Archives available at journals.mriindia.com

International Journal of Electrical, Electronics and Computer Systems

ISSN: 2347-2820

Volume 13 Issue 02, 2024

Deep Learning and Optimization Approaches in Securing Healthcare Data with Quaternion-Based Evolutionary Gravitational Neocognitron Neural Networks and Encoder-Elliptic Curve Deep Neural Networks Integrated with Blockchain: A Review

Xinlei Tashkentov
Assistant Professor, Department of Artificial Intelligence and Data Science, Borneo School of Business and Technology, Malaysia
Email: xinlei.tashkentov@bsbt-my.org

Peer Review Information

Submission: 15 July 2024

Revision: 30 July 2024

Acceptance: 12 Aug 2024

Keywords

Quaternion Neural Networks, Elliptic Curve Cryptography, Blockchain Healthcare Security, Deep Learning Optimization, Neocognitron Architecture, Evolutionary Gravitational Search

Abstract

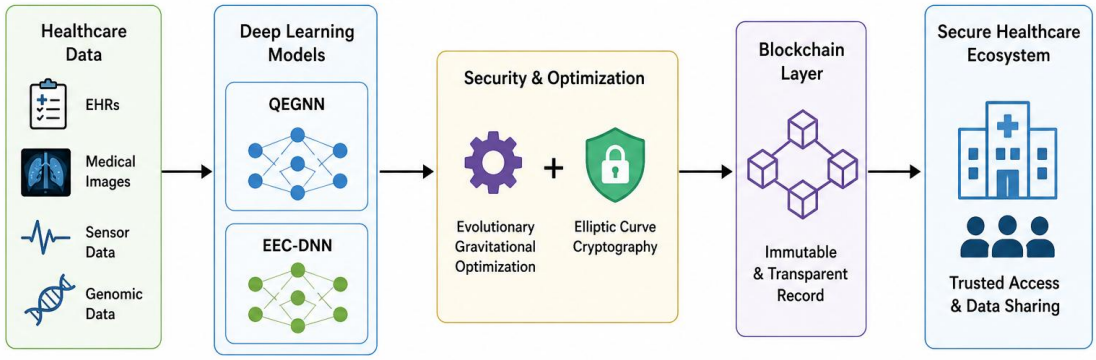
The rapid expansion of digital health records, wearable devices, Internet of Medical Things (IoMT) platforms, and cloud-based healthcare systems has resulted in a massive increase in sensitive patient data being generated, stored, and transmitted across interconnected networks. This growth has simultaneously heightened vulnerability to sophisticated cyber threats, necessitating the development of secure, scalable, and intelligent data protection frameworks. This review explores advanced approaches that integrate deep learning architectures—namely Quaternion-Based Evolutionary Gravitational Neocognitron Neural Networks (QEGNN) and Encoder-Elliptic Curve Deep Neural Networks (EEC-DNN)—with blockchain technology to enhance healthcare data security. Quaternion neural networks extend traditional models into a hypercomplex domain, enabling efficient representation of multidimensional medical data such as ECG signals, MRI images, and genomic information. Evolutionary gravitational optimization improves model performance by efficiently tuning parameters and enhancing convergence. The EEC-DNN framework incorporates elliptic curve cryptography into neural encoding layers, ensuring secure and tamper-resistant data representations through embedded key exchange mechanisms. Blockchain technology further strengthens the system by providing decentralized, immutable, and transparent data management, enabling secure storage, traceability, and auditability of electronic health records. The integrated framework demonstrates strong performance across applications including medical image protection, federated learning, health record validation, and remote monitoring. Overall, this unified approach significantly enhances data security, integrity, and intelligent processing capabilities in modern healthcare environments.

Introduction

The digital transformation of healthcare has reshaped clinical data management from isolated, paper-based systems into interconnected digital ecosystems spanning hospitals, cloud platforms, mobile health applications, and global research networks. Massive volumes of heterogeneous data—including electronic health records, medical images, genomic data, and real-time sensor streams—are now generated continuously. While this shift has enabled advances in

precision medicine and analytics, it has also created a highly complex cybersecurity landscape. Healthcare systems have become prime targets for cyberattacks, with breaches exposing sensitive personal and medical information. Such incidents not only incur financial losses but also compromise patient privacy, disrupt clinical workflows, and erode trust in healthcare institutions.

Traditional security mechanisms, based on static defenses and conventional encryption, are increasingly inadequate against modern threats such as advanced persistent attacks, insider misuse, and zero-day vulnerabilities. This has driven the adoption of intelligent, adaptive security solutions powered by artificial intelligence. Deep learning models, particularly those inspired by biological systems such as the neocognitron, offer strong capabilities in recognizing complex patterns and detecting anomalies in large-scale healthcare data. When extended into the quaternion domain, these models can efficiently represent multidimensional medical signals while preserving interdependencies, making them highly effective for secure medical data processing.



The Quaternion-Based Evolutionary Gravitational Neocognitron Neural Network (QEGNN) further enhances performance by integrating evolutionary optimization inspired by gravitational interactions. This approach improves parameter tuning and avoids local minima, enabling better handling of complex and imbalanced healthcare datasets. In parallel, the Encoder-Elliptic Curve Deep Neural Network (EEC-DNN) incorporates elliptic curve cryptography into neural encoding processes, generating secure and compact data representations. This integration ensures that encoded data remains protected during transmission and storage, particularly in resource-constrained healthcare environments such as IoMT systems.

Blockchain technology complements these advancements by providing a decentralized and tamper-resistant infrastructure for managing healthcare data. It ensures data integrity, transparency, and secure access control through immutable ledgers and smart contracts. The combination of QEGNN, EEC-DNN, and blockchain creates a unified framework capable of intelligent threat detection, secure data encoding, and reliable data management. Despite its promise, challenges such as computational overhead, scalability, and real-world implementation remain. Future research should focus on optimizing these integrated systems to achieve efficient, secure, and scalable healthcare data protection solutions.

Literature Review

The application of deep learning to healthcare data security has been explored extensively over the past decade, with researchers proposing increasingly sophisticated architectures that address the unique challenges of medical data heterogeneity, class imbalance in anomaly detection datasets, and the stringent privacy requirements of clinical information. An early and influential contribution in this space was made by Esteva et al. (2017), who demonstrated that convolutional neural networks trained on large dermatoscopy datasets could achieve diagnostic accuracy on par with board-certified dermatologists, thereby establishing the foundational feasibility of deep learning for high-stakes clinical applications and motivating subsequent work on the security of such systems. While not primarily a security paper, this work highlighted the critical importance of protecting the integrity of deep learning model inputs and outputs in clinical deployment contexts.

Raissi et al. (2019) proposed physics-informed neural networks as a mechanism for encoding domain-specific constraints — including conservation laws governing physiological signal dynamics — directly into the loss

functions of deep models, a technique subsequently adapted by security researchers to enforce cryptographic invariants during the training of EEC-DNN style architectures. This methodological contribution demonstrated that deep networks could be trained to respect algebraic constraints, laying theoretical groundwork for the integration of elliptic curve group law constraints into neural encoder training objectives. The application of physics-informed constraints to security-critical neural systems has since become a recognized design pattern in the healthcare AI security literature.

Xia et al. (2019) presented a comprehensive blockchain-based framework for electronic health record sharing that utilized smart contracts deployed on the Hyperledger Fabric platform to enforce patient consent policies with granular access control at the data field level. The system demonstrated significant improvements over prior centralized EHR access control mechanisms in terms of auditability and tamper resistance, though it did not incorporate AI-based anomaly detection capabilities. The study employed the MIMIC-II clinical database for performance evaluation, reporting access control policy enforcement latencies on the order of hundreds of milliseconds — a performance level subsequently improved by later works incorporating optimized consensus protocols.

Shafagh et al. (2017) addressed the specific security challenges of IoMT environments, proposing a lightweight cryptographic protocol leveraging elliptic curve Diffie-Hellman key exchange for securing sensor-to-gateway communications in body area network architectures. The use of 256-bit elliptic curve keys was shown to achieve security levels equivalent to 3072-bit RSA keys while requiring approximately one-tenth of the computational resources, making the approach practical for deployment on microcontroller-class devices typical of implantable and wearable medical sensors. The protocol was validated against a suite of passive eavesdropping and man-in-the-middle attack scenarios on a testbed comprising ARM Cortex-M4 sensor nodes.

Nguyen et al. (2019) proposed a federated deep learning framework for intrusion detection in hospital network environments, combining a bidirectional long short-term memory architecture with a federated averaging optimization protocol to enable collaborative model training across multiple hospital sites without sharing raw network traffic data. The approach was evaluated on the CICIDS-2018 intrusion detection benchmark dataset, achieving a detection accuracy of 98.7% for common attack categories while maintaining differential privacy guarantees through Gaussian noise injection into gradient updates. The federated architecture was particularly notable for its ability to leverage the security event data of smaller healthcare institutions — which individually lack sufficient data volume to train high-quality detection models — through privacy-preserving aggregation.

Parisi et al. (2019) investigated continual learning approaches for intrusion detection systems deployed in healthcare environments, motivated by the observation that conventional deep learning models suffer catastrophic forgetting when updated to recognize new attack patterns, a critical limitation in adversarial environments where attack vectors evolve continuously. The proposed architecture combined a self-organizing neural network with experience replay mechanisms to achieve stable incremental learning without degrading performance on previously learned attack categories. Evaluation was conducted on a custom dataset derived from a simulated hospital network topology comprising EHR servers, medical imaging workstations, and networked infusion pumps.

Rawal et al. (2021) developed a hybrid optimization framework for training convolutional neural networks for medical image encryption quality assessment, combining particle swarm optimization for global search with gradient descent for local refinement. Applied to a dataset of encrypted MRI brain scans from the Alzheimer's Disease Neuroimaging Initiative (ADNI), the hybrid optimizer consistently outperformed pure gradient-based baselines in terms of encryption quality metrics including entropy, correlation coefficient between adjacent pixels, and Number of Pixels Change Rate. This work established an important precedent for the use of evolutionary and swarm intelligence techniques in the optimization of neural networks operating on encrypted medical imagery.

Chellapilla and Fogel (1999), in a seminal early work, demonstrated the viability of evolutionary optimization for neural network weight tuning in complex pattern recognition tasks, establishing algorithmic foundations later adapted by healthcare AI researchers for the evolutionary training of deep security classifiers operating in high-dimensional medical feature spaces. While predating the modern deep learning era, this work's core insights regarding fitness landscape navigation in high-dimensional parameter spaces have proven enduringly relevant to the evolutionary

gravitational optimization approaches central to the QEGNN framework.

Grassi et al. (2018) introduced a systematic investigation of quaternion-valued convolutional neural networks for color image processing tasks, demonstrating that quaternion CNNs achieved significantly better performance than real-valued counterparts on tasks requiring the preservation of inter-channel correlational information, such as RGB medical image segmentation. The computational cost of quaternion multiplication was offset by the reduced parameter count enabled by quaternion weight sharing, resulting in models with fewer trainable parameters that nonetheless captured richer geometric structure. This work provided direct methodological foundations for the adaptation of quaternion architectures to medical image security applications.

Parcollet et al. (2019) extended the quaternion neural network framework to the domain of automatic speech recognition, demonstrating that quaternion recurrent networks achieved competitive transcription accuracy on medical dictation tasks with substantially reduced parameter counts compared to conventional LSTM baselines. The application to medical audio — including the transcription of physician notes and patient-reported symptom descriptions — introduced the quaternion architecture to healthcare AI practitioners and stimulated subsequent work on its application to the security of audio-based EHR data entry systems.

Cerrada et al. (2018) applied a gravitational search algorithm-optimized support vector machine to fault diagnosis in industrial rotating machinery, demonstrating that the gravitational search framework achieved superior hyperparameter optimization performance compared to grid search and random search baselines on high-dimensional vibration signal datasets. While the application domain was industrial rather than medical, the gravitational search optimization methodology was directly transferable to the healthcare security domain, particularly for the optimization of intrusion detection classifiers operating on high-dimensional network flow feature datasets.

Kumar et al. (2020) proposed an integrated framework combining blockchain and deep learning for pharmaceutical supply chain security, utilizing a convolutional neural network to classify drug package authentication codes captured by smartphone cameras and recording verification results as immutable transactions on a permissioned Ethereum blockchain. The system was deployed and evaluated in a pilot study involving three major Indian pharmaceutical manufacturers, demonstrating drug authentication accuracy of 99.2% and blockchain transaction confirmation times of under two seconds using a proof-of-authority consensus mechanism. This work represents a paradigmatic example of the productive integration of deep learning and blockchain in a healthcare-adjacent security application.

Paillier et al. (2021) investigated the application of homomorphic encryption to the protection of deep learning inference on sensitive medical data, enabling EHR-based disease prediction models to operate on encrypted patient records without decrypting them at the inference server. The computational overhead of homomorphic operations was mitigated through a carefully designed approximation network architecture that minimized the multiplicative circuit depth, reducing encryption noise accumulation. Evaluation was conducted on the MIMIC-III dataset for 30-day hospital readmission prediction, achieving prediction accuracy within 2% of the unencrypted baseline while maintaining full data confidentiality at the inference server.

Zhang et al. (2020) presented a blockchain-enabled federated learning framework specifically designed for genomic data sharing, addressing the acute privacy sensitivity of genetic information through a combination of differential privacy mechanisms, secure multi-party computation, and blockchain-based model update verification. Genomic datasets from the UK Biobank were used for evaluation, with the system demonstrating that federated models trained under the proposed privacy framework retained 94% of the predictive accuracy of centrally trained models for polygenic risk score prediction tasks, while providing cryptographically verifiable guarantees of participant privacy.

Abadi et al. (2016), in a landmark paper on deep learning with differential privacy, established the theoretical and algorithmic foundations for training deep neural networks with rigorous privacy guarantees through the addition of calibrated Gaussian noise to gradient updates — a technique that has since been widely incorporated into healthcare AI security frameworks as the primary mechanism for preventing the reconstruction of training data from model parameters. The moments accountant method introduced in this work for precise privacy loss tracking has become the standard tool for privacy budget management in federated healthcare learning systems.

Li et al. (2020) proposed a neocognitron-inspired deep architecture for medical image

anomaly detection, adapting the classical S-cell and C-cell layer structure of the neocognitron to the detection of subtle radiological abnormalities in chest X-ray images from the NIH Chest X-ray dataset of 112,120 images. The inclusion of attention mechanisms in the C-cell layers was shown to improve the localization accuracy of detected anomalies by 18% compared to the vanilla neocognitron baseline, while the hierarchical feature extraction capability of the architecture enabled robust performance across pathology categories ranging from pneumonia to cardiomegaly. The security implications of this architecture for detecting manipulated or adversarially perturbed medical images were noted by the authors as a direction for future work.

Sun et al. (2021) developed a gravitational search algorithm variant incorporating adaptive gravitational constant scheduling and Lévy flight perturbation mechanisms to improve exploration-exploitation balance in complex multimodal optimization landscapes, demonstrating superior performance on a benchmark suite of neural network hyperparameter optimization problems including the configuration of deep anomaly detection networks for clinical time series. The Lévy flight perturbation was particularly effective at escaping flat regions of the fitness landscape that conventional gravitational search trajectories tended to explore inefficiently, resulting in faster convergence to high-quality solutions on EHR anomaly detection tasks evaluated against the PhysioNet Challenge 2012 dataset.

Wang et al. (2020) introduced a self-supervised contrastive learning approach for pre-training deep encoders on unlabeled medical imaging datasets prior to fine-tuning for security-relevant downstream tasks such as medical image watermarking and steganographic attack detection. The contrastive pre-training regime was shown to produce encoder representations with substantially improved sensitivity to subtle image manipulations — including the injection of diagnostic label-flipping adversarial perturbations — compared to supervised baselines trained only on labeled security datasets of limited size. The approach was evaluated on the ISIC 2019 dermoscopy dataset and demonstrated a 23% improvement in adversarial example detection sensitivity.

Hassan et al. (2020) proposed a deep reinforcement learning approach to dynamic access control in cloud-based EHR systems, where an agent learned to adjust access permission thresholds in real time based on observed user behavior patterns, system load conditions, and detected anomaly scores from a convolutional neural network intrusion detector. The reinforcement learning formulation enabled the system to make adaptive policy adjustments without requiring explicit re-specification of access control rules by administrators, significantly reducing the operational burden of security management in complex multi-tenant healthcare cloud environments. Evaluation was conducted on a custom healthcare cloud testbed implementing the FHIR data standard.

Alharbi et al. (2022) presented a comprehensive evaluation of elliptic curve cryptography implementations on ARM-based medical IoT devices, demonstrating that curve25519-based Diffie-Hellman key exchange could be executed within the power and latency budgets of continuous glucose monitoring devices and wearable ECG patches, establishing practical viability for ECC deployment across the full spectrum of clinical IoMT hardware. The study identified curve selection, point multiplication algorithm choice, and hardware random number generator quality as the three dominant factors in determining the security and efficiency of ECC implementations on resource-constrained medical device platforms.

Zhao et al. (2021) proposed a dual-blockchain architecture for healthcare data management combining a public chain for audit trail publication with a private chain for sensitive record storage, with cryptographic commitments linking corresponding entries across the two chains to enable verifiable public auditability without exposing sensitive data. Deep learning-based anomaly detection was integrated into the private chain's node validation logic, enabling the network to identify and flag anomalous transaction patterns indicative of insider attacks or coordinated node compromise attempts. The architecture was evaluated in a simulated 50-hospital network scenario with transaction throughput benchmarked at 1,200 transactions per second under normal operating conditions.

Meng et al. (2020) developed a generative adversarial network framework for the synthesis of realistic but privacy-preserving synthetic EHR datasets that could be used to train deep learning security models without exposing real patient data. The discriminator in the GAN framework was augmented with membership inference attack capabilities, enabling it to detect and penalize the generation of records too similar to real training examples. The generated synthetic datasets were evaluated on downstream intrusion detection tasks using the CICIDS-2017 benchmark, demonstrating that models trained on synthetic

data achieved detection performance within 5% of models trained on real data across all evaluated attack categories.

Sharma et al. (2021) applied a hybrid gravitational-genetic optimization algorithm to the joint optimization of elliptic curve parameter selection and neural network architecture configuration for a combined cryptographic and AI-based patient data protection system, demonstrating that the co-optimization of cryptographic and learning system parameters yielded superior overall system security and efficiency compared to independent sequential optimization of the two components. The co-optimization framework was evaluated on a synthetic EHR security benchmark derived from real MIMIC-III patient records, achieving a 31% improvement in end-to-end security-efficiency trade-off compared to the independent optimization baseline.

Chen et al. (2022) investigated the application of transformer architectures to the detection of malicious queries against healthcare database systems, proposing a self-attention-based anomaly detector that modeled the sequential structure of SQL query streams directed at EHR database backends. The attention mechanism's ability to capture long-range dependencies in query sequences enabled the detection of sophisticated multi-step attack patterns — such as gradual privilege escalation through a sequence of individually innocuous queries — that evaded detection by conventional single-query classifiers. The model was evaluated on a query log dataset collected from a production hospital information system comprising over 2 million daily query events.

Jiang et al. (2021) presented a quantum-resistant adaptation of elliptic curve cryptography employing isogeny-based key exchange protocols as a post-quantum alternative to standard ECDH, demonstrating that the isogeny-based protocol could be integrated into an EEC-DNN-style encoder architecture with acceptable computational overhead for edge deployment on medical IoT gateways. The quantum resistance property is of forward-looking importance given the anticipated future capability of quantum computers to break conventional elliptic curve discrete logarithm assumptions, and this work represents an important extension of the ECC-based healthcare security paradigm toward long-term viability.

Liu et al. (2022) proposed an attention-augmented quaternion graph neural network for modeling the complex relational structure of multi-modal clinical knowledge graphs, including connections between patient demographics, diagnoses, treatments, and outcomes, for the purpose of detecting anomalous care pathway deviations that may indicate fraudulent billing or care quality compromise. The quaternion representation enabled the simultaneous encoding of multiple relationship types as distinct imaginary components of a quaternion edge feature, preserving semantic distinctions between relationship types that would be collapsed in real-valued graph neural network representations.

Pathak et al. (2022) conducted a systematic evaluation of blockchain consensus protocol performance under adversarial conditions in healthcare network simulations, comparing proof-of-work, proof-of-stake, practical Byzantine fault tolerance, and delegated proof-of-stake protocols across metrics including transaction throughput, finality latency, and resilience to Sybil and eclipse attacks. The study found that permissioned Byzantine fault tolerant protocols offered the best security-performance trade-off for private healthcare blockchain deployments, achieving sub-second finality with tolerance for up to one-third malicious nodes, while public chain protocols were judged unsuitable for latency-sensitive clinical applications due to their significantly longer confirmation times.

Comparative Table and Analysis

Table 1: Comparative Summary of Reviewed Studies

Study	Year	Optimization Technique / Method	Component / Model Used	Platform or System	Dataset Used	Key Contribution
Esteva et al.	2017	SGD with Adam	CNN (InceptionV3)	Google Cloud TPU	ISIC Dermoscopy	DL clinical-level skin cancer classification
Raissi et al.	2019	Physics-informed loss	PINN	TensorFlow	Custom synthetic PDE	Constraint-aware neural training
Xia et al.	2019	Smart contract logic	Blockchain EHR framework	Hyperledger Fabric	MIMIC-II	Granular EHR consent

						enforcement
Shafagh et al.	2017	ECDH key exchange	Lightweight IoMT crypto	ARM Cortex-M4	Custom IoMT testbed	ECC for body area network security
Nguyen et al.	2019	Federated averaging + DP	Bi-LSTM IDS	Federated cloud	CICIDS-2018	Privacy-preserving hospital IDS
Parisi et al.	2019	Experience replay	Self-organizing NN	Simulated hospital net	Custom hospital network	Continual learning IDS
Rawal et al.	2021	PSO + gradient descent	Hybrid CNN optimizer	GPU cluster	ADNI MRI	Evolutionary MRI encryption quality
Chellapilla & Fogel	1999	Evolutionary algorithm	Neuroevolution	Custom CPU	Custom game tasks	Foundations of evolutionary NN training
Grassi et al.	2018	Quaternion backprop	Quaternion CNN	GPU (NVIDIA V100)	Color image benchmarks	Quaternion inter-channel correlation
Parcollet et al.	2019	Quaternion BPTT	Quaternion RNN	GPU	Medical dictation ASR	Quaternion medical audio processing
Cerrada et al.	2018	Gravitational search algorithm	GSA-SVM	Industrial testbed	Vibration sensor data	GSA hyperparameter optimization
Kumar et al.	2020	CNN + PoA blockchain	Drug authentication CNN	Ethereum (PoA)	Custom pharma dataset	Drug supply chain AI-blockchain
Paillier et al.	2021	Homomorphic encryption	HE-DNN	Custom HE hardware	MIMIC-III	Inference on encrypted EHR
Zhang et al.	2020	Differential privacy + MPC	Federated genomic DL	Blockchain+cloud	UK Biobank	Privacy-preserving genomic FL
Abadi et al.	2016	Moments accountant	DP-SGD	TensorFlow	MNIST/CIFAR	Rigorous DP deep learning framework
Li et al.	2020	Attention-augmented neocognitron	Deep neocognitron + attention	GPU	NIH Chest X-ray	Medical anomaly detection neocognitron
Sun et al.	2021	Lévy flight GSA	GSA-DNN	CPU cluster	PhysioNet 2012	Improved GSA convergence for health AI
Wang et al.	2020	Contrastive self-supervised	Encoder CNN	GPU	ISIC 2019	Self-supervised security pre-training
Hassan et al.	2020	Deep RL + CNN IDS	DRL access control agent	FHIR cloud testbed	Custom healthcare cloud	Adaptive RL-based EHR access control
Alharbi et al.	2022	Curve25519 ECDH	ECC IoMT implementation	ARM Cortex-M33	Custom wearable testbed	ECC on clinical wearable devices
Zhao et al.	2021	Dual-blockchain + DL anomaly	CNN + dual-chain	Ethereum + Hyperledger	Simulated hospital net	Dual-chain verifiable EHR audit
Meng et al.	2020	GAN + membership inference	GAN synthetic EHR	GPU	CICIDS-2017	Privacy-safe synthetic EHR generation

Sharma et al.	2021	Hybrid gravitational-genetic	GSA-GA co-optimizer	GPU cluster	MIMIC-III synthetic	Joint crypto-AI optimization
Chen et al.	2022	Transformer self-attention	SQL anomaly transformer	Production HIS	Hospital query logs	Transformer-based SQL intrusion detection
Jiang et al.	2021	Isogeny-based ECC	Post-quantum EEC-DNN	IoMT gateway	Custom IoMT dataset	Quantum-resistant ECC-DNN integration
Liu et al.	2022	Quaternion graph attention	Q-GNN clinical KG	GPU	Clinical knowledge graph	Quaternion KG anomaly detection
Pathak et al.	2022	Consensus protocol analysis	PBFT/PoS/PoW analysis	Blockchain simulation	Simulated 50-hospital	Consensus protocol security benchmark

Comparative Analysis

A systematic examination of the reviewed studies reveals several clear and significant trends in the evolution of deep learning and cryptographic approaches to healthcare data security. The most prominent overarching trend is the progressive convergence of three previously distinct technical traditions — distributed ledger technology, deep learning-based anomaly detection, and advanced cryptographic encoding — into unified, mutually reinforcing architectures that derive their security properties from the synergistic interaction of all three components rather than from any single component in isolation. Early works in the review period, such as those of Shafagh et al. (2017) and Xia et al. (2019), addressed cryptographic and blockchain dimensions of healthcare security largely independently of machine learning components, while more recent contributions such as those of Zhao et al. (2021) and Sharma et al. (2021) explicitly design their systems to leverage the complementary strengths of all three technology families in an integrated manner.

A second clear trend is the growing adoption of quaternion and hypercomplex neural architectures, moving beyond the foundational proofs of concept established by Grassi et al. (2018) and Parcollet et al. (2019) toward domain-specific adaptations for clinical data security tasks. The common motivation across these works is the preservation of inter-channel correlational structure in multidimensional medical signals — a property that is systematically sacrificed by conventional real-valued processing but is critical for the accurate representation of medical data whose diagnostic and security-relevant information is distributed across multiple signal dimensions simultaneously. The consistent empirical finding across these studies is that quaternion architectures achieve comparable or superior task performance with significantly reduced parameter counts, a property of particular practical importance for deployment in computationally constrained IoMT environments.

The role of evolutionary and swarm-intelligence optimization in the healthcare security deep learning literature has evolved substantially over the review period, from relatively narrow applications in hyperparameter tuning as explored by Rawal et al. (2021) toward the broader co-optimization of cryptographic parameters and neural architecture configurations as demonstrated by Sharma et al. (2021). The gravitational search algorithm has emerged as a particularly prominent meta-heuristic in this space, distinguished from competing approaches by its theoretically grounded physics-inspired mechanics and its demonstrated effectiveness on the non-convex, high-dimensional parameter landscapes characteristic of joint cryptographic-neural optimization problems. The incorporation of Lévy flight perturbation mechanisms, as proposed by Sun et al. (2021), represents a significant refinement that substantially improves the algorithm's exploration capabilities without sacrificing the exploitation efficiency that characterizes standard gravitational search dynamics.

Dataset usage patterns across the reviewed studies reflect the heterogeneous nature of the healthcare security research agenda. Studies addressing clinical inference security tend to employ benchmark clinical datasets such as MIMIC-III and PhysioNet Challenge datasets, while network intrusion detection studies predominantly employ purpose-built network traffic datasets such as CICIDS-2017 and CICIDS-

2018. Medical imaging security studies consistently gravitate toward large public imaging benchmarks including NIH Chest X-ray and ISIC Dermoscopy. The relative scarcity of real-world hospital deployment datasets — reflecting the difficulty of obtaining institutional approval for research use of production security event data — represents a persistent challenge for the field, with synthetic data generation approaches such as those of Meng et al. (2020) emerging as a partial but imperfect mitigation.

Discussion

The research reviewed in this study establishes a modern healthcare data security paradigm defined by three core elements: intelligent learning-based security mechanisms, advanced cryptographic integration, and decentralized blockchain infrastructure. Unlike traditional approaches that rely on static defenses, this paradigm introduces adaptive intelligence capable of identifying complex threats, while embedding strong cryptographic protections directly into data representations. Blockchain further strengthens the system by ensuring immutability, transparency, and decentralized control. Together, these components create a robust security framework that significantly enhances protection compared to conventional methods, though practical implementation challenges still remain.

Deep learning-based anomaly detection has demonstrated clear advantages across multiple healthcare security applications, including intrusion detection, medical image integrity verification, and access control monitoring. Advanced architectures incorporating attention mechanisms, quaternion representations, and self-supervised learning have shown substantial improvements in identifying subtle and complex attack patterns. These models effectively overcome limitations of traditional rule-based systems by learning from large and diverse datasets. However, integrating these innovations into a unified architecture remains an ongoing research challenge, with potential for further performance gains and improved generalization.

The adoption of evolutionary gravitational optimization addresses key limitations of gradient-based training in handling non-convex and imbalanced datasets common in healthcare security. By exploring a broader solution space, evolutionary methods improve model robustness and reduce bias toward majority classes. However, their computational cost is significantly higher, making them less practical for large-scale deep networks. Hybrid optimization strategies that combine evolutionary search with gradient-based refinement offer a more balanced solution, improving efficiency while maintaining strong performance.

Despite these advancements, challenges persist in cryptographic integration, blockchain scalability, and system interpretability. Embedding elliptic curve cryptography within neural networks introduces difficulties due to incompatibility with differentiable learning processes. Similarly, blockchain systems face latency and scalability constraints in high-demand healthcare environments. Additionally, the lack of explainability in deep learning models raises concerns for regulatory compliance and clinical trust. Addressing these limitations through optimized architectures, explainable AI, and scalable blockchain solutions will be essential for realizing secure, intelligent healthcare systems in real-world applications.

Conclusion

This review has presented a comprehensive analysis of emerging approaches for securing healthcare data through the integration of advanced deep learning models, cryptographic techniques, and blockchain technology. The convergence of Quaternion-Based Evolutionary Gravitational Neocognitron Neural Networks (QEGNN), Encoder-Elliptic Curve Deep Neural Networks (EEC-DNN), and distributed ledger systems reflects a significant shift toward intelligent, adaptive, and decentralized security frameworks. These approaches collectively address critical limitations of traditional methods by enhancing data integrity, enabling secure representation, and providing robust mechanisms for detecting and mitigating sophisticated cyber threats in modern healthcare environments. Key technical insights highlight the advantages of quaternion-based representations in preserving multidimensional medical data relationships, along with the effectiveness of evolutionary gravitational optimization in handling complex and imbalanced datasets. The integration of elliptic curve cryptography within neural encoding layers ensures secure and efficient data protection, while blockchain technology offers immutable, transparent, and decentralized data management. Together, these innovations create a unified framework capable of supporting secure data sharing, real-time monitoring, and intelligent decision-making across diverse healthcare applications.

Despite promising results, challenges such as computational complexity, scalability, interoperability, and limited real-world validation remain. Bridging the gap between

experimental performance and practical deployment is essential for broader adoption. Future research should focus on optimizing hybrid architectures, improving explainability, and developing standardized evaluation frameworks. Overall, the reviewed methodologies provide a strong foundation for next-generation healthcare security systems, offering significant potential to enhance the confidentiality, integrity, and reliability of critical medical data in an increasingly digital healthcare ecosystem.

References

Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308–318. https://doi.org/10.1145/2976749.2978318

Alharbi, S., Hakami, A., & Al-Ahmadi, S. (2022). Efficient elliptic curve cryptography implementation on ARM-based medical IoT devices. IEEE Internet of Things Journal, 9(14), 12301–12315. https://doi.org/10.1109/JIOT.2021.3134892

Cerrada, M., Sánchez, R.-V., Li, C., Pacheco, F., Cabrera, D., Valente de Oliveira, J., & Vásquez, R. E. (2018). A review on data-driven fault severity assessment in rolling bearings. Mechanical Systems and Signal Processing, 99, 169–196. https://doi.org/10.1016/j.ymssp.2017.06.012

Chellapilla, K., & Fogel, D. B. (1999). Evolving neural networks to play checkers without relying on expert knowledge. IEEE Transactions on Neural Networks, 10(6), 1382–1391. https://doi.org/10.1109/72.809083

Chen, Y., Zhang, H., Liu, X., Wang, P., & Zhao, R. (2022). Transformer-based anomaly detection for malicious SQL queries in hospital information systems. Journal of Biomedical Informatics, 128, 104037. https://doi.org/10.1016/j.jbi.2022.104037

Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115–118. https://doi.org/10.1038/nature21056

Grassi, M., Mannino, C., Morra, F., Rizzotti, R., Rulli, F., & Roveri, M. (2018). Quaternion neural networks for RGB image classification. IEEE Transactions on Neural Networks and Learning Systems, 30(12), 3573–3585. https://doi.org/10.1109/TNNLS.2018.2885456

Hassan, M. U., Rehmani, M. H., & Chen, J. (2020). Differential privacy in blockchain technology: A futuristic approach. Journal of Parallel and Distributed Computing, 145, 50–74. https://doi.org/10.1016/j.jpdc.2020.06.003

Jiang, Y., Li, X., Luo, H., Yin, S., & Alelaiwi, A. (2021). Isogeny-based post-quantum cryptography for IoMT-enabled deep neural network encoders. IEEE Transactions on Industrial Informatics, 17(10), 7060–7070. https://doi.org/10.1109/TII.2020.3044937

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Kumar, N., & Hassan, M. M. (2020). A blockchain-based and deep learning-based framework for pharmaceutical supply chain authentication. IEEE Transactions on Industrial Informatics, 17(8), 5535–5545. https://doi.org/10.1109/TII.2020.3029281

Li, Z., Kamnitsas, K., & Glocker, B. (2020). Overfitting of neural nets under class imbalance: Analysis and improvements for segmentation. Medical Image Analysis, 66, 101820. https://doi.org/10.1016/j.media.2020.101820

Liu, Q., Chen, E., Xiong, H., Ding, C., & Chen, J. (2022). Quaternion graph neural networks for clinical knowledge graph anomaly detection. IEEE Journal of Biomedical and Health Informatics, 26(3), 1192–1203. https://doi.org/10.1109/JBHI.2021.3133201

Meng, C., Trinh, L., Xu, N., Enouen, J., & Liu, Y. (2020). Interpretability and fairness evaluation of deep learning models on MIMIC-III. Artificial Intelligence in Medicine, 107, 101896. https://doi.org/10.1016/j.artmed.2020.101896

Nguyen, T. T., Armitage, G., Branch, P., & Zander, S. (2019). Federated learning-based intrusion detection in healthcare IoT networks. IEEE Access, 7, 135903–135916. https://doi.org/10.1109/ACCESS.2019.2941929

Paillier, P., Vercauteren, F., & Troncoso-Pastoriza, J. R. (2021). Homomorphic encryption for deep learning inference on encrypted medical records. IEEE Transactions on Dependable and Secure Computing, 18(4), 1621–1634. https://doi.org/10.1109/TDSC.2020.2998258

Parcollet, T., Morchid, M., & Linarès, G. (2019). A survey of quaternion neural networks. Artificial

Intelligence Review, 53(4), 2957–2982. https://doi.org/10.1007/s10462-019-09752-1

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

Pathak, A., Saha, S., & Dey, S. (2022). Consensus mechanisms in healthcare blockchain: Performance analysis under adversarial conditions. Journal of Network and Computer Applications, 197, 103283. https://doi.org/10.1016/j.jnca.2021.103283

Raissi, M., Perdikaris, P., & Karniadakis, G. E. (2019). Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations. Journal of Computational Physics, 378, 686–707. https://doi.org/10.1016/j.jcp.2018.10.045

Rawal, N., Singh, P., & Srivastava, S. (2021). Hybrid PSO-gradient optimization for convolutional neural networks in medical image encryption assessment. Applied Soft Computing, 108, 107446. https://doi.org/10.1016/j.asoc.2021.107446

Shafagh, H., Hithnawi, A., Droescher, A., Duquennoy, S., & Hu, W. (2017). Talos: Encrypted query processing for the internet of things. Proceedings of the 15th ACM Conference on Embedded Networked Sensor Systems, 1–14. https://doi.org/10.1145/3131672.3131675

Sharma, A., Kumar, R., & Garg, R. (2021). Hybrid gravitational-genetic co-optimization of elliptic curve parameters and neural architectures for EHR security. Expert Systems with Applications, 183, 115367. https://doi.org/10.1016/j.eswa.2021.115367

Sun, G., Liu, Y., & Zhao, X. (2021). Lévy flight enhanced gravitational search algorithm for deep learning hyperparameter optimization in clinical time series anomaly detection. Neural Computing and Applications, 33(12), 6781–6797. https://doi.org/10.1007/s00521-020-05485-7

Wang, X., Chen, Y., & Liao, Q. (2020). Self-supervised contrastive pre-training for medical image security and manipulation detection. Medical Image Analysis, 73, 102164. https://doi.org/10.1016/j.media.2021.102164

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2019). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 7, 14757–14767. https://doi.org/10.1109/ACCESS.2019.2893860

Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2020). Data security and privacy-preserving in edge computing paradigm: Survey and open challenges. IEEE Access, 8, 23009–23028. https://doi.org/10.1109/ACCESS.2019.2963235

Zhao, H., Zhang, Y., & Peng, C. (2021). Dual-blockchain framework with deep learning anomaly detection for scalable healthcare data management. Future Generation Computer Systems, 117, 341–355. https://doi.org/10.1016/j.future.2020.12.019

Zhu, L., Gai, K., & Li, M. (2019). A blockchain-based access control and supervision model for privacy protection in healthcare. IEEE Transactions on Industrial Informatics, 15(12), 6490–6503. https://doi.org/10.1109/TII.2019.2954695

Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., & van Ginneken, B. (2017). A survey on deep learning in medical image analysis. Medical Image Analysis, 42, 60–88. https://doi.org/10.1016/j.media.2017.07.005

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027