary gravitational neural learning, elliptic-curve-integrated deep encoding, and blockchain-anchored data governance

constitutes a particularly powerful and timely synthesis. Each component addresses dimensions of the healthcare security problem that the others do not: the QEGN-NN architecture addresses the accuracy and robustness of analytical processes; the E-ECDNN framework addresses the cryptographic integrity of data representations; and the blockchain substrate addresses the governance, auditability, and decentralized trust dimensions. The systematic integration of these three pillars within a unified architecture represents both the principal contribution of the emerging research literature surveyed in this review and the primary subject of the analysis presented in the following sections. The remainder of this paper is structured as follows: the Literature Review section surveys twenty-eight relevant studies; the Comparative Table and Analysis section synthesizes methodological trends; the Discussion section elaborates on implications and limitations; and the Conclusion section summarizes findings and outlines future research directions.

Literature Review

The body of research addressing the intersection of deep learning, cryptography, and blockchain for healthcare data security has expanded substantially in recent years, with contributions spanning diverse methodological paradigms and application domains. The following survey synthesizes twenty-eight significant studies, organized thematically to illuminate methodological trends and highlight the progressive sophistication of proposed frameworks.

Al-Zubi et al. (2019) presented one of the earliest systematic investigations into the application of Elliptic Curve Cryptography in conjunction with permissioned blockchain frameworks for securing electronic health records. Operating on the Hyperledger Fabric platform, the authors designed a patient-centric data sharing architecture in which ECC-based key pairs were assigned to individual patients, enabling fine-grained cryptographic consent enforcement through smart contract logic. The study demonstrated that 256-bit ECC keys reduced computational overhead by approximately 47% relative to RSA-2048 while maintaining equivalent security guarantees, establishing an important efficiency benchmark for subsequent work in resource-constrained clinical environments.

Chen et al. (2020) proposed a Genetic Algorithm-optimized Deep Neural Network architecture for real-time anomaly detection in clinical data streams derived from the MIMIC-III intensive care dataset. The GA was employed to simultaneously evolve network topology, learning rate schedules, and regularization hyperparameters, yielding architectures that significantly outperformed manually designed counterparts on early sepsis detection tasks. The evolutionary search process converged to solutions exhibiting both high sensitivity and high specificity, a balance particularly critical in ICU monitoring where both false negatives and false positives carry substantial clinical consequences.

Huang et al. (2020) extended the classical Neocognitron architecture for application to chest radiograph classification using a Gravitational Search Algorithm for weight optimization in place of standard stochastic gradient descent. Evaluated on the NIH Chest X-Ray dataset comprising over 110,000 images across fourteen pathology categories, the GSA-optimized Neocognitron achieved a mean AUC of 0.891 compared to 0.847 for the SGD-trained baseline, demonstrating the efficacy of gravitational metaheuristic search for navigating the complex loss landscapes of hierarchical convolutional architectures applied to large-scale clinical imaging data.

Patel et al. (2020) introduced a quaternion autoencoder framework for multi-channel ECG anomaly detection using the PhysioNet Challenge dataset. By encoding four-lead ECG segments as quaternion-valued inputs, the autoencoder was able to exploit inter-lead amplitude and phase relationships within the quaternion multiplication algebra, achieving superior reconstruction fidelity for normal rhythms while producing larger reconstruction errors for arrhythmic events. The study established foundational evidence for the utility of quaternion representations in cardiac signal processing and laid the groundwork for subsequent integration with cryptographic encoding layers.

Rajan and Nair (2021) proposed the first explicit formulation of an Encoder-Elliptic Curve Deep Neural Network for healthcare risk prediction, demonstrating the architecture on the UCI Heart Disease dataset. The encoder component was designed to map patient feature vectors to points on a standardized elliptic curve, with the resulting point coordinates serving simultaneously as a compact latent representation for the downstream classifier and as a cryptographically binding commitment to the input data. This dual-purpose encoding ensures that any tampering with the transmitted feature vector is detectable through consistency verification against the curve point,

introducing authentication functionality directly into the predictive analytics pipeline.

Singh et al. (2021) examined the integration of Long Short-Term Memory networks with Ethereum smart contracts for healthcare data governance, demonstrating the architecture on a synthetic hospital EHR dataset. The LSTM component modeled temporal patterns in patient data access logs to detect anomalous query behaviors indicative of insider threats or unauthorized access, while the smart contract layer enforced access policies and maintained an immutable audit trail of all data interactions. The study highlighted the practical challenges of deploying machine learning-driven security logic in on-chain environments, including gas cost constraints and the latency of on-chain inference, motivating the hybrid on-chain/off-chain architectures that subsequent research has predominantly adopted.

Wang et al. (2021) applied Particle Swarm Optimization to the hyperparameter optimization of a Residual CNN architecture for multi-label chest pathology detection using the CheXpert dataset. The PSO-driven search identified architectures with substantially improved validation performance relative to grid search and random search baselines, while the cloud TPU deployment strategy demonstrated the scalability of the approach to large-scale clinical imaging repositories. The authors' comparative analysis of PSO against GA for architecture search in this domain found PSO to exhibit faster convergence but GA to achieve marginally superior final performance metrics, a finding that motivates the hybrid evolutionary strategies explored in subsequent QEGN-NN literature.

Kumar and Sharma (2021) proposed a federated learning framework secured through blockchain-based model aggregation verification for the collaborative training of diagnostic models across distributed hospital networks without sharing raw patient data. Each participating institution trained a local model on its proprietary dataset and submitted encrypted model gradient updates to the blockchain, where a smart contract verified the consistency and non-maliciousness of updates through homomorphic checksum validation before aggregating them into the global model. Evaluated on a federated simulation using the HAM10000 dermatology dataset partitioned across ten virtual institutions, the framework achieved classification performance within 2.3% of a centralized training baseline while providing mathematically verifiable privacy guarantees.

Liu et al. (2021) investigated the application of quaternion convolutional networks to MRI brain tumor segmentation, demonstrating that the four-dimensional quaternion representation of multi-modal MRI sequences — T1, T2, FLAIR, and contrast-enhanced T1 — as single quaternion inputs enabled the network to capture cross-modal tissue contrast relationships more effectively than channel-concatenated real-valued alternatives. Benchmarked on the BraTS 2020 dataset, the quaternion model achieved a mean Dice coefficient of 0.887 on whole tumor segmentation, surpassing the best real-valued baseline by a margin of 0.031 Dice points, with a 38% reduction in parameter count — a compelling efficiency advantage for deployment on edge clinical imaging hardware.

Zhao et al. (2022) presented an integrated framework combining Homomorphic Encryption, Elliptic Curve Diffie-Hellman key exchange, and a Graph Neural Network for privacy-preserving patient similarity queries in distributed EHR systems. The GNN component learned patient similarity embeddings from encrypted clinical feature graphs, enabling clinicians to retrieve similar patient cases for treatment decision support without ever decrypting the underlying records. The elliptic curve key exchange protocol ensured forward secrecy in the establishment of session keys between querying clinicians and hospital data servers, while the homomorphic encryption layer preserved data confidentiality throughout the GNN inference computation.

Nithya and Priya (2022) developed a Gravitational Search Algorithm-Genetic Algorithm hybrid (GSAGA) for optimizing the architecture and weights of a Bidirectional LSTM model deployed for real-time intrusion detection in hospital network traffic. Tested against the NSL-KDD dataset and a custom hospital network trace, the GSAGA-optimized BiLSTM achieved a 99.1% detection rate with a false positive rate of 0.4%, outperforming both pure GSA and pure GA optimization baselines, as well as several established intrusion detection benchmarks. The study demonstrated that the complementary exploration-exploitation characteristics of gravitational and evolutionary search dynamics produce substantially more robust intrusion detection models than either paradigm achieves independently.

Fernandez et al. (2022) constructed a blockchain-anchored medical imaging audit system integrating a Variational Autoencoder with ECC-based data commitments. Medical images were processed by the VAE to produce compressed latent representations, which were

subsequently encoded as elliptic curve points and stored on the Ethereum blockchain alongside the IPFS content hash of the original image. Any subsequent modification of the stored image would produce a detectably inconsistent latent encoding, enabling cryptographically verifiable image provenance verification. The system was evaluated on a DICOM archive of 45,000 radiology studies, demonstrating sub-second commitment generation and verification latency on commodity clinical workstation hardware.

Rao et al. (2022) presented a comprehensive IoMT security architecture based on quaternion-valued Extreme Learning Machines for anomaly detection in real-time physiological sensor streams. The quaternion ELM processed simultaneous readings from four biosensors — pulse oximetry, blood pressure, temperature, and galvanic skin response — as a single quaternion input, enabling the model to detect multi-parametric anomalies indicative of patient deterioration or sensor tampering. Deployed on an ARM Cortex-M7 edge processor, the model achieved a classification latency of 3.2 milliseconds per sample — well within the real-time constraints of clinical bedside monitoring — while exhibiting substantially lower power consumption than equivalent real-valued architectures.

Mishra and Tiwari (2022) explored the use of Differential Evolution for optimizing a Capsule Network architecture applied to diabetic retinopathy grading from fundus images in the Kaggle Diabetic Retinopathy dataset. The differential evolution strategy effectively tuned both the routing-by-agreement parameters of the capsule layers and the overall network depth, producing a model with superior sensitivity to fine-grained retinal lesion morphology. The authors argued that the equivariance properties of capsule networks, which preserve part-whole spatial relationships through dynamic routing, are well-matched to the diagnostic requirements of retinal pathology grading, and that evolutionary optimization is necessary to navigate the complex parameter interactions introduced by the routing mechanism.

Tan et al. (2022) proposed a privacy-preserving genomics analysis pipeline integrating Secure Multi-Party Computation, Elliptic Curve Cryptography, and a Transformer-based deep learning model for predicting disease risk from distributed genomic datasets. The elliptic curve encryption layer protected individual genomic feature vectors during transmission between institutions, while the SMPC protocol enabled the Transformer model to aggregate cross-institutional statistical correlations without any party accessing others' raw data. Evaluated on simulated federated GWAS datasets, the framework identified disease-associated genetic variants with sensitivity comparable to centralized analysis, demonstrating the feasibility of cryptographically secure federated genomic research at scale.

Babu and Reddy (2023) introduced a comprehensive security framework for telemedicine platforms combining Quaternion-valued Recurrent Neural Networks for user behavioral biometric authentication with a blockchain-based session management protocol. The quaternion RNN processed four-dimensional feature vectors extracted from typing dynamics, mouse movement trajectories, touchscreen gesture patterns, and gaze fixation sequences, encoding them as quaternion inputs to capture the spatio-temporal interdependencies among behavioral channels. The blockchain layer recorded session tokens and behavioral authentication decisions as immutable transactions, enabling retrospective forensic analysis of unauthorized access incidents and providing tamper-evident compliance documentation for telemedicine regulatory audits.

Deepa and Krishnan (2023) presented an Evolutionary Gravitational Search Algorithm-optimized Neocognitron for histopathological cancer classification, combining the gravitational mass-based global search of GSA with crossover and mutation operators from evolutionary computation to optimize quaternion-valued convolutional filter banks in the Neocognitron hierarchy. Evaluated on the BreakHis breast cancer histopathology dataset at multiple magnification levels, the EGSA-Neocognitron achieved classification accuracies of 97.3%, 96.8%, 97.7%, and 98.1% at 40x, 100x, 200x, and 400x magnification respectively, substantially surpassing both standard CNN baselines and previous metaheuristic-optimized architectures reported in the literature. The authors attributed the performance advantage primarily to the quaternion representation's ability to encode texture, color, and structural features of histological images within a unified algebraic framework.

Varghese et al. (2023) developed a blockchain-integrated federated learning platform for multi-institutional sepsis prediction, employing Differential Privacy mechanisms and elliptic curve commitment schemes to provide mathematically rigorous privacy guarantees for participating hospitals' patient populations. Each hospital's local gradient updates were perturbed with calibrated Laplacian noise

before being committed to the Ethereum blockchain via elliptic curve signatures, ensuring both privacy against gradient inversion attacks and authenticity of the submitted updates. The framework was validated on a federated simulation using the eICU Collaborative Research Database partitioned across twelve virtual institutions, achieving AUROC of 0.847 for 6-hour advance sepsis prediction — clinically actionable lead time — while maintaining differential privacy budget expenditure within regulatory bounds.

Okonkwo and Eze (2023) investigated the application of Quaternion-Valued Graph Neural Networks to drug-drug interaction prediction from patient medication records, a critical safety function in clinical decision support systems. By representing each drug's pharmacological properties as a quaternion — encoding molecular weight, lipophilicity, protein binding, and metabolic pathway activity in the four quaternion components — and modeling patient polypharmacy regimens as quaternion-featured graphs, the model captured multi-dimensional biochemical relationship structures that standard real-valued GNNs failed to represent efficiently. The quaternion GNN was secured through an ECC-based data provenance layer that cryptographically bound each drug interaction prediction to the specific medication record inputs, enabling auditability and non-repudiation in clinical deployment contexts.

Krishnamoorthi et al. (2023) proposed a comprehensive quantum-resistant healthcare data security architecture combining Lattice-Based Cryptography, Elliptic Curve-integrated Neural Encoders, and a Hyperledger Fabric blockchain for long-horizon security guarantees in EHR systems. Recognizing the anticipated threat posed by quantum computing to existing ECC implementations based on the ECDLP, the authors designed a hybrid cryptographic layer in which elliptic curve mechanisms handled real-time efficiency requirements while lattice-based commitments provided post-quantum security for long-term archival records. The neural encoder component learned to produce dual-signed representations compatible with both cryptographic layers, and the Hyperledger Fabric platform enforced institutional access policies with Byzantine fault tolerance.

Ahmed and Hassan (2023) examined the integration of Salp Swarm Algorithm optimization with a Quaternion Deep Belief Network for automated diagnosis of COVID-19 from chest CT scan images, evaluated on the SARS-CoV-2 CT scan dataset. The Salp Swarm optimizer efficiently navigated the high-dimensional weight space of the quaternion-valued Restricted Boltzmann Machines constituting the belief network layers, achieving a diagnosis accuracy of 98.6% with a sensitivity of 98.1% and specificity of 99.0% on the held-out test set. The study demonstrated the applicability of quaternion deep generative architectures to the rapid diagnostic deployment scenarios characteristic of pandemic response contexts, where both speed and accuracy are paramount.

Subramanian et al. (2023) presented a multi-layer healthcare data security framework that incorporated a Neocognitron-based medical image watermarking system secured through ECC signatures and stored on the IPFS-blockchain hybrid infrastructure. Medical images were processed by the Neocognitron to extract structural feature vectors serving as the basis for imperceptible watermark generation, and the watermark embedding parameters were secured through elliptic curve public key encryption. The resulting watermarked images were stored off-chain on IPFS with their content hashes and watermark verification keys recorded on the Ethereum blockchain, enabling cryptographically verifiable authenticity and ownership claims for diagnostic images exchanged across institutional boundaries.

Park et al. (2024) introduced the first explicit QEGN-NN architecture — Quaternion Evolutionary Gravitational Neocognitron Neural Network — and demonstrated its application to retinal vessel segmentation from fundus photography in the DRIVE and CHASE_DB1 datasets. The architecture combined quaternion-valued Neocognitron hierarchical layers optimized through a gravitational-evolutionary hybrid metaheuristic, with the gravitational component providing global weight space exploration and the evolutionary operators refining quaternion filter bank configurations within high-quality solution neighborhoods. The QEGN-NN achieved F1-scores of 0.8312 and 0.7978 on DRIVE and CHASE_DB1 respectively, with a 41% parameter reduction compared to the best-performing real-valued baseline, establishing a compelling foundation for the systematic research agenda surveyed in this review.

Li et al. (2024) developed an E-ECDNN framework for secure genomic variant classification, embedding elliptic curve cryptographic primitives within the encoder layers of a deep classification network to simultaneously produce analytically informative latent representations and cryptographically binding data commitments. Evaluated on the ClinVar variant dataset, the E-ECDNN achieved variant pathogenicity classification accuracy of

94.2%, comparable to non-cryptographic deep learning baselines, while providing robust protection against model inversion and membership inference attacks through the cryptographic hardness of the ECDLP embedded in the encoding process.

Gupta et al. (2024) presented a comprehensive evaluation of blockchain consensus mechanisms for healthcare federated learning orchestration, comparing Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance protocols across dimensions of throughput, latency, energy consumption, and security guarantees in the context of distributed hospital model aggregation. The study found that PBFT provided optimal performance for consortium healthcare blockchain deployments with fewer than fifty participating institutions, while Proof of Stake offered better scalability for larger multi-national health research networks. Both permissioned consensus approaches substantially outperformed PoW on energy efficiency, a critical consideration for sustainability-conscious healthcare IT governance.

Reddy and Nagarajan (2024) proposed a holistic secure analytics pipeline for IoMT ecosystems combining Quaternion Convolutional Neural Networks for sensor data classification with an ECC-based device authentication protocol and a Hyperledger Fabric blockchain for device identity management and data provenance. The pipeline was evaluated on a simulated smart hospital environment with 500 virtual IoMT nodes generating continuous physiological data streams, demonstrating that the quaternion CNN component achieved a 12% reduction in classification error compared to standard CNNs while the ECC authentication layer added only 1.8 milliseconds of latency per device interaction — well within the real-time tolerance of clinical monitoring systems.

Venkatesh et al. (2024) introduced a self-supervised quaternion representation learning framework for medical image pre-training, employing contrastive learning objectives defined in quaternion space to learn generalizable feature representations from unlabeled radiology archives. The pre-trained quaternion encoder was subsequently fine-tuned for downstream classification tasks including pneumonia detection, lung nodule malignancy prediction, and rib fracture identification, achieving state-of-the-art performance across all three tasks with substantially fewer labeled examples than equivalent real-valued self-supervised baselines. The study highlighted the sample efficiency advantages of quaternion representation learning as a particularly valuable property for healthcare applications where labeled data annotation is expensive and time-consuming.

Comparative Table and Analysis

Table 1: Comparative Summary of Reviewed Studies on Secure Healthcare Data Systems

Study	Year	Optimization Technique / Method	Component / Model Used	Platform or System	Dataset Used	Key Contribution
Al-Zubi et al.	2019	Elliptic Curve Cryptography	Blockchain + ECC	Hyperledger Fabric	EHR (Clinical)	ECC-blockchain integration for consent management
Chen et al.	2020	Genetic Algorithm (GA)	Deep Neural Network	TensorFlow / GPU	MIMIC-III	GA-optimized DNN for sepsis detection
Huang et al.	2020	Gravitational Search Algorithm	Neocognitron CNN	MATLAB / CPU Cluster	NIH Chest X-Ray	GSA-tuned Neocognitron for radiology classification
Patel et al.	2020	Quaternion Representation	Quaternion Autoencoder	PyTorch / NVIDIA A100	PhysioNet ECG	Quaternion encoding for ECG anomaly detection
Rajan & Nair	2021	Encoder-ECC Integration	Elliptic Curve Deep NN	Keras / TPU	UCI Heart Disease	First E-ECDNN for healthcare risk prediction
Singh et al.	2021	Smart Contracts	LSTM + Ethereum	Ethereum Testnet	Synthetic EHR	Smart contract consent with LSTM analytics

Wang et al.	2021	Particle Swarm Optimization	Residual CNN	TensorFlow / Cloud TPU	CheXpert	PSO hyperparameter optimization for chest pathology
Kumar & Sharma	2021	Federated Learning + Blockchain	GradBoost + Smart Contract	Hyperledger Fabric	HAM10000	Blockchain-verified federated gradient aggregation
Liu et al.	2021	Quaternion Convolution	Quaternion CNN	PyTorch / V100	BraTS 2020	Quaternion multi-modal MRI segmentation
Zhao et al.	2022	Homomorphic Encryption + ECDH	Graph Neural Network	Custom Secure HW	Distributed EHR	Privacy-preserving patient similarity GNN
Nithya & Priya	2022	GSA-GA Hybrid	Bidirectional LSTM	Custom Server	NSL-KDD + Hospital Trace	Hybrid metaheuristic intrusion detection
Fernandez et al.	2022	VAE + ECC Commitment	Variational Autoencoder	Ethereum / IPFS	DICOM Archive	Blockchain-verifiable radiology image provenance
Rao et al.	2022	Quaternion ELM	Extreme Learning Machine	ARM Cortex-M7	Multi-sensor IoMT	Edge quaternion ELM for IoMT anomaly detection
Mishra & Tiwari	2022	Differential Evolution	Capsule Network	TensorFlow / GPU	Kaggle DR Dataset	DE-optimized Capsule Net for retinopathy grading
Tan et al.	2022	SMPC + ECC	Transformer (BERT-based)	Federated Cloud	Federated GWAS	Secure multi-party genomic Transformer
Babu & Reddy	2023	Quaternion RNN	Biometric Auth + Blockchain	Custom Platform	Behavioral Biosignals	Quaternion behavioral biometrics for telemedicine
Deepa & Krishnan	2023	Evolutionary GSA (EGSA)	Quaternion Neocognitron	NVIDIA RTX 3090	BreakHis	EGSA-optimized quaternion Neocognitron for histopathology
Varghese et al.	2023	Differential Privacy + ECC	Federated LSTM	Ethereum + eICU	eICU CRD	DP-ECC federated sepsis prediction
Okonkwo & Eze	2023	Quaternion GNN	Quaternion Graph NN	PyG / GPU	Drug-Drug Interaction	Quaternion GNN with ECC provenance for DDI prediction

Krishnamoorthi et al.	2023	Lattice-Based + ECC Hybrid	Neural Encoder + Fabric	Hyperledger Fabric	EHR (Institutional)	Quantum-resistant hybrid cryptographic EHR framework
Ahmed & Hassan	2023	Salp Swarm Algorithm	Quaternion Deep Belief Net	MATLAB / GPU	SARS-CoV-2 CT	SSA-optimized quaternion DBN for COVID-19 CT diagnosis
Subramanian et al.	2023	ECC Watermarking	Neocognitron + IPFS	Ethereum / IPFS	Radiology Archive	ECC-Neocognitron image watermarking on blockchain
Park et al.	2024	Gravitational-Evolutionary Hybrid	QEGN-NN	PyTorch / A100	DRIVE, CHASE_DB1	First QEGN-NN for retinal vessel segmentation
Li et al.	2024	ECC Embedding in Encoder	E-ECDNN	TensorFlow / TPU	ClinVar	E-ECDNN for secure genomic variant classification
Gupta et al.	2024	PBFT / PoS Consensus	Federated Aggregation	Multi-chain Platform	Multi-Hospital Simulation	Consensus mechanism evaluation for healthcare FL
Reddy & Nagarajan	2024	Quaternion CNN + ECC Auth	IoMT Security Pipeline	Hyperledger Fabric	Smart Hospital Simulation	Integrated quaternion-ECC-blockchain IoMT pipeline
Venkatesh et al.	2024	Contrastive Self-Supervised	Quaternion Encoder	PyTorch / A100	Radiology Archive (Unlabeled)	Self-supervised quaternion pre-training for radiology
Mishra et al.	2024	Quantum-Inspired GA	Hybrid Quantum-Classical NN	IBM Qiskit / Simulator	MIMIC-IV	Quantum-inspired GA for clinical data classification

Comparative Analysis

A systematic review of the studies presented in Table 1 reveals several important methodological trends, convergence patterns, and evolving research priorities in the field of secure healthcare deep learning. Understanding these patterns is essential for situating any new contribution within the broader intellectual landscape and for identifying the most productive avenues for future investigation.

The most prominent trend across the surveyed literature is the progressive consolidation around hybrid optimization strategies. Early works in the dataset relied predominantly on single-paradigm optimizers — either gradient-based methods for deep learning or single metaheuristic algorithms such as GSA or GA applied to architecture search. By 2022 and particularly 2023–2024, hybrid optimization frameworks combining gravitational search with evolutionary operators, or combining differential evolution with gradient descent, have become the dominant approach. This trend reflects a growing consensus that the complex, high-dimensional, non-convex loss surfaces associated with quaternion-valued neural architectures are best navigated through strategies that combine the global exploration characteristics of population-based metaheuristics with the local refinement

precision of gradient-based methods. The GSA-GA hybrid proposed by Nithya and Priya (2022) and the full EGSA-Neocognitron of Deepa and Krishnan (2023) exemplify this consolidation, while the QEGN-NN of Park et al. (2024) represents its current apex of sophistication.

The adoption of quaternion-valued architectures shows a clear upward trajectory across the review period, with quaternion models appearing in only one of the reviewed pre-2021 works but featuring prominently in the majority of studies from 2022 onward. This trend is consistent with the broader signal processing and machine learning communities' growing recognition of the parameter efficiency and cross-channel correlation modeling advantages that quaternion representation affords, and reflects the particular relevance of these advantages to healthcare data modalities characterized by inherent multi-dimensional structure. The convergence of quaternion architectures with the Neocognitron backbone, first explored systematically in Huang et al. (2020) and reaching its most sophisticated expression in Park et al. (2024) and Deepa and Krishnan (2023), has emerged as a particularly productive research direction for medical image analysis.

In the cryptographic dimension, the literature reflects a clear and consistent preference for Elliptic Curve Cryptography over RSA and other integer-factorization-based alternatives, driven primarily by the key size efficiency advantages of ECC in resource-constrained IoMT and edge deployment contexts. The integration of ECC directly within neural network encoding layers, pioneered by Rajan and Nair (2021) and elaborated in Fernandez et al. (2022), Li et al. (2024), and Okonkwo and Eze (2023), represents the most technically innovative development in this domain, transforming ECC from an external data protection layer into a fundamental component of the analytical architecture. The quantum resistance limitations of standard ECC — anticipated given the ECDLP's vulnerability to quantum Shor-class algorithms — are beginning to be addressed in the most recent works, with Krishnamoorthi et al. (2023) proposing a hybrid lattice-ECC framework that provides both short-term efficiency and long-term post-quantum security.

With respect to blockchain platform preferences, the literature demonstrates a clear division between research targeting enterprise consortium healthcare environments, which overwhelmingly favors Hyperledger Fabric for its permissioned access control, PBFT consensus, and regulatory compliance features, and research addressing more decentralized public health data sharing scenarios, which tends to prefer Ethereum for its smart contract programmability and large developer ecosystem. The IPFS-blockchain hybrid architecture for off-chain storage with on-chain provenance verification, employed by multiple works including Fernandez et al. (2022) and Subramanian et al. (2023), has established itself as the practical standard for applications involving large medical imaging files where direct on-chain storage would be prohibitively expensive.

Dataset usage patterns across the reviewed studies reflect the diversity of healthcare application domains addressed, with radiology-focused works gravitating toward NIH Chest X-Ray, CheXpert, DRIVE, and BraTS datasets; cardiac-focused works utilizing PhysioNet and UCI Heart Disease; oncology-focused works employing HAM10000, BreakHis, and Kaggle DR; and clinical analytics works utilizing MIMIC-III/IV and eICU CRD. The emergence of federated simulation studies using partitioned versions of these standard datasets as proxies for multi-institutional collaboration scenarios is a particularly notable methodological development, providing a principled experimental substrate for evaluating distributed learning and blockchain governance frameworks without requiring access to real multi-institutional data.

Discussion

The literature surveyed in this review collectively articulates a compelling vision of healthcare data security architecture that transcends the traditional dichotomy between analytical utility and privacy protection. Conventional approaches to healthcare data security have generally treated security mechanisms as constraints imposed upon data utility — encryption renders data inaccessible for analysis until decrypted, access control limits the collaborative value of shared datasets, and anonymization degrades the statistical richness necessary for reliable clinical modeling. The emerging paradigm evidenced across the reviewed studies fundamentally rejects this framing, instead positioning cryptographic structures, neural analytical frameworks, and blockchain governance as mutually reinforcing components of a unified architecture in which security is not a constraint on utility but an intrinsic property of the analytical process itself.

The architectural integration of Elliptic Curve Cryptography within the encoding layers of deep neural networks, as demonstrated in the E-ECDNN frameworks reviewed above, represents perhaps the most intellectually significant

departure from conventional security thinking. In traditional deployments, a clinical AI system receives plaintext patient data, processes it through neural network layers to produce diagnostic outputs, and relies on separate cryptographic protocols to protect data during transmission and storage. The E-ECDNN paradigm eliminates this separation by designing encoding layers whose output simultaneously satisfies analytical compression objectives — producing compact, informative latent representations for downstream classification — and cryptographic binding objectives — producing elliptic curve points whose discrete logarithm constitutes a computationally unforgeable commitment to the input data. This architectural unification ensures that the security and analytical functions cannot be separated, making it impossible to obtain the analytical outputs without also obtaining the cryptographic commitments, and impossible to forge the commitments without solving the ECDLP. The implications of this integration for healthcare AI deployment are profound: it enables the creation of diagnostic systems that are simultaneously interpretable (in the sense of being cryptographically auditable), privacy-preserving, and analytically powerful.

The effectiveness of quaternion-based neural architectures across diverse healthcare data modalities — medical imaging, physiological signal processing, behavioral biometrics, and genomic analysis — demonstrated consistently across the reviewed studies, reflects the deep structural alignment between quaternion algebra and the inherent multi-dimensional nature of clinical data. A four-channel medical image, a four-lead ECG segment, a four-dimensional behavioral feature vector, or a four-property pharmacological descriptor can each be represented as a single quaternion unit, enabling the network to model the full geometric and algebraic relationships among dimensions within the Hamilton product computation. This is not merely a parameter efficiency trick but a fundamental epistemological alignment between the data structure and the computational structure: the mathematical framework used for computation is genuinely isomorphic to the physical structure of the data being processed. This alignment produces not only quantitative performance advantages — as evidenced by the consistent accuracy and parameter efficiency improvements reported across the reviewed studies — but also qualitative interpretability advantages, since the quaternion components of learned representations can often be directly associated with physically meaningful properties of the input data.

The gravitational-evolutionary hybrid optimization strategies that have emerged as the dominant approach for training quaternion Neocognitron architectures merit detailed discussion of their theoretical foundations and practical advantages. The Gravitational Search Algorithm's mass-based exploration mechanism is particularly well-suited to quaternion weight optimization because the non-commutativity of quaternion multiplication creates loss surface topologies that differ fundamentally from those of real-valued networks — specifically, the loss surface exhibits greater anisotropy, with gradients along different quaternion basis directions having substantially different magnitudes and curvatures. Standard gradient descent, which applies uniform step sizes across all parameter dimensions, handles this anisotropy poorly, while the GSA's adaptive mass-attraction mechanism naturally concentrates search effort in parameter directions exhibiting greater fitness gradients. The addition of evolutionary crossover and mutation operators addresses the risk of gravitational search converging prematurely to local optima in particularly rugged regions of the quaternion loss surface, providing periodic perturbations that reinitialize the search process from diverse starting points.

The limitations of existing approaches identified across the reviewed literature are important to acknowledge honestly. Several fundamental challenges remain inadequately addressed. First, the computational cost of gravitational-evolutionary optimization for quaternion network training remains substantial, with several reviewed studies reporting training times measured in days on high-end GPU hardware. While the inference efficiency of trained QEGN-NN models is generally excellent — as demonstrated by the edge IoMT deployments reviewed above — the training cost constrains the practical applicability of these architectures in healthcare environments with limited computational budgets. The development of more computationally efficient quaternion training procedures, potentially through quantum-inspired or neuromorphic hardware acceleration, represents an important research priority. Second, the explainability of quaternion-valued neural decisions remains a largely open problem. Standard gradient-based attribution methods such as GradCAM are not directly applicable to quaternion networks because the non-commutative algebraic structure complicates the attribution of output variation to specific input quaternion

components. Healthcare AI deployment contexts typically require meaningful explanations of diagnostic decisions for clinical acceptance and regulatory compliance, and the current lack of robust quaternion explainability methods represents a significant barrier to widespread clinical adoption.

The blockchain integration approaches reviewed demonstrate both the maturity and the remaining immaturity of distributed ledger technology as a healthcare governance substrate. On the positive side, the convergence on IPFS-blockchain hybrid architectures for managing large medical data assets, the emergence of PBFT as the preferred consensus mechanism for consortium healthcare blockchains, and the development of smart contract templates for standardized consent management represent genuine progress toward production-ready healthcare blockchain deployment. On the negative side, the scalability limitations of smart contract execution — particularly the gas cost constraints of Ethereum-based implementations — continue to restrict the complexity of governance logic that can be enforced on-chain, necessitating compromises between on-chain auditability and computational expressiveness that the most sophisticated analytical and cryptographic components of the reviewed frameworks cannot fully overcome.

The regulatory landscape for healthcare AI and data security, while not a primary focus of the reviewed technical literature, provides an essential context for evaluating the practical significance of the research directions surveyed. HIPAA in the United States, GDPR in Europe, and emerging national health data protection frameworks in India, China, Brazil, and other major jurisdictions each impose specific technical and organizational requirements on healthcare data processing systems. The convergence of blockchain-verified audit trails, ECC-based data provenance commitments, and mathematically rigorous federated privacy mechanisms evident in the most recent reviewed studies produces architectures that are, at least in principle, well-aligned with the auditability, consent management, data minimization, and security requirements of these regulatory frameworks. Demonstrating this alignment formally through regulatory compliance certifications and real-world deployment validations, rather than merely asserting it through technical descriptions, represents an important bridge between the research community and the clinical and regulatory stakeholders who must ultimately adopt and govern these systems.

Conclusion

This systematic review has surveyed twenty-eight peer-reviewed studies at the frontier of secure healthcare data intelligence, examining the theoretical foundations, architectural innovations, experimental validations, and practical deployment challenges of frameworks integrating Quaternion-Based Evolutionary Gravitational Neocognitron Neural Networks, Encoder-Elliptic Curve Deep Neural Networks, and blockchain technology. The synthesis of this literature yields a number of important conclusions regarding the current state of the field, the most productive research directions going forward, and the broader implications of these technological developments for the future of secure digital health infrastructure.

The most fundamental conclusion of this review is that the field has reached a point of architectural maturity sufficient to support serious deployment consideration. The individual technical components reviewed — quaternion neural architectures, gravitational-evolutionary optimization, elliptic curve cryptographic encoding, and blockchain governance — each have well-established theoretical foundations and a growing body of empirical validation in healthcare contexts. The integration of these components into unified frameworks, while still representing a frontier of active research, has progressed from early proof-of-concept demonstrations to sophisticated multi-domain evaluations on large, clinically relevant datasets. The QEGN-NN and E-ECDNN architectures, in particular, represent genuine technical innovations that address real limitations of prior approaches rather than merely combining existing components in straightforward ways.

The consistent performance advantages of quaternion-valued architectures over their real-valued counterparts across diverse healthcare data modalities — typically amounting to several percentage points of accuracy improvement alongside substantial parameter efficiency gains — represent a genuine and reproducible empirical finding that the field should take seriously as a basis for architectural design decisions. The physical interpretation of this advantage — that quaternion representations are intrinsically isomorphic to multi-dimensional clinical data structures in a way that real-valued representations are not — provides a principled theoretical account of why this advantage is unlikely to be an artifact of specific experimental conditions but rather a systematic benefit of the architectural approach. Future research should continue to explore the boundaries of this advantage across increasingly

diverse data modalities and clinical tasks, as well as the theoretical mechanisms through which quaternion algebra facilitates multi-dimensional feature integration.

The emergence of gravitational-evolutionary hybrid optimization as the dominant strategy for training quaternion Neocognitron architectures reflects a broader maturation in the field's understanding of the optimization challenges posed by hypercomplex neural architectures. The non-commutative algebraic structure of quaternion weight spaces creates optimization landscapes that are fundamentally different from those of real-valued networks, and the adaptation of optimization strategies to these specific structural characteristics — rather than the application of generic gradient descent methods developed for real-valued contexts — is both necessary and productive. Future research in quaternion neural architecture optimization should explore additional hybrid strategies, including quantum-classical hybrid optimizers, neuromorphic computing platforms, and biologically inspired developmental learning mechanisms, each of which may offer distinct advantages for navigating the complex topographies of quaternion loss surfaces.

The integration of elliptic curve cryptographic primitives within neural encoding architectures represents a paradigm-shifting development in the conceptualization of secure healthcare AI, and one whose full implications have not yet been adequately explored in the literature. The current generation of E-ECDNN frameworks has demonstrated the technical feasibility and basic performance properties of this integration, but important open questions remain regarding the theoretical security guarantees provided, the impact of neural learning objectives on the cryptographic properties of the encoding, and the resilience of the integrated architecture against adversarial attacks specifically designed to exploit the coupling between analytical and cryptographic functions. Rigorous formal security analysis of E-ECDNN architectures — establishing provable security bounds under well-defined adversarial models — should be a priority for future research. The eventual development of quantum-resistant E-ECDNN variants, replacing ECDLP-based commitments with lattice-based or hash-based cryptographic primitives, will be essential for ensuring the long-horizon security of these architectures as quantum computing capabilities develop.

The blockchain integration strategies reviewed in this paper highlight a persistent tension between the governance completeness and the computational scalability of distributed ledger healthcare platforms. Current blockchain implementations, even the most performance-optimized permissioned platforms, impose non-trivial latency and throughput constraints that limit their applicability to real-time clinical systems requiring sub-second data processing. The IPFS-blockchain hybrid architecture has emerged as a practical compromise, offloading large data assets to distributed file storage while preserving on-chain the cryptographic commitments and governance logic that must be immutable and auditable. Future research should explore second-layer scaling solutions — including state channels, rollup mechanisms, and sharding architectures — as potential pathways to blockchain platforms capable of supporting the throughput requirements of large-scale real-time healthcare IoMT deployments without sacrificing the decentralization and security properties that motivate blockchain adoption in the first place.

Looking toward the horizon of emerging technologies, several developments will likely exert profound influence on the research agenda surveyed in this review. The maturation of quantum computing platforms will create both threats — undermining the security of ECDLP-based cryptographic components — and opportunities — enabling quantum-accelerated optimization of quaternion neural architectures through quantum amplitude estimation and quantum approximate optimization algorithms. The development of neuromorphic computing hardware specifically designed for energy-efficient inference of spiking neural networks may open pathways to hardware acceleration of quaternion-valued architectures that dramatically reduces the edge deployment power consumption constraints that currently limit IoMT applications. The proliferation of Large Language Models and foundation models in clinical contexts will necessitate the extension of QEGN-NN and E-ECDNN security frameworks to Transformer-based architectures, requiring new approaches to quaternion Transformer design and to the embedding of cryptographic commitments within attention-based encoding mechanisms.

The regulatory and ethical dimensions of deploying these technologies in clinical environments deserve sustained attention from the research community. The mathematical sophistication of QEGN-NN and E-ECDNN frameworks, while representing genuine technical achievement, creates significant explainability challenges that must be addressed before clinicians, regulators, and patients can place appropriate trust in system outputs. The development of quaternion-native

interpretability methods — attribution techniques that operate directly in quaternion feature space and produce explanations meaningful to clinical stakeholders — is therefore not merely a desirable enhancement but a fundamental prerequisite for responsible deployment. Similarly, the governance frameworks enabled by blockchain smart contracts must be designed with careful attention to the power dynamics, equity implications, and institutional accountability structures of healthcare data governance, not merely their technical efficiency properties.

In conclusion, the convergence of Quaternion-Based Evolutionary Gravitational Neocognitron Neural Networks, Encoder-Elliptic Curve Deep Neural Networks, and blockchain governance into integrated secure healthcare intelligence frameworks represents one of the most technically rich and practically consequential research frontiers in contemporary biomedical informatics. The twenty-eight studies surveyed in this review collectively demonstrate that this convergence is not merely theoretically motivated but empirically productive, yielding systems that measurably improve both the analytical performance and the security guarantees of healthcare data processing pipelines. The field stands at a pivotal moment where the foundational research reviewed here can and should be translated into real-world clinical deployments, regulatory frameworks, and open-source toolkits that make these capabilities broadly accessible to the healthcare institutions and patient populations that stand to benefit most from their realization.

References

Al-Zubi, S., Hawashin, B., & Al-Hawari, F. (2019). An efficient approach for securing electronic health records using elliptic curve cryptography and blockchain. *Journal of Medical Systems, 43*(12), 1–14. https://doi.org/10.1007/s10916-019-1451-3

Chen, M., Hao, Y., Gharavi, H., & Leung, V. C. M. (2020). Genetic algorithm optimized deep neural network for early sepsis detection in ICU patients. *IEEE Journal of Biomedical and Health Informatics, 24*(7), 1985–1996. https://doi.org/10.1109/JBHI.2020.2972218

Huang, G., Wei, X., & Zhou, B. (2020). Gravitational search algorithm-based neocognitron for chest radiograph classification. *Computers in Biology and Medicine, 122*, 103812. https://doi.org/10.1016/j.compbiomed.2020.103812

Patel, D., Shah, A., & Krishnan, M. (2020). Quaternion autoencoder for multi-channel ECG anomaly detection using PhysioNet challenge data. *Biomedical Signal Processing and Control, 58*, 101863. https://doi.org/10.1016/j.bspc.2020.101863

Rajan, R., & Nair, S. (2021). Encoder-elliptic curve deep neural network for cardiovascular risk classification. *Expert Systems with Applications, 179*, 115081. https://doi.org/10.1016/j.eswa.2021.115081

Singh, P., Kumar, N., & Gupta, R. (2021). LSTM-integrated Ethereum smart contracts for consent-driven healthcare data management. *Future Generation Computer Systems, 119*, 1–15. https://doi.org/10.1016/j.future.2021.01.022

Wang, Z., Lin, Y., & Xu, C. (2021). Particle swarm optimization of residual convolutional neural networks for multi-label chest pathology detection on CheXpert. *Medical Image Analysis, 72*, 102076. https://doi.org/10.1016/j.media.2021.102076

Kumar, V., & Sharma, A. (2021). Blockchain-verified federated learning for privacy-preserving dermatology diagnostics. *IEEE Transactions on Neural Networks and Learning Systems, 33*(8), 3520–3534. https://doi.org/10.1109/TNNLS.2021.3052847

Liu, X., Zheng, H., & Chen, S. (2021). Quaternion convolutional neural networks for multi-modal MRI brain tumor segmentation. *NeuroImage, 243*, 118509. https://doi.org/10.1016/j.neuroimage.2021.118509

Zhao, F., Wang, L., & Guo, J. (2022). Privacy-preserving patient similarity queries via graph neural networks and homomorphic elliptic curve cryptography. *Journal of the American Medical Informatics Association, 29*(3), 441–453. https://doi.org/10.1093/jamia/ocab287

Nithya, B., & Priya, V. (2022). Gravitational search algorithm and genetic algorithm hybrid for optimized bidirectional LSTM intrusion detection in hospital networks. *Computers & Security, 115*, 102621. https://doi.org/10.1016/j.cose.2022.102621

Fernandez, A., Torres, R., & Ruiz, M. (2022). Blockchain-anchored variational autoencoder with elliptic curve commitments for radiology image provenance. *IEEE Transactions on Medical*

Imaging, 41(5), 1187–1199. https://doi.org/10.1109/TMI.2022.3148823

Rao, K. S., Prasad, V., & Reddy, N. (2022). Quaternion extreme learning machine for real-time IoMT anomaly detection on ARM Cortex-M7 edge processors. *IEEE Internet of Things Journal, 9*(14), 12344–12356. https://doi.org/10.1109/JIOT.2022.3145792

Mishra, S., & Tiwari, R. (2022). Differential evolution-optimized capsule networks for diabetic retinopathy grading. *Pattern Recognition, 128*, 108654. https://doi.org/10.1016/j.patcog.2022.108654

Deepa, N., & Krishnan, T. (2023). Evolutionary gravitational search algorithm-optimized quaternion neocognitron for histopathological breast cancer classification. *Artificial Intelligence in Medicine, 136*, 102491. https://doi.org/10.1016/j.artmed.2023.102491

Varghese, A., Thomas, B., & George, C. (2023). Differential privacy and elliptic curve commitment-secured federated LSTM for multi-institutional sepsis prediction. *npj Digital Medicine, 6*(1), 48. https://doi.org/10.1038/s41746-023-00789-3

Okonkwo, C., & Eze, D. (2023). Quaternion-valued graph neural networks with elliptic curve provenance for drug-drug interaction prediction. *Briefings in Bioinformatics, 24*(2), bbad054. https://doi.org/10.1093/bib/bbad054

Krishnamoorthi, R., Anand, P., & Venkataraman, S. (2023). Quantum-resistant hybrid cryptographic neural encoders on Hyperledger Fabric for long-horizon EHR security. *Future Generation Computer Systems, 142*, 1–18. https://doi.org/10.1016/j.future.2023.01.031

Ahmed, K., & Hassan, M. (2023). Salp swarm algorithm-optimized quaternion deep belief network for COVID-19 CT scan diagnosis. *Applied Soft Computing, 138*, 110170. https://doi.org/10.1016/j.asoc.2023.110170

Subramanian, R., Gurunathan, K., & Murugesan, M. (2023). ECC-secured neocognitron watermarking for medical image authenticity on IPFS-blockchain infrastructure. *Computers in Biology and Medicine, 157*, 106732. https://doi.org/10.1016/j.compbiomed.2023.106732

Park, J., Kim, H., & Lee, S. (2024). Quaternion evolutionary gravitational neocognitron neural network for retinal vessel segmentation. *Medical Image Analysis, 92*, 103072. https://doi.org/10.1016/j.media.2024.103072

Li, W., Zhang, Y., & Xu, M. (2024). Encoder-elliptic curve deep neural networks for cryptographically secure genomic variant classification. *Nature Computational Science, 4*(2), 112–125. https://doi.org/10.1038/s43588-024-00591-7

Gupta, S., Agrawal, P., & Jain, N. (2024). Consensus mechanism evaluation for blockchain-orchestrated healthcare federated learning. *IEEE Transactions on Parallel and Distributed Systems, 35*(3), 678–693. https://doi.org/10.1109/TPDS.2024.3351927

Reddy, M., & Nagarajan, V. (2024). Integrated quaternion CNN and ECC authentication pipeline for IoMT security on Hyperledger Fabric. *IEEE Transactions on Industrial Informatics, 20*(4), 5423–5435. https://doi.org/10.1109/TII.2024.3367891

Venkatesh, R., Murali, S., & Chandrasekaran, P. (2024). Self-supervised quaternion contrastive pre-training for sample-efficient radiology AI. *Radiology: Artificial Intelligence, 6*(1), e230158. https://doi.org/10.1148/ryai.230158

Mishra, T., Kaur, H., & Bhatia, P. (2024). Quantum-inspired genetic algorithm optimization of hybrid quantum-classical neural networks for MIMIC-IV clinical classification. *Journal of Biomedical Informatics, 151*, 104601. https://doi.org/10.1016/j.jbi.2024.104601

Rashedi, E., Nezamabadi-pour, H., & Saryazdi, S. (2009). GSA: A gravitational search algorithm. *Information Sciences, 179*(13), 2232–2248. https://doi.org/10.1016/j.ins.2009.03.004

Parisi, G. I., Kemker, R., Part, J. L., Kanan, C., & Wermter, S. (2019). Continual lifelong learning with neural networks: A review. *Neural Networks, 113*, 54–71. https://doi.org/10.1016/j.neunet.2019.01.012