JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Machine Learning-Driven Security and Post-Quantum Cryptographic Integration for Secure Blockchain Systems: A Comprehensive Literature Review

[1]Ashok Raj R, [2]Dr. D. Maruthanayagam
[1]Research Scholar, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India
[2] Dean Cum Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.

Abstract: The rapid advancement of distributed systems, blockchain platforms, and quantum computing is fundamentally transforming modern cybersecurity requirements. While blockchain enables decentralized trust and immutable record management, the classical cryptographic foundations of these systems remain vulnerable to quantum-enabled attacks. Simultaneously, Machine Learning (ML) has emerged as a powerful tool for intelligent threat detection, anomaly analysis, ransomware identification, and adaptive intrusion prevention across large-scale digital infrastructures. The review categorizes existing works across five major dimensions: ML-driven cyber-threat intelligence, PQC-based cryptographic modernization, blockchain security enhancement, federated and decentralized learning protection, and integrated ML–PQC defense architectures. Reported findings demonstrate substantial improvements in detection accuracy (frequently exceeding 95–99%), enhanced blockchain throughput under quantum-resilient designs, optimized energy efficiency through adaptive consensus models, and stronger privacy guarantees via decentralized learning and zero-knowledge mechanisms. However, critical challenges remain, including scalability limitations, computational overhead of PQC algorithms, large signature sizes, reliance on simulated environments and integration complexity across heterogeneous platforms, dataset constraints, adversarial ML risks, and insufficient real-world quantum validation. The study analyzes ML-based blockchain threat detection, federated learning enabled privacy preservation, quantum-resistant cryptographic architectures, lightweight PQC deployments for IoT environments, intelligent consensus optimization, decentralized auditing mechanisms, and implementation-level cryptographic vulnerabilities. Sustainability considerations such as energy efficiency and carbon footprint also require deeper evaluation in quantum-safe deployments. Finally, this literature review paper systematically examines recent research focusing on the convergence of Machine Learning–driven security mechanisms and Post-Quantum Cryptographic (PQC) frameworks for building resilient and future-proof distributed ecosystems.

Keywords: Machine Learning, Artificial Intelligence, Federated Learning, Post-Quantum Cryptography (PQC), Blockchain Security, Quantum-Resistant Consensus, Intrusion Detection Systems, Smart Grid Security, IoT Security, Zero-Knowledge Proofs.

I. INTRODUCTION

The digital transformation of modern society has accelerated the adoption of distributed systems, machine Learning, artificial intelligence (AI), cloud computing, Internet of Things (IoT), and blockchain technologies across critical sectors such as finance, healthcare, smart grids, supply chains, and industrial automation. While these technologies enhance efficiency, transparency, and automation, they simultaneously introduce complex cybersecurity challenges. The increasing sophistication of cyber threats, combined with the rapid advancement of quantum computing, has raised serious concerns regarding the long-term security of existing cryptographic infrastructures [1]. Blockchain technology has emerged as a trusted decentralized framework offering immutability, transparency, and distributed consensus. However, most blockchain platforms rely on classical public-key cryptographic schemes such as RSA and Elliptic Curve Cryptography (ECC), which are vulnerable to quantum algorithms such as Shor's and Grover's. The potential capability of quantum computers to break widely deployed cryptographic primitives threatens the foundational trust mechanisms of blockchain networks, digital signatures, and secure communications. Consequently, Post-Quantum Cryptography (PQC) has become a critical research priority to ensure resilience against future quantum-enabled adversaries [2]. Parallel to cryptographic modernization, Artificial Intelligence and Machine Learning (ML) have become indispensable tools for dynamic threat detection, anomaly identification, ransomware classification, and intrusion detection in distributed environments. AI-driven models enhance adaptive defense mechanisms by analyzing large-scale network traffic, blockchain transactions, and IoT telemetry data. Furthermore, Federated Learning (FL) and privacy-preserving techniques such as Zero-Knowledge Proofs (ZKPs) enable decentralized intelligence without exposing sensitive data, addressing both privacy and scalability concerns. Recent research increasingly explores hybrid frameworks that integrate AI, ML, blockchain, and PQC to build secure, scalable, and future-proof infrastructures [3]. These approaches aim to combine quantum-resistant cryptographic primitives, intelligent consensus mechanisms, decentralized storage models, and ML-based detection engines. While promising results demonstrate high detection accuracy, improved throughput, and enhanced privacy preservation, significant challenges remain in scalability, computational overhead, interoperability, real-world validation, and sustainability evaluation.

This literature review systematically examines recent advancements (2022–2026) in ML-enhanced blockchain security and post-quantum cryptographic integration. The study categorizes existing works based on architectural design, cryptographic enhancements, ML-driven security mechanisms, consensus optimization, and domain-specific applications such as IoT, smart grids, cloud auditing, and healthcare systems. By identifying key trends, strengths, limitations, and open research gaps, this review provides a comprehensive roadmap for developing resilient, intelligent, and quantum-safe cybersecurity frameworks for next-generation distributed ecosystems.

II.LITERATURE REVIEW

2.1. Machine Learning–Based Security Approaches

Noha E. El-Attar et al. (2025) [4] address the critical challenge of detecting cryptocurrency-based money laundering within blockchain ecosystems, particularly the Ethereum network. As blockchain transactions are pseudonymous and globally accessible, identifying illicit financial flows remain a complex task for regulatory authorities. The authors propose a blockchain-oriented anomaly detection framework that integrates advanced machine learning techniques with metaheuristic optimization methods to enhance detection accuracy and robustness. The proposed model employs Particle Swarm Optimization (PSO) to select the most relevant feature subsets from a large-scale Ethereum dataset comprising 50 million transactions across 9,841 unique accounts. For classification, three machine learning algorithms like XGBoost, Support Vector Machine (SVM), and Isolation Forest (IF) are evaluated. To further enhance predictive performance, a Genetic Algorithm (GA) is applied for hyperparameter optimization. Experimental results indicate that XGBoost outperforms the other models, achieving 98% accuracy and 0.98 recall. When combined with GA optimization, performance improves further, reaching 99% across accuracy, precision, recall, and F1-score metrics. Although SVM and IF also benefit from GA tuning, they do not match the superior results achieved by XGBoost. Despite its strong performance, the framework demonstrates sensitivity to noisy or incomplete transaction data, with declines in precision and recall under such conditions. Additionally, GA-based hyperparameter tuning introduces computational overhead, particularly under extreme transaction volumes. The authors suggest future research directions including adaptive feature selection, data augmentation strategies, computational optimization, and validation across other blockchain platforms such as Bitcoin and Quorum to assess generalizability. Overall, the study contributes a robust, optimization-driven approach to blockchain-based financial crime detection. **Advantages:** The integration of PSO for feature selection and GA for hyperparameter tuning significantly enhances XGBoost performance, achieving up to 99% accuracy and recall. The model is validated on a substantial Ethereum dataset (50 million transactions), demonstrating practical applicability in real-world blockchain environments. **Disadvantages:** The framework’s performance declines when dealing with noisy, incomplete, or mislabeled transaction data. Genetic Algorithm-based hyperparameter optimization increases computational cost, potentially limiting scalability under very high transaction volumes.

Er. Kritika et al. (2025) [5] provide a comprehensive review of ransomware detection approaches, emphasizing the sharp rise in ransomware incidents in 2023 and the growing misuse of Ransomware-as-a-Service (RaaS) platforms. The study highlights how artificial intelligence has lowered the entry barrier for novice attackers, increasing the sophistication and frequency of attacks targeting individuals and organizations. In response, the paper explores deep learning–based mitigation frameworks as proactive early detection mechanisms. The review examines various deep learning architectures applied to ransomware detection, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Deep Belief Networks (DBN), and hybrid models such as CNN-BiLSTM and CNN-BiGRU. These models demonstrate high detection accuracy by extracting both spatial and sequential features from opcode sequences, API calls, and system behavior data. The paper particularly discusses hybrid frameworks like MRm-DLDet, which integrates ResNet-18, GRU, and attention mechanisms for memory forensics analysis using tools such as the Volatility framework. Additionally, the incorporation of GPT-3.5 for suspicious process analysis illustrates the emerging role of large language models in cybersecurity workflows. Despite promising results, the review identifies key challenges, including limited availability of labeled datasets, feature selection complexity, computational overhead, model interpretability issues, and vulnerability to adversarial attacks. Concerns regarding privacy, hallucination risks in AI-driven analysis and scalability constraints are also noted. The authors emphasize the need for collaborative data sharing, adversarial training, integration with broader cybersecurity frameworks, and expansion into domains such as cloud computing and cyber-physical systems. Overall, the literature reflects substantial progress in deep learning–based ransomware detection, while underscoring persistent practical and operational limitations. **Advantages:** Hybrid deep learning frameworks (e.g., CNN-BiLSTM, ResNet-GRU) effectively detect known and novel ransomware variants by capturing spatial and sequential features. Integration with memory forensics tools and AI models enhances detection depth and supports early-stage ransomware identification. **Disadvantages:** Scarcity of publicly available labeled datasets and dataset constraints affect model generalization and robustness. Deep learning models require significant computational resources and often function as black-box systems, reducing transparency and explainability.

Omar Dib et al., (2024) [6] address this challenge by proposing a Hybrid Ransomware Detection System (RDS) tailored to cryptocurrency transactions using the BitcoinHeist dataset. The dataset comprises 28 ransomware families grouped into three major categories Princeton, Montreal, and Padua alongside a white class representing legitimate transactions. This comprehensive dataset enables fine-grained classification of ransomware behaviors within blockchain transaction flows. The authors introduce a multistage hybrid framework combining supervised and semi-supervised learning techniques. For known ransomware families, ensemble-based supervised models such as Decision Tree, Random Forest, XGBoost, and Stacking are employed to enhance predictive accuracy and robustness. To address the limitation of traditional signature-based detection systems in identifying novel threats, the study integrates a semi-supervised anomaly detection mechanism. This component utilizes L-kmeans clustering and biased classifiers to detect previously unseen ransomware variants, thereby strengthening the system's adaptability. A notable contribution of the research lies in its feature engineering strategy, which incorporates a Gradient Boosting Classifier to extract discriminative transaction features. Hyperparameter optimization further refines model performance. Experimental evaluation using comprehensive metrics including accuracy, precision, recall, F1-score, ROC score, and prediction time demonstrates that the proposed RDS outperforms state-of-the-art ransomware detection approaches. The study also outlines future research directions, including real-time deployment in live cryptocurrency systems, scalability testing on larger datasets, integration of external threat intelligence, and expansion to other blockchain platforms. Overall, this work contributes significantly to blockchain security literature by combining signature-based and anomaly-based detection within a scalable, intelligent hybrid framework. **Advantages:** The hybrid supervised and semi-supervised framework effectively identifies both previously known ransomware families and unseen variants. The use of ensemble learning, feature engineering, and hyperparameter optimization results in superior accuracy, precision, recall, and ROC scores compared to existing methods. **Disadvantages:** The framework is primarily evaluated on the BitcoinHeist dataset and has not yet been fully tested in real-time cryptocurrency transaction environments. The multistage hybrid model, including clustering and ensemble techniques, may require significant computational resources when applied to large-scale blockchain networks.

Georgios Palaiokrassas et al. (2024) [7] present a systematic mapping study examining the application of Machine Learning (ML) techniques to blockchain data. Recognizing the exponential growth of blockchain-generated data and its analytical potential, the study aims to provide a structured overview of state-of-the-art research in this interdisciplinary domain. Following rigorous inclusion and exclusion criteria across major scientific databases such as Google Scholar, Springer, and ScienceDirect, the authors selected and analyzed 159 relevant articles. The selected studies were classified along four primary dimensions: domain and use case, blockchain platform, data characteristics, and ML models. The findings reveal that anomaly detection constitutes the most dominant use case (49.7%), reflecting growing concerns over fraud detection, illicit transactions, and network attacks. Address classification, cryptocurrency price prediction, smart contract vulnerability detection, and performance prediction were also significant areas of focus. In terms of blockchain platforms, Bitcoin (47.2%) and Ethereum received the most attention, indicating a concentration on widely adopted public blockchains. From a data perspective, a substantial proportion of studies (31.4%) utilized datasets exceeding one million data points, demonstrating the large-scale analytical nature of blockchain research. However, many studies did not publicly share their datasets, limiting reproducibility. Regarding ML tasks, classification (46.5%) emerged as the most prevalent approach, followed by clustering, regression, deep learning, graph learning, and time series analysis. Popular algorithms included Random Forest and Support Vector Machine, with common evaluation metrics such as Accuracy, Precision, Recall, F1-score, and ROC curves. The study highlights ongoing challenges, including the need for novel ML algorithms, lack of standardization frameworks, blockchain scalability constraints, and complexities in cross-chain analysis, suggesting promising avenues for future research. **Advantages:** The systematic mapping of 159 studies provides a well-organized overview of ML applications in blockchain, identifying trends, gaps, and research opportunities. The study highlights critical challenges such as scalability, cross-chain interactions, and lack of standardization, guiding future research directions. **Disadvantages:** Many reviewed studies did not share datasets, reducing reproducibility and comparability across research efforts. The strong focus on Bitcoin and Ethereum may overlook insights from emerging or private blockchain platforms, limiting generalizability.

Saveetha et al. (2024) [8] examine the vulnerability of blockchain networks to Distributed Denial of Service (DDoS) attacks, which remain one of the most severe threats affecting availability and network performance. Although blockchain systems are designed to provide transparency and immutability, their decentralized architecture can still be exploited by large-scale traffic flooding attacks. Traditional centralized machine learning (ML) approaches for DDoS detection require aggregation of global attack data, which is impractical due to privacy, scalability, and data-sharing constraints. To address this challenge, the authors propose a Blockchain-Integrated Federated Machine Learning (FML) framework for DDoS detection. Federated learning enables distributed model training across nodes without sharing raw data, thus preserving privacy. However, federated learning is itself susceptible to model poisoning attacks during the aggregation phase. To mitigate this, the study integrates blockchain mechanisms to securely store model updates and introduces a dynamic reputation-based miner selection strategy. This mechanism balances exploration and exploitation to select trustworthy miners for block validation and model training, thereby enhancing both blockchain integrity and model robustness. The proposed framework evaluates three machine learning models like Random Forest (RF), Multilayer Perceptron (MLP), and Logistic Regression (LR) for detecting varying levels of attack complexity. Experimental results indicate that Random Forest achieves superior performance with 99.1% accuracy, outperforming MLP (95.1%) and LR (88.5%). Comparative analysis with related works demonstrates improved detection metrics across evaluation parameters. While the study focuses solely on DDoS attacks, it suggests future extensions to other attack types and real-world Software-Defined Networking (SDN) environments, emphasizing the need for integrated detection and mitigation mechanisms in blockchain ecosystems. **Advantages:** The Random Forest-based model achieves 99.1% accuracy, outperforming other ML models and existing detection mechanisms. The reputation-based miner selection and blockchain storage protect both the federated learning model and the blockchain network from poisoning and DDoS attacks. **Disadvantages:** The framework addresses only DDoS attacks, limiting its applicability to other blockchain security threats. Integrating federated learning with blockchain and reputation mechanisms may introduce additional latency and resource consumption in real-world deployments.

Suliman Aladhadh et al. (2022) [9] address the growing need to secure blockchain platforms against cyberthreats, despite their inherent properties of decentralization and immutability. While blockchain and smart contracts provide strong guarantees for data integrity and peer-to-peer trust, they remain vulnerable to various attacks, including phishing, scamming, reentrancy, integer overflow, and other smart contract exploits. Existing protection mechanisms largely rely on statistical analysis embedded within smart contracts, often introducing significant deployment and runtime overhead. The authors observe that machine learning (ML), despite its strong potential for anomaly detection, has been insufficiently leveraged for blockchain protection. To overcome these limitations, the study proposes BChainGuard, a novel protection layer integrated into the Ethereum blockchain. The framework distinguishes between normal and abnormal network behavior using locally executed classification models, specifically Support Vector Machines (SVM) and Multilayer Perceptron (MLP). Instead of deploying full ML models on-chain, only the decision function is embedded as a smart contract. This design significantly reduces gas consumption and runtime overhead while maintaining security. Experimental evaluation demonstrates promising detection performance, achieving approximately 95% accuracy with SVM and 98.02% accuracy with MLP. BChainGuard not only enhances detection accuracy but also aims to protect datasets against poisoning attacks. However, the framework currently focuses on binary attack detection and is validated using datasets limited to phishing and scamming scenarios. The authors suggest future improvements including the use of more realistic datasets, additional ML/DL techniques and continuous model updates for emerging threats, and secure performance testing under adversarial conditions. Overall, the study contributes a lightweight and efficient ML-integrated blockchain defense framework. **Advantages:** By embedding only the decision function on-chain, BChainGuard achieves up to 98.02% accuracy while minimizing gas consumption and runtime overhead. Local ML execution combined with blockchain-based verification enhances security without overloading the blockchain network. **Disadvantages:** The framework detects only whether an attack occurred and focuses on two attack types (phishing and scamming), limiting general applicability. Only SVM and MLP are evaluated, potentially overlooking more advanced machine learning or deep learning techniques that could improve detection performance.

2.2. Post-Quantum Cryptography (PQC)–Based Security Approaches

Shirisha N et al. (2026) [10] investigate the practical deployment of lattice-based post-quantum cryptography (PQC) in resource-constrained Internet of Things (IoT) environments. While lattice-based schemes such as Kyber and NTRU are widely recognized as strong candidates for quantum-resistant security against threats posed by Shor’s and Grover’s algorithms, their real-world adoption in low-power and limited-memory devices remains challenging. The authors identify a critical research gap: most PQC proposals prioritize theoretical security without sufficiently addressing computational efficiency, energy consumption, and environmental sustainability in constrained systems. To bridge this gap, the study proposes a lightweight lattice-based security framework integrating encryption/decryption and key encapsulation/decapsulation mechanisms optimized for IoT scenarios. The methodology includes modeling a quantum-capable adversary, defining security objectives for constrained networks, tuning cryptographic parameters inspired by Kyber/NTRU configurations, and validating protocol feasibility through Contiki-NG and NS-3 simulations. Performance metrics include latency, communication overhead, and energy usage, while sustainability is assessed through carbon footprint estimations derived from device-level energy models. Simulation results demonstrate average encryption and decryption latencies of approximately 120 ms and 110 ms, respectively, with energy consumption below 4 mJ on edge devices. Although communication overhead increases by around 72% compared to classical schemes, it remains acceptable in low-power IoT settings. The study further compares the proposed solution with classical and alternative PQC approaches, confirming its balanced trade-off between security, efficiency, and sustainability. By incorporating environmental impact analysis, the research extends PQC evaluation beyond traditional performance metrics, offering a scalable roadmap for quantum-secure, energy-aware IoT ecosystems. **Advantages:** The framework evaluates not only performance but also energy consumption and carbon footprint, providing a holistic view of PQC deployment in IoT. Implementation and testing using Contiki-NG and NS-3 demonstrate realistic feasibility in heterogeneous, resource-constrained IoT networks. **Disadvantages:** The framework introduces approximately 72% higher communication overhead compared to classical schemes. Results are based on simulated environments, and large-scale real-world deployment validation is still required.

Abdullah Ayub Khan et al. (2025) [11] address the growing security concerns surrounding multimedia data storage and migration to cloud environments, particularly in the context of emerging quantum computing threats. As multimedia platforms increasingly rely on Blockchain Distributed Ledger Technology (BDLT) to ensure transparency and decentralized trust, the vulnerability of classical cryptographic primitives to quantum attacks poses a serious risk to data integrity, confidentiality, and privacy. To mitigate these challenges, the authors propose a novel framework that integrates BDLT with quantum-resilient post-quantum cryptographic (PQC) schemes for secure cloud-based multimedia auditing. The proposed architecture combines lattice-based cryptography, Zero-Knowledge Proofs (ZKPs), and smart contract automation to ensure secure and privacy-preserving public auditing of multimedia content. By embedding PQC mechanisms within blockchain-based verification processes, the framework aims to provide long-term resistance against quantum-enabled adversaries. Simulation results demonstrate promising performance improvements, achieving 98.21% accuracy in data integrity verification, a 96.84% reduction in quantum vulnerability, and an 87.85% increase in auditing efficiency compared to classical BDLT systems. Additionally, privacy leakage is reportedly reduced by 92.47%, highlighting the effectiveness of ZKP integration in maintaining stakeholder confidentiality. The study emphasizes scalability and transparency while maintaining robust privacy guarantees. However, the authors acknowledge several open research challenges, including optimization of PQC algorithms, scalability improvements in Hyperledger-based systems, integration of Quantum Machine Learning (QML) for threat analysis, and adaptation to multi-cloud and edge computing infrastructures. Overall, the work contributes a forward-looking, quantum-secure blueprint for privacy-preserving multimedia data management in decentralized cloud ecosystems. **Advantages:** Integrates BDLT, post-quantum cryptography, and ZKPs to ensure long-term data integrity and privacy protection against quantum threats. To demonstrates significant improvements in auditing efficiency, integrity verification accuracy, and reduction of privacy leakage. **Disadvantages:** Post-quantum cryptographic operations and Hyperledger-based blockchain integration may face scalability and computational efficiency limitations. Results are based on simulations, and practical implementation across multi-cloud or edge environments requires further empirical evaluation.

Nalavala Ramanjaneya Reddy et al. (2025) [12] examine the profound implications of quantum computing on blockchain security, emphasizing that widely deployed cryptographic primitives such as RSA, ECDSA, and SHA-256 are vulnerable to Shor’s and Grover’s algorithms. These vulnerabilities threaten the integrity and trustworthiness of blockchain-based systems used in finance, healthcare, and supply chains. The authors argue that existing mitigation efforts often address isolated components such as signatures or key exchange without offering a comprehensive, end-to-end quantum-resilient architecture. To overcome these limitations, the study proposes QuantumShield-BC, a modular blockchain framework integrating post-quantum cryptographic (PQC) signatures, Quantum Key Distribution (QKD), and a novel Quantum Byzantine Fault Tolerance (Q-BFT) consensus mechanism powered by Quantum Random Number Generation (QRNG). The framework aims to ensure secure transaction signing, tamper-proof key exchange, and fair validator consensus in adversarial quantum scenarios. Experimental simulations demonstrate that QuantumShield-BC achieves over 7,000 transactions per second with 100 validators, significantly outperforming many classical blockchain systems. Additionally, the framework reportedly eliminates Sybil attack effectiveness (0%) and mitigates replay and man-in-the-middle vulnerabilities. An ablation study confirms the importance of each quantum component in maintaining overall system robustness. Despite its promising results, the framework currently relies on simulated QKD environments and faces computational overhead from PQC operations. The authors suggest future work including real-world quantum hardware integration, optimization for low-resource nodes, large-scale validator testing, and exploration of multi-chain interoperability. Overall, QuantumShield-BC contributes a holistic roadmap for scalable, quantum-resistant blockchain infrastructures suitable for critical digital ecosystems. **Advantages:** Integrates PQC, QKD, QRNG, and a novel Q-BFT consensus mechanism to provide end-to-end quantum-resistant security. It achieves over 7,000 TPS with 100 validators while eliminating Sybil, replay, and MITM attack effectiveness in simulated environments. **Disadvantages:** QKD and quantum elements are tested in simulated settings, lacking real-world quantum hardware validation. Post-quantum cryptographic operations introduce additional computational costs, potentially impacting scalability in resource-constrained environments.

Velmurugan M et al. (2025) [13] propose PQ-PoETChain, a quantum-resistant blockchain architecture designed to address scalability, energy inefficiency, and vulnerability of classical cryptographic primitives to quantum attacks. Traditional blockchain systems rely on RSA/DSA signatures and consensus protocols such as Proof of Work (PoW) and Proof of Stake (PoS), which incur significant computational overhead and energy consumption, particularly in cloud-scale environments. Moreover, these classical schemes are susceptible to quantum algorithms, necessitating a shift toward post-quantum cryptographic (PQC) solutions. PQ-PoETChain integrates NTRU-based post-quantum signatures, an adaptive Proof of Elapsed Time (PoET) consensus mechanism executed within Trusted Execution Environments (TEEs), and a Lightweight Hash Validation (LHV) scheme. The adaptive PoET protocol dynamically adjusts consensus delay based on network load, improving efficiency under varying conditions. LHV further optimizes block verification by replacing traditional Merkle-tree traversal with constant-time hash-pointer validation, reducing cryptographic complexity to O(1). Experimental simulations conducted across 50–1000 nodes demonstrate strong performance: approximately 195 transactions per second (TPS), latency around 189 ± 4 ms at 500 nodes, and up to 91.8% energy reduction compared to PoW. NTRU signature operations remain under 2 ms, outperforming RSA, ECC, and DSA while providing quantum resistance. Despite these promising results, the framework depends heavily on TEEs (e.g., Intel SGX), introducing potential risks related to enclave attacks and side-channel vulnerabilities. Furthermore, evaluation is limited to controlled simulation environments, lacking real-world adversarial-scale testing. The study suggests future work including formal security proofs, heterogeneous network stress testing, TEE-independent trust primitives, and prototype deployment. Overall, PQ-PoETChain presents a scalable and energy-efficient blueprint for next-generation quantum-safe blockchain infrastructures. **Advantages:** Achieves ~195 TPS, low latency (<200 ms), and significant energy savings while integrating NTRU-based post-quantum security. Lightweight Hash Validation reduces verification complexity to O(1), lowering computational overhead compared to traditional Merkle-tree approaches. **Disadvantages:** Security relies on hardware-based TEEs, which may be vulnerable to side-channel or enclave attacks. Performance results are based on controlled simulations rather than large-scale, adversarial public blockchain environments.

Filip Opiłka et al. (2024) [14] examine the growing necessity of post-quantum cryptography (PQC) in response to the rapid advancement of quantum computing, which threatens the security of widely deployed public-key algorithms such as RSA. The study focuses specifically on digital signature schemes, evaluating the performance and practicality of leading PQC candidates CRYSTALS-Dilithium, Falcon, and SPHINCS+ implemented using the liboqs library. Through systematic benchmarking, the authors analyze key generation, signature creation, and verification processes, comparing them against the classical RSA algorithm to highlight trade-offs between computational efficiency and enhanced security. The experimental findings demonstrate that Dilithium, particularly Dilithium5, provides strong overall performance. It dominates in key pair generation and signing speed while maintaining relatively moderate verification times. Additionally, Dilithium produces significantly smaller signatures than SPHINCS+, making it suitable for bandwidth-sensitive applications. Falcon, on the other hand, generates the smallest signature sizes among the evaluated algorithms, positioning it as an optimal choice where storage or transmission constraints are critical. SPHINCS+, a hash-based signature scheme, offers flexibility through compatibility with various hash functions but generally produces larger signatures, though size disparities decrease with increasing file size. The study confirms that certain PQC algorithms can replace RSA with only marginal performance overhead while substantially improving security against quantum threats. The results are particularly relevant for emerging 5G and 6G services, where secure and efficient digital signature mechanisms are essential. Ultimately, the choice of a specific post-quantum algorithm depends on application requirements such as signature size, computational cost, and verification speed. **Advantages:** The study provides detailed comparative analysis of major PQC signature schemes against RSA, supporting informed algorithm selection. Real-world testing using the liboqs library confirms feasibility for deployment in next-generation communication systems like 5G/6G. **Disadvantages:** The analysis focuses only on signature schemes and does not evaluate encryption or key exchange mechanisms. The work emphasizes computational metrics, with limited discussion on implementation-level security issues such as side-channel resistance.

P. Thanalakshmi et al. (2023) [15] investigate the implications of quantum computing on blockchain security, particularly focusing on the vulnerability of classical digital signature schemes such as ECDSA. As blockchain systems rely heavily on digital signatures to ensure authenticity, integrity, and non-repudiation, the emergence of quantum algorithms capable of breaking elliptic curve cryptography poses a serious threat. To address this concern, the authors explore the integration of NIST-recommended post-quantum signature schemes Dilithium, FALCON, and SPHINCS+ within a blockchain framework. The study further enhances the proposed architecture by incorporating the InterPlanetary File System (IPFS) for decentralized data storage. Instead of storing full signatures and public keys directly on-chain, the system records only their hash values on the blockchain while storing the larger cryptographic artifacts in IPFS. This design reduces on-chain storage overhead and mitigates block capacity constraints. Performance comparisons are conducted within a Bitcoin-based UTXO transaction model, evaluating key generation, signing, and verification times of post-quantum algorithms against ECDSA. Experimental results indicate that Dilithium and FALCON demonstrate strong performance across cryptographic operations, making them suitable for practical deployment, especially when combined with IPFS for efficient key management. SPHINCS+, while secure, produces comparatively larger signatures. The study concludes that integrating post-quantum signatures with IPFS not only enhances quantum resistance but also improves blockchain efficiency. Although primarily evaluated within Bitcoin systems, the authors note the potential applicability to other blockchain platforms such as Ethereum and Polygon, while acknowledging additional complexity in smart contract-based environments. Overall, the work contributes to the long-term sustainability of blockchain infrastructures in the quantum era. **Advantages:** Integrates NIST-recommended post-quantum signature schemes, strengthening blockchain security against future quantum attacks. It is storing only hash values on-chain while offloading large cryptographic data to IPFS reduces block size constraints and enhances system efficiency. **Disadvantages:** The integration of IPFS with post-quantum signatures adds architectural complexity and potential interoperability challenges. The performance analysis focuses mainly on the Bitcoin UTXO model, with limited empirical validation in smart contract-based blockchains like Ethereum.

2.3. Integrated Machine Learning and Post-Quantum Cryptography Approaches

Mudassir Peeran et al., (2026) [16] examine this transition phase, highlighting the security vulnerabilities that emerge during the migration from conventional cryptographic systems (e.g., RSA and elliptic curve cryptography) to PQC algorithms. One of the most critical risks identified is the downgrade attack, wherein adversaries exploit protocol negotiation mechanisms to force communication endpoints to revert to weaker legacy cryptographic schemes despite mutual PQC capability. To address this emerging threat, the authors propose a hybrid machine learning (ML)–based Intrusion Detection System (IDS) integrated with a PQC-ready security framework. Their work situates itself within the broader research domain that combines artificial intelligence with network security to detect sophisticated cyberattacks. Unlike traditional signature-based IDS solutions, which struggle to identify evolving cryptographic downgrade patterns, their approach leverages Deep Neural Networks (DNNs) and Decision Tree (DT) classifiers trained on flow-level features derived from network traffic. The study introduces a structured label-engineering pipeline that assigns PQC-likeness scores using handshake-derived attributes, enabling the classification of traffic into PQC, legacy, downgrade, and bot-related categories. This multi-class classification strategy enhances the detection granularity compared to binary benign/malicious models commonly seen in earlier IDS frameworks. The Decision Tree classifier demonstrates high accuracy in distinguishing benign from malicious traffic, while a class-weighted DNN improves detection sensitivity toward rare downgrade events an area often overlooked due to class imbalance issues. Experimental validation using CICIDS2018-derived traffic demonstrates test accuracy exceeding 98%, including strong performance in detecting downgrade attacks. The findings contribute to the literature by bridging PQC migration security with explainable, ML-driven intrusion detection, offering practical deployment guidance for integrating PQC-aware detection into real-world enterprise environments. Overall, the study advances existing research by combining deep learning–based intrusion detection with cryptographic modernization strategies, thereby addressing both detection accuracy and future-proof cryptographic resilience during the quantum transition era. **Advantages:** The proposed DNN-based IDS achieve over 98% accuracy, including strong detection of rare downgrade attacks, improving reliability in PQC migration environments. The framework supports seamless substitution of traditional algorithms (RSA, Ed25519) with PQC algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium) without redesigning the system, ensuring long-term quantum resilience. **Disadvantages:** The model is validated using CICIDS2018-derived traffic, which may not fully represent real-world PQC migration scenarios, potentially affecting generalization. The integration of DNN-based detection and cryptographic protection layers (AES-GCM, asymmetric encapsulation, digital signatures) may introduce processing latency and resource consumption in high-throughput networks.

Daniel Commey et al. (2026) [17] address the emerging security risks posed by quantum computing to Federated Learning (FL), particularly in privacy-sensitive domains such as healthcare. While FL enables decentralized model training without sharing raw data, its reliance on classical cryptographic mechanisms (e.g., ECDSA) makes it vulnerable to quantum attacks. To mitigate this risk, the authors propose PQS-BFL (Post-Quantum Secure Blockchain-based Federated Learning), a framework that integrates post-quantum cryptography (PQC) with blockchain-based verification to ensure long-term security and transparency. The framework employs ML-DSA-65, a FIPS 204 candidate algorithm formerly known as Dilithium, to authenticate model updates. Blockchain smart contracts are optimized for decentralized validation, ensuring integrity and non-repudiation of client contributions. Experimental evaluations on benchmark datasets such as MNIST, SVHN, and HAR demonstrate that PQS-BFL maintains competitive model performance, achieving over 98.8% accuracy on MNIST while preserving quantum-resistant security. Cryptographic operations remain efficient, with average signing and verification times below one millisecond. Although PQC introduces larger signature sizes (3309 bytes) and higher gas consumption compared to ECDSA, the study finds that PQC overhead accounts for only 0.01–0.02% of total blockchain transaction latency, indicating that network and consensus mechanisms dominate system delays. Furthermore, the framework exhibits favorable scalability, with training round times increasing sub-linearly as client numbers grow. The open-source implementation and reproducible benchmarks strengthen the study's contribution. Overall, PQS-BFL provides a practical and empirically validated roadmap for deploying quantum-resistant, blockchain-secured federated learning systems in critical infrastructure environments. **Advantages:** The integration of ML-DSA-65 ensures post-quantum resilience while maintaining sub-millisecond cryptographic operations and negligible impact on overall transaction latency. The framework preserves competitive model accuracy (e.g., >98.8% on MNIST) and demonstrates sub-linear scalability as client participation increases. **Disadvantages:** PQC signatures (3309 bytes) and higher blockchain gas consumption increase storage and transaction expenses compared to classical cryptographic methods. Although PQC overhead is minimal, overall system performance remains dependent on blockchain network latency and consensus mechanisms, which may limit real-time applications.

Ravi Kumar Inakoti et al. (2025) [18] explore the integration of Artificial Intelligence (AI) techniques into quantum cryptographic frameworks to address persistent challenges in secure quantum communication. Although quantum cryptography particularly Quantum Key Distribution (QKD) is recognized as a promising solution for next-generation secure communication, practical deployment remains constrained by high computational complexity, scalability limitations, quantum decoherence, and vulnerability to side-channel attacks. The authors argue that Machine Learning (ML) and Deep Learning (DL) can enhance the efficiency, adaptability, and robustness of quantum security mechanisms. The study proposes a hybrid AI-enabled architecture that incorporates multiple learning paradigms. Reinforcement Learning (RL) is utilized to optimize post-quantum cryptographic algorithm performance, while Generative Adversarial Networks (GANs) assess system robustness against adversarial threats. Federated Learning (FL) is introduced to improve scalability in distributed quantum key distribution environments. Additionally, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are employed for quantum authentication and secure key exchange, while Graph Neural Networks (GNNs) optimize network-level performance. Adversarial Machine Learning (AML) techniques are integrated to detect and mitigate runtime cyber threats. The framework also incorporates Quantum Neural Networks (QNNs) to reduce reliance on expensive quantum hardware, enhancing practical feasibility. Experimental results indicate that the AI-driven model improves computational efficiency and real-time threat resistance, achieving 93% accuracy and an F1-score of 0.98. However, the reported AUC score of 0.5 suggests limitations in multi-class discrimination, highlighting the need for improved dataset diversity and feature optimization. Overall, the study contributes a roadmap for AI-powered post-quantum security, emphasizing scalability, accessibility, and resilience for applications in financial systems, secure communications, and critical infrastructure protection. **Advantages:** The hybrid AI framework improves Quantum Key Distribution, authentication, and post-quantum resilience while addressing scalability challenges through Federated Learning. The incorporation of Quantum Neural Networks (QNNs) helps lower reliance on expensive specialized quantum infrastructure, increasing real-world applicability. **Disadvantages:** The reported AUC score (0.5) indicates challenges in multi-class classification performance, suggesting the need for better feature engineering and dataset expansion. The integration of multiple AI paradigms (RL, GANs, FL, CNNs, GNNs, QNNs, AML) increases architectural complexity and may introduce implementation and computational overhead challenges.

Sivasubramanian Ravisankar et al. (2025) [19] address critical limitations in the Internet of Medical Things (IoMT), where real-time analytics, long-term data security, and system scalability remain challenging. They propose Med-Q Ledger, a multi-layered architecture that combines a permissioned Hyperledger Fabric for transactional integrity with a scalable Holochain Distributed Hash Table to manage high-volume medical telemetry. This dual-ledger design enables horizontal scalability and achieves sub-second transaction finality, overcoming bottlenecks common in conventional blockchain-based healthcare systems. To ensure future-ready protection of sensitive medical records, the framework integrates post-quantum cryptography using CRYSTALS-Dilithium digital signatures and CRYSTALS-Kyber key encapsulation mechanisms. Privacy-preserving intelligence is delivered through an edge-based federated learning pipeline that employs lightweight autoencoders for anomaly detection while keeping data localized. For clinical validation, the system is applied to predicting intestinal complications such as necrotizing enterocolitis in preterm infants using multimodal physiological and imaging data. An integrated Random Forest model demonstrates strong predictive capability, translating raw IoMT streams into actionable medical insights. Performance evaluation reports ~3400 transactions per second with ~180 ms end-to-end latency, anomaly detection rates exceeding 95% with <2% false positives, and only ~11% computational overhead from post-quantum security on constrained devices. Clinical prediction achieves an F1-score of 0.90, contributing to a 25% reduction in emergency surgeries and 31% lower energy consumption compared to MQTT-based systems. Overall, the framework presents a practical blueprint balancing scalability, privacy, performance, and quantum-resilient security for next-generation healthcare IoT ecosystems. **Advantages:** Dual-ledger design enables thousands of TPS with low latency, suitable for large-scale medical telemetry. Integrates post-quantum cryptography and privacy-preserving federated learning for long-term data protection and ethical analytics. **Disadvantages:** Combining dual-ledger blockchain, PQC, and federated learning increases integration and deployment difficulty. Post-quantum cryptographic operations introduce additional computational load for constrained medical IoT hardware.

Soundes Marzougui et al. (2022) [20] investigate the security of lattice-based post-quantum signature schemes, focusing on BLISS and its constant-time implementation, GALACTICS. As quantum computing advances threaten conventional public-key cryptography, lattice-based schemes such as BLISS have emerged as promising post-quantum alternatives. However, their practical security depends not only on mathematical hardness but also on secure implementation. In particular, Gaussian sampling a core subroutine in BLISS has been identified as a critical vulnerability due to challenges in achieving both efficiency and resistance to physical side-channel attacks. The study presents three power side-channel key recovery attacks targeting GALACTICS, exploiting leakages in Gaussian sampling and related signing operations. Specifically, the attacks focus on cumulative distribution table (CDT) sampling, Bernoulli rejection, and sign-flip operations during signature generation. Using a profiling phase on an identical Cortex-M4 device, machine learning classifiers are trained to analyze power traces and predict sensitive internal variables with high accuracy. Experimental results demonstrate that leakage from Bernoulli rejection alone can enable secret key recovery using approximately 2000 signatures, while combining multiple leakage sources reduces this requirement to around 320 signatures. Importantly, the authors note that similar subroutines are used in other lattice-based schemes such as FALCON and FrodoKEM, suggesting broader vulnerability implications. As countermeasures, the paper proposes masking techniques for Gaussian sampling and sign-flip operations, including partial masking strategies to mitigate exploitable leakage. While promising, comprehensive evaluation of masking against machine learning-based side-channel attacks remains an open research area. Overall, the study highlights the critical importance of implementation-level security in post-quantum cryptographic schemes. **Advantages:** The study provides proof-of-concept attacks on actual hardware (Cortex-M4), demonstrating realistic risks in post-quantum implementations. The use of ML-based side-channel analysis offers a systematic and high-accuracy method for identifying exploitable implementation weaknesses. **Disadvantages:** The attacks require access to a similar device for training classifiers, which may limit feasibility in some real-world scenarios. While masking techniques are proposed, a full side-channel security evaluation of these defenses is not comprehensively validated.

B.S. Rocha et al. (2022) [21] investigate the feasibility of identifying post-quantum cryptographic (PQC) algorithms using machine learning techniques in a ciphertext-only scenario. As post-quantum algorithms advance through the NIST standardization process, understanding their distinguishability becomes important for cryptanalysis, digital forensics, and algorithm classification research. The study encodes plaintext files using four NIST PQC candidates FrodoKEM-1344, CRYSTALS-Kyber1024, NTRU-HRSS-701, and FireSaber in Electronic Codebook (ECB) mode. For comparison, classical algorithms such as AES and Blowfish are also included. The resulting ciphertexts are analyzed using the NIST Statistical Test Suite to generate metadata, which serve as input features for machine learning classifiers. Six data mining algorithms, along with an ensemble learning model named HLRNRF, are evaluated for their ability to identify the encryption algorithm. Experimental results demonstrate that identification accuracy significantly exceeds random guessing (16.67%), with hit rates ranging from 73% to 100% depending on ciphertext size and classifier type. The study finds that ciphertext file size influences classification performance, with ensemble learning achieving superior accuracy for 20KB and 100KB samples, while K-Nearest Neighbors (KNN) performs better for intermediate sizes (40KB–80KB). The findings highlight that even in ciphertext-only conditions, machine learning models can detect statistical patterns that differentiate cryptographic algorithms. While the work primarily focuses on ECB mode, the authors suggest future research into other modes such as CBC to further examine algorithm distinguishability. Overall, the study contributes to the intersection of machine learning and cryptographic analysis by demonstrating practical algorithm identification techniques for both classical and post-quantum schemes. **Advantages:** Demonstrates high accuracy (up to 100%) in distinguishing between classical and post-quantum algorithms using machine learning. It evaluates multiple classifiers and an ensemble model across varying ciphertext sizes, providing detailed performance insights. **Disadvantages:** The experiments focus only on ECB encryption mode, which may not reflect real-world secure encryption practices such as CBC or GCM. The identification approach relies on statistical metadata and controlled datasets, which may reduce effectiveness in more complex, real-world scenarios.

2.4. AI–Blockchain or Security Architecture Studies (Other Related Research Area)

Yazeed Yasin Ghadi et al. (2025) [22] present a systematic literature review (SLR) examining cybersecurity challenges in smart grids (SGs) and the role of blockchain (BC) and artificial intelligence (AI) in strengthening grid resilience. As smart grids integrate advanced communication networks, IoT devices, and real-time data exchange, they become increasingly vulnerable to sophisticated cyberattacks, particularly those targeting communication layers and control systems. The study categorizes smart grid attacks based on communication classes, including false data injection, topology manipulation, denial-of-service, and software-level exploits, highlighting the growing frequency and complexity of such threats. The review emphasizes the importance of AI-driven techniques such as anomaly detection, predictive analytics, and machine learning-based intrusion detection for identifying deceptive data injection and abnormal network behavior. These intelligent systems enhance proactive threat detection and automated response mechanisms. Concurrently, blockchain technology is explored as a decentralized trust framework capable of ensuring data integrity, secure energy trading, and tamper-proof logging of grid transactions. By combining AI's analytical intelligence with blockchain's transparency and immutability, the study proposes a synergistic defense architecture for smart grid protection. The authors identify ongoing challenges, including counterfeit topological data, imprecise data labeling, integration of big data analytics with blockchain, and the absence of standardized frameworks for AI–BC integration. Ethical considerations and regulatory aspects are also highlighted as areas requiring further exploration. Overall, the study provides a structured taxonomy of attacks and countermeasures while underscoring the transformative potential of AI and blockchain in enhancing smart grid cybersecurity. It establishes a foundation for future research aimed at building secure, adaptive, and resilient energy infrastructures. **Advantages:** Provides a structured categorization of smart grid cyberattacks and integrates AI and blockchain-based mitigation strategies. Demonstrates how combining AI-driven detection with blockchain-based integrity mechanisms enhances overall smart grid security. **Disadvantages:** The study lacks empirical performance validation of integrated AI–blockchain defense implementations. Absence of standardized frameworks and complexity in combining big data, AI, and blockchain may hinder practical deployment.

Gerardo Iovane et al., (2025) [23] propose modular, quantum-resilient security architecture for Internet of Things (IoT) ecosystems, addressing the limitations of traditional ECC-based and centralized security paradigms. As IoT deployments expand across industrial, healthcare, and automotive domains, conventional security frameworks struggle to ensure scalability, resilience, and preparedness against emerging quantum threats. The authors introduce an integrated framework combining quantum-inspired cryptography (QI), epistemic uncertainty reasoning, the multiscale blockchain MuReQua, and a decentralized storage engine (DeSSE) based on fragmented entropy storage. Each architectural layer addresses a specific vulnerability. Quantum-inspired cryptographic managers secure communication and authentication against quantum-capable adversaries. The epistemic reasoning layer enhances adaptive decision-making by allowing devices to assess trust probabilistically rather than through binary logic, improving responses in dynamic environments. MuReQua provides lightweight, adaptive consensus suitable for resource-constrained IoT systems, while DeSSE enhances fault tolerance and privacy through distributed entropy-based storage. Simulation-based evaluations demonstrate improvements in latency, decision accuracy, recoverable memory volume, and fault tolerance compared to conventional architectures. The modular design supports horizontal scalability and incremental deployment, allowing domain-specific customization without requiring complete system redesign. The framework also aligns with existing standards, supporting NIST-recommended cryptographic primitives and interoperability with platforms such as Hyperledger and distributed storage systems. However, the study acknowledges challenges including computational overhead in ultra-dense IoT environments, integration complexity, hardware constraints for post-quantum operations, and the need for broader empirical validation across heterogeneous devices. Overall, the work presents a forward-looking blueprint for decentralized, intelligent, and quantum-aware IoT security infrastructures. **Advantages:** Integrates quantum-inspired cryptography, adaptive reasoning, blockchain consensus, and decentralized storage, providing multi-layered resilience. The plug-and-play modular design enables incremental deployment and domain-specific adaptation across industrial, healthcare, and automotive IoT systems. **Disadvantages:** Quantum-inspired and epistemic reasoning modules may impose overhead unsuitable for ultra-resource-constrained IoT devices. The multi-layered architecture increases system integration complexity and requires extensive empirical validation before large-scale deployment.

Rami Almatarneh et al. (2025) [24] investigate security challenges emerging in Web 4.0 environments, which are characterized by decentralized architectures, AI-driven automation, real-time analytics, and IoT integration. The convergence of these technologies introduces complex attack vectors, including SQL injection (SQLi), adversarial model poisoning in federated learning systems, and IoT device spoofing. To address these threats, the authors propose a unified AI-blockchain security framework that integrates adaptive machine learning models with decentralized verification mechanisms. The framework incorporates bidirectional Long Short-Term Memory (BiLSTM) networks for detecting SQL injection attacks, achieving 96.2% accuracy and significantly outperforming traditional rule-based systems such as Snort. For adversarial model poisoning, the study applies Trimmed Mean aggregation combined with a dynamic reputation scoring system, reducing attack success rates from 78% to 12%. IoT spoofing detection is handled through Convolutional Neural Networks (CNNs) that analyze traffic embeddings using cosine similarity, attaining an F1-score of 91.3%. To ensure transparency and tamper resistance, the framework integrates a blockchain layer using Delegated Proof-of-Stake (DPoS) consensus (agreement), achieving 1,450 transactions per second with a validation latency of 220 milliseconds. The modular architecture allows deployment across decentralized finance (DeFi) platforms and IoT ecosystems. Additionally, user trust scores reportedly increased by 48% after implementation, highlighting practical applicability. Despite promising results, the study acknowledges limitations such as reliance on synthetic IoT datasets and a 15% latency overhead due to federated learning processes. Future work includes optimizing aggregation mechanisms, incorporating real-world datasets, exploring quantum-resistant hashing techniques, and validating performance in live production environments. **Advantages:** The framework simultaneously addresses SQLi, model poisoning, and IoT spoofing using specialized AI models integrated with blockchain verification. Achieves strong detection metrics (96.2% SQLi accuracy, 91.3% IoT F1-score) and high blockchain throughput (1,450 TPS), demonstrating scalability for Web 4.0 applications. **Disadvantages:** The system introduces approximately 15% additional latency, which may affect real-time applications. Use of synthetic datasets may limit generalizability and real-world validation of IoT spoofing detection performance.

Subhita Menon et al. (2025) [25] address the growing security challenges in smart home environments driven by the rapid expansion of Internet of Things (IoT) devices and their interconnected communication networks. As smart homes increasingly rely on real-time data exchange across heterogeneous devices, ensuring secure authentication, data integrity, and efficient communication becomes critical. The authors propose a hybrid architecture integrating blockchain, cloud computing, and artificial intelligence (AI) to create a secure and intelligent smart home communication framework. The proposed system introduces a learning engine that classifies network transactions into three categories: Smart T, Mod T, and Avoid T. A neural network-based training mechanism supports precise classification, while an enhanced Swarm Intelligence (SI)-based dragonfly algorithm optimizes sample selection for training. The blockchain layer provides secure user authentication and decentralized ledger generation, ensuring transparency and tamper resistance. Meanwhile, a cloud-based data evaluation layer ranks and processes transaction data to support informed decision-making within the network. Experimental evaluation demonstrates improved performance compared to existing methods such as Fused Real-Time Sequential Deep Extreme Learning Machine (RTS-DELM) and other blockchain-based AI techniques. The proposed model achieves a prediction accuracy of 96.54% for detecting false authentications, reduces computation complexity by approximately 10.14%, and lowers false authentication rates compared to prior works. Although performance gains slightly diminish with increasing test sample sizes, the architecture consistently outperforms baseline models. The study suggests potential integration with 5G and edge computing technologies to further enhance scalability and responsiveness. Overall, this work contributes a secure, AI-enhanced blockchain framework tailored for smart home IoT ecosystems. **Advantages:** Combines blockchain authentication, cloud-based evaluation, and neural network classification to enhance smart home communication security. Achieves 96.54% prediction accuracy with lower computation complexity and reduced false authentication rates compared to existing systems. **Disadvantages:** Performance improvement percentage decreases as the number of test samples increases, indicating potential scalability limitations. Reliance on cloud-based data evaluation may introduce latency, privacy concerns, or availability issues in real-world deployments.

Oleksandr Kuznetsov et al. (2024) [26] present a comprehensive survey examining the integration of Artificial Intelligence (AI) and Blockchain Technology (BCT) from a security-centric perspective. While both technologies have independently attracted significant research attention, the authors highlight a gap in systematic studies addressing their combined security implications. The survey analyzes how AI and blockchain can mutually reinforce each other to enhance transparency, automation, trust, and operational efficiency across diverse sectors such as finance, healthcare, supply chains, and public administration. The study identifies key security strengths arising from integration. Blockchain can enhance AI systems by ensuring data integrity, auditability, and decentralized trust management, while AI can improve blockchain efficiency through intelligent consensus optimization, anomaly detection, and smart contract auditing. However, the convergence of these technologies also introduces complex vulnerabilities. In AI systems, threats such as adversarial attacks, data poisoning, model bias, and privacy leakage remain significant concerns. In blockchain systems, challenges include smart contract vulnerabilities, key management risks, scalability limitations, and potential quantum threats to cryptographic primitives. When integrated, these risks may compound, amplifying attack surfaces and governance complexities. To address these challenges, the authors propose mitigation strategies including robust and explainable AI model design, improved blockchain consensus mechanisms, secure key management practices, and quantum-resistant cryptographic approaches. The survey also emphasizes the importance of adaptive regulatory frameworks that are technology-neutral, globally cooperative, and stakeholder-inclusive to maintain public trust. Overall, the paper contributes a structured overview of the security opportunities and risks in AI–blockchain convergence, offering guidance for policymakers, researchers, and practitioners navigating this evolving technological landscape. **Advantages:** Provides an integrated analysis of AI and blockchain security challenges and mitigation strategies, filling a research gap in combined technology assessment. It offers practical regulatory recommendations to support secure, ethical, and trustworthy AI–blockchain integration. **Disadvantages:** The study is primarily survey-based and lacks empirical validation or performance benchmarking of integrated frameworks. While covering many issues, the wide scope may limit detailed technical analysis of specific security mechanisms or implementation strategies.

Hamed Taherdoost et al. (2023) [27] present a critical review of the intersection between blockchain and machine learning (ML), focusing on their combined role in enhancing cybersecurity. While blockchain is widely recognized for its decentralized and immutable ledger structure, its built-in cryptographic protections do not guarantee comprehensive security, particularly at the application and integration layers. The study emphasizes that although blockchain provides strong data integrity and tamper resistance, additional components built on top of blockchain networks remain vulnerable to attacks. Consequently, the integration of ML techniques has emerged as a promising approach to strengthen blockchain-based systems. The review analyzes literature published between 2012 and 2022, identifying a significant rise in research activity after 2019. ML techniques have been applied to blockchain for anomaly detection, fraud detection, consensus optimization, and smart contract vulnerability analysis. The authors note that ML benefits from blockchain's decentralized data structure, which can enhance model robustness through distributed datasets. Conversely, blockchain systems can leverage ML for adaptive threat detection and improved network management. Despite the synergistic potential, the study highlights ongoing challenges, including scalability limitations, interoperability concerns, privacy issues, and susceptibility of ML models to adversarial attacks. Advances such as federated learning and zero-knowledge proofs are recognized as promising mechanisms to address privacy and trust concerns in integrated systems. The review concludes that while ML and blockchain together can significantly enhance security, further research is needed to improve scalability, privacy preservation, and cross-technology integration for real-world deployment across diverse industries. **Advantages:** Provides a structured assessment of how ML enhances blockchain security, identifying key trends and research gaps from 2012–2022. Highlights promising approaches such as federated learning and zero-knowledge proofs for privacy-preserving blockchain-ML integration. **Disadvantages:** The study is primarily survey-based and does not include empirical benchmarking of integrated ML-blockchain systems. Covers multiple domains and challenges but provides limited detailed analysis of specific implementation frameworks or performance metrics.

Summary of the Literature review,

Author et al., (Year)	Method / Technique	Key Findings	Pros	Cons
Noha El-Attar et al. (2025)	PSO + GA + XGBoost for Ethereum AML detection	99% accuracy after GA optimization	Large dataset validation; Optimized ML performance	Sensitive to noisy data; High GA computational cost
Er. Kritika et al. (2025)	Hybrid deep learning frameworks	Attention mechanisms for memory forensics ; Volatility framework	Hybrid deep learning frameworks (e.g., CNN-BiLSTM, ResNet-GRU) effectively detect known and novel ransomware	Scarcity of publicly available labeled ; affect model generalization and robustness.
Omar Dib et al. (2024)	Hybrid Ransomware Detection System using supervised ensembles (DT, RF, XGBoost, Stacking) + semi-supervised L-kmeans anomaly detection + Gradient Boosting feature engineering	Achieved superior ransomware detection on BitcoinHeist dataset; effectively classifies known families and detects unseen variants;	Detects both known and novel ransomware; Ensemble learning + feature engineering improves accuracy and robustness	Evaluated mainly on one dataset; High computational cost for large-scale blockchain deployment
Georgios Palaiokrassas et al. (2024)	Systematic Mapping Study of 159 papers on ML for blockchain analytics	Anomaly detection most studied use case (49.7%); Bitcoin & Ethereum dominate research;	Comprehensive structured review; Identifies research gaps, trends, scalability and cross-chain challenges	Limited dataset sharing reduces reproducibility; Over-focus on major blockchains limits generalization
Suliman Aladhadh et al. (2022)	BChainGuard (SVM/MLP on Ethereum)	98.02% accuracy with low gas overhead	Lightweight on-chain decision logic	Limited attack types; Only SVM/MLP tested
Shirisha N et al. (2026)	Lightweight lattice-based PQC for IoT (Contiki-NG, NS-3)	Acceptable latency (~120ms); Energy <4mJ	Sustainability & carbon analysis; IoT feasibility	72% communication overhead; Simulation-based validation
Abdullah Ayub Khan et al. (2025)	BDLT + PQC + ZKP for multimedia auditing	98% integrity accuracy; 92% privacy leakage reduction	Strong privacy protection; Quantum resistance	Scalability issues; Simulation-only results
Nalavala R. Reddy et al. (2025)	QuantumShield-BC (PQC + QKD + Q-BFT + QRNG)	>7000 TPS; Eliminates Sybil & MITM attacks	End-to-end quantum security; High throughput	QKD simulated; PQC computational cost
Velmurugan M et al. (2025)	PQ-PoETChain (NTRU + Adaptive PoET + LHV)	195 TPS; 91% energy reduction vs PoW	Energy efficient; O(1) validation	TEE dependency; No real-world adversarial testing
Filip Opiłka et al. (2024)	PQC Signature Benchmarking (Dilithium, Falcon, SPHINCS+)	Dilithium best overall; Falcon smallest signatures	Practical benchmarking; 5G/6G relevance	Only signature schemes evaluated; Limited side-channel discussion
Thanalakshmi et al. (2023)	PQ Signatures + IPFS integration	Reduced on-chain storage; Improved efficiency	NIST PQC integration; Storage optimization	Added architectural complexity; Limited Ethereum testing
Mudassir Peeran et al. (2026)	DNN + Decision Tree IDS with PQC-ready framework	>98% accuracy in detecting downgrade & malicious traffic	High detection accuracy; PQC migration support	Validated on CICIDS dataset only; Added computational overhead
Daniel Commey et al. (2026)	PQS-BFL (Blockchain + ML-DSA-65 + Federated Learning)	98.8% accuracy (MNIST); negligible PQC latency impact	Quantum-resilient FL; Sub-linear scalability	Large PQC signatures; Blockchain gas overhead
Ravi Kumar Inakoti et al. (2025)	Hybrid AI-enabled quantum security framework integrating RL, GANs, FL, CNNs, RNNs, GNNs, QNNs, AML	Improves quantum cryptographic efficiency and resilience; 93% accuracy and F1-score 0.98; enhanced real-time threat resistance	Enhances QKD and post-quantum resilience; Federated Learning improves scalability; QNN reduces hardware dependency	Low AUC (0.5) shows multi-class limitations; Highly complex multi-AI architecture with overhead
Sivasubramanian Ravisankar et al.	Dual-ledger IoMT architecture combining Hyperledger Fabric	Achieved ~3400 TPS with ~180 ms latency;	High scalability and low latency for medical	High architectural and integration

(2025)	+ Holochain DHT; Post-Quantum Cryptography (CRYSTALS-Dilithium & Kyber); Edge-based Federated Learning with autoencoders; Random Forest clinical prediction model	>95% anomaly detection with <2% false positives; PQC overhead ~11% on constrained devices; 0.90	telemetry; Quantum-resilient security with privacy-preserving real-time intelligence	complexity; Additional computational overhead for resource-constrained IoMT devices
B.S. Rocha et al. (2022)	ML-based PQC algorithm identification (ECB mode)	73–100% identification accuracy	High classification success; Ensemble evaluation	ECB-only; Controlled datasets
Soundes Marzougui et al. (2022)	ML-based side-channel attack on BLISS	Key recovery with ~320 signatures	Real hardware validation; Implementation-level insight	Requires profiling device; Masking not fully validated
Yazeed Yasin Ghadi et al. (2025)	AI + Blockchain hybrid smart grid defense	Structured attack taxonomy; AI anomaly detection	Comprehensive security mapping; Integrated defense	No empirical integrated testing; High integration complexity
Gerardo Iovane et al. (2025)	Modular quantum-resilient IoT security using Quantum-Inspired Cryptography + Epistemic Reasoning + MuReQua Blockchain + DeSSE storage	Improves latency, decision accuracy, memory recovery, and fault tolerance; supports scalable decentralized IoT security	Multi-layer resilience; Modular plug-and-play architecture; Domain customization possible	Overhead for ultra-constrained IoT devices; High integration complexity; Needs large-scale validation
Rami Almatarneh et al. (2025)	Unified AI-Blockchain security: BiLSTM (SQLi), Trimmed Mean FL defense, CNN IoT spoofing detection + DPoS blockchain	SQLi detection accuracy 96.2%; Poisoning attacks reduced from 78%→12%; IoT spoofing F1 91.3%; 1,450 TPS blockchain throughput	Multi-threat coverage; Strong detection metrics; High blockchain scalability; Improves user trust	~15% latency overhead; Synthetic datasets limit real-world validation
Oleksandr Kuznetsov et al. (2024)	Survey on AI–Blockchain security integration	Identified AI & blockchain mutual reinforcement	Structured integration analysis; Regulatory insight	No experimental validation; Broad scope
Hamed Taherdoost et al. (2023)	Critical Review of ML + Blockchain Security	ML enhances blockchain anomaly detection	Identifies research gaps; Privacy focus	Survey-only; No benchmarking

III. CONCLUSION

The convergence of Machine Learning, Artificial Intelligence (AI), Blockchain Technology, and Post-Quantum Cryptography (PQC) represents a transformative direction in next-generation cybersecurity research. As quantum computing advances threaten the integrity of classical cryptographic primitives such as RSA and ECC, the urgency to redesign secure digital infrastructures has become increasingly evident. This literature review examined recent contributions (2022–2026) that integrate Machine Learning-driven security mechanisms, quantum-resistant cryptographic algorithms, federated learning, decentralized storage, and adaptive consensus protocols to build resilient and scalable distributed systems. The surveyed studies demonstrate that hybrid Machine Learning–blockchain frameworks significantly enhance anomaly detection, ransomware classification, intrusion detection, and fraud analysis, often achieving accuracy levels exceeding 95–99%. Post-quantum signature schemes such as CRYSTALS-Dilithium, Falcon, NTRU, and Kyber-based key encapsulation mechanisms show promising performance with manageable computational overhead. Moreover, innovative consensus mechanisms, lightweight validation models, and decentralized federated learning architectures contribute to improved throughput, energy efficiency, and privacy preservation across IoT, smart grid, healthcare, and cloud environments.

Despite these advancements, several challenges persist. Many frameworks rely on simulated environments rather than large-scale adversarial deployments, limiting empirical generalization. PQC algorithms introduce increased signature sizes and communication overhead, potentially affecting scalability in resource-constrained systems. Integration complexity, Trusted Execution Environment (TEE) dependencies, dataset limitations, adversarial machine learning risks, and cross-chain interoperability issues remain open research problems. Additionally, sustainability considerations such as energy consumption and carbon footprint require deeper evaluation in quantum-safe deployments. Overall, the reviewed literature confirms that isolated security upgrades are insufficient; instead, a holistic, multi-layered approach combining intelligent detection, decentralized trust, and quantum-resistant cryptography is essential. Future research should focus on real-world validation, formal security proofs under quantum adversarial models and Machine learning, scalable and energy-efficient PQC optimization, standardized integration frameworks, and cross-domain interoperability.

IV.REFERENCES

[1]. Nachaat Mohamed,"Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms", Knowledge and Information Systems (2025) 67:6969–7055, https://doi.org/10.1007/s10115-025-02429-y.

[2]. Safak Kayikci and Taghi M. Khoshgoftaar," Blockchain meets machine learning: a survey", Kayikci and Khoshgoftaar Journal of Big Data (2024) 11:9, https://doi.org/10.1186/s40537-023-00852-y.

[3]. Yonas Teweldemedhin Gebrezgiher , Sekione Reward Jeremiah , Xianjun Deng and Jong Hyuk Park, "Machine Learning-Based Blockchain Technology for Secure V2X Communication: Open Challenges and Solutions", MDPI, Sensors 2025, 25, 4793. https://doi.org/10.3390/s25154793.

[4]. Noha E. El-Attar, Marwa H. Salama, Mohamed Abdelfattah and Sanaa Taha, " An Optimized Framework for Detecting Suspicious Accounts in the Ethereum Blockchain Network",MDPI, Cryptography 2025, 9, 63. https://doi.org/10.3390/cryptography9040063.

[5]. Er. Kritika, "A comprehensive literature review on ransomware detection using deep learning, Cyber Security and Applications", Volume 3, 2025, 100078, ISSN 2772-9184, https://doi.org/10.1016/j.csa.2024.100078.

[6]. Omar Dib, Zhenghan Nan, Jinkua Liu, "Machine learning-based ransomware classification of Bitcoin transactions", Journal of King Saud University - Computer and Information Sciences, Volume 36, Issue 1, 2024, 101925, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2024.101925.

[7]. Georgios Palaiokrassas, Sarah Bouraga, Leandros Tassiulas, "Machine Learning on Blockchain Data: A Systematic Mapping Study", arXiv e-prints, Art. no. arXiv:2403.17081, 2024. doi:10.48550/arXiv.2403.17081.

[8]. D. Saveetha, G. Maragatham, V. Ponnusamy and N. Zdravković, "An Integrated Federated Machine Learning and Blockchain Framework With Optimal Miner Selection for Reliable DDOS Attack Detection," in IEEE Access, vol. 12, pp. 127903-127915, 2024, doi: 10.1109/ACCESS.2024.3413076.

[9]. Suliman Aladhadh , Huda Alwabli, Tarek Moulahi and Muneerah Al Asqah," BChainGuard: A New Framework for Cyberthreats Detection in Blockchain Using Machine Learning," MDPI, Appl. Sci. 2022, 12, 12026. https://doi.org/10.3390/app122312026.

[10]. Shirisha, N., Manoj, H.M., Hussain, S.J. *et al,* " Post-quantum security framework for resource-constrained systems: emerging trends, challenges, sustainability, and future directions.", *Discov Computing* **29**, 85 (2026). https://doi.org/10.1007/s10791-026-09982-2.

[11]. Abdullah Ayub Khan, Asif Ali Laghari, Hamad Almansour, Leila Jamel, Fahima Hajjej, Vania V. Estrela, Mohamad Afendee Mohamed and Sajid Ullah," Quantum computing empowering blockchain technology with post quantum resistant cryptography for multimedia data privacy preservation in cloud-enabled public auditing platforms," *J Cloud Comp* **14**, 43 (2025), https://doi.org/10.1186/s13677-025-00771-8.

[12]. Nalavala Ramanjaneya Reddy, Supriya Suryadevara, K. Guru Raghavendra Reddy, Ramisetty Umamaheswari, Ramakrishna Guttula & Rajitha Kotoju, "Quantum secured blockchain framework for enhancing post quantum data security", Scientific Report 15, 31048 (2025). https://doi.org/10.1038/s41598-025-16315-8.

[13]. Velmurugan, M., Kumar, M.R, "A scalable post quantum secure blockchain framework with adaptive time consensus in cloud environments," Sci Rep 15, 45090 (2025). https://doi.org/10.1038/s41598-025-32745-w.

[14]. Filip Opiłka, Marcin Niemiec, Maria Gagliardi and Michail Alexandros Kourtis, "Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature", MDPI, Appl.Sci. 2024, 14, 4994. https://doi.org/10.3390/app14124994.

[15]. P. Thanalakshmi, A. Rishikhesh , Joel Marion Marceline , Gyanendra Prasad Joshi and Woong Cho, "A Quantum-Resistant Blockchain System: A Comparative Analysis", MDPI, Mathematics 2023, 11, 3947. https://doi.org/10.3390/math11183947.

[16]. Mudassir Peeran A, A.R. Mohamed Shanavas, "A Hybrid Post-Quantum Cryptography and Machine Learning and Framework for Intrusion Detection and Downgrade Attack Prevention throughout PQC Migration," The Scientific Temper (2026) Vol. 17 (1): 5402-5408 E-ISSN: 2231-6396, ISSN: 0976-8653, https://doi.org/10.58414/SCIENTIFICTEMPER.2026.17.01.01.

[17]. Daniel Commey, Garth V. Crosby, "PQS-BFL: A post-quantum secure blockchain-based federated learning framework, Expert Systems with Applications," Volume 312, 2026, 131449, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2026.131449.

[18]. Ravi Kumar Inakoti, Meka James Stephen, P.V.G.D.Prasad Reddy, "Enhancing Quantum Cryptography with Machine and Deep Learning a Hybrid Approach for Secure and Scalable Post-Quantum Security", Journal of Theoretical and Applied Information Technology, 15th June 2025. Vol.103. No.11, Little Lion Scientific ISSN: 1992-8645 ,pp -4972-4988.

[19]. Sivasubramanian Ravisankar and Rajagopal Maheswar," SecureEdge-MedChain: A Post-Quantum Blockchain and Federated Learning Framework for Real-Time Predictive Diagnostics in IoMT", MDPI, Sensors 2025, 25, 5988. https://doi.org/10.3390/s25195988.

[20]. B.S. Rocha, J. A. M. Xexeo and R. H. Torres (2022), "Post-quantum cryptographic algorithm identification using machine learning", Journal of Information Security and Cryptography (Enigma). 9. 1-8. 10.17648/jisc.v9i1.81.

[21]. Soundes Marzougui, Nils Wisiol, Patrick Gersch, Juliane Krämer, and Jean-Pierre Seifert. 2022, "Machine-Learning Side-Channel Attacks on the GALACTICS Constant-Time Implementation of BLISS. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)", Association for Computing Machinery, New York, NY, USA, Article 34, 1–11. https://doi.org/10.1145/3538969.3538980.

[22]. Yazeed Yasin Ghadi, Tehseen Mazhar, Tariq Shahzad, Ines Hilali Jaghdam, Sanwar khan, Muhammad Amir Khan& Habib Hamam, "A hybrid AI-Blockchain security framework for smart

grids", Scientific Report 15, 20882 (2025). https://doi.org/10.1038/s41598-025-05257-w.

[23]. Gerardo Iovane, "A Multi-Layer Quantum-Resilient IoT Security Architecture Integrating Uncertainty Reasoning, Relativistic Blockchain, and Decentralised Storage", MDPI, Appl. Sci. 2025, 15, 9218, https://doi.org/10.3390/app15169218.

[24]. Rami Almatarneh, Mohammad Aljaidi, Ayoub Alsarhan, Sami Aziz Alshammari, Fahd Alhamazani, Ahmed Badi Alshammari, "An integrated AI-blockchain framework for securing web applications, mitigating SQL injection, model poisoning, and IoT spoofing attacks", International Journal of Innovative Research and Scientific Studies, 8(3) 2025, pages: 2759-2773, ISSN: 2617-6548.

[25]. Subhita Menon , Divya Anand , Kavita , Sahil Verma , Manider Kaur , N. Z. Jhanjhi, Rania M. Ghoniem and Sayan Kumar Ray, "Blockchain and Machine Learning Inspired Secure Smart Home Communication Network", MDPI, Sensors 2023, 23, 6132. https://doi.org/10.3390/s23136132.

[26]. Oleksandr Kuznetsov , Paolo Sernani , Luca Romeo , Emanuele Frontoni And Adriano Mancini. "On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective about Security," in IEEE Access, vol. 12, pp. 3881-3897, 2024, doi: 10.1109/ACCESS.2023.3349019.

[27]. Hamed Taherdoost, "Blockchain and Machine Learning: A Critical Review on Security", MDPI, Information 2023, 14, 295, https://doi.org/10.3390/info14050295.

ABOUT THE AUTHORS

Ashok Raj R received his **MCA** Degree from Coimbatore Institute of Management and Technology affiliated to Bharathiar University, Coimbatore in the year 2000. He has received his **B.Sc.,(Computer Science)** Degree from Nehru Memorial College, affiliated to Bharathidasan University, Tiruchirappalli in the year1997. He has 26 Years of experience (10 Years in IT industry and 16 Years in Academics). He is pursuing his **Ph.D (Computer Science –Full-Time)** Degree at Sri Vijay Vidyalaya College of Arts and Science, Nallampalli, Dharmapuri, Tamil Nadu, India. His current research interests are Artificial Intelligence, Machine Learning, Quantum Computing and Block-Chain Technologies.

Dr.D.Maruthanayagam received his **Ph.D** Degree from Manonmaniam Sundaranar University, Tirunelveli in the year 2014. He received his **M.Phil** Degree from Bharathidasan University, Trichy in the year 2005. He received his **M.C.A** Degree from Madras University, Chennai in the year 2000. He is working as **Dean cum Professor**, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. He has above **25 years** of experience in the academic field. He has published **11 books**, more than **70 papers** in International Journals and **45 papers** in National & International Conferences so far. His areas of interest include Computer Networks, Grid Computing, Cloud Computing and Mobile Computing.