Secure and Scalable Financial Fraud Detection via Blockchain and Hybrid Cloud Technologies: A Systematic Review

KhushiPatel[1], Khyati Prajapati[2]

Master's In Computer Engineering / Sankalchand Patel University, Visnagar, India [1]
Assistant Professor, Department of Computer Engineering / Sankalchand Patel University, Visnagar, India [2]

khushi0812patel@gmail.com, kaprajapatice_spce@spu.ac.in

Abstract: The quick emergence and evolution of digital financial services have given rise to high-return crimes like credit card fraud, money laundering, and various scams through digital payments, which in turn have posed severe economic and security challenges. Traditional anti-fraud systems often struggle with scalability, flexibility, and response, rendering them ineffective in countering sophisticated cyber attacks. Recent advances in blockchain, hybrid cloud computing, and artificial intelligence (AI) provide promising directions for designing secure and scalable fraud detection frameworks. The blockchain provides secure and traceable transactions, and hybrid cloud systems facilitate rapid and flexible processing of substantial financial data. AI- driven models, incorporating methods such as federated learning and explainable AI, also enhance anomaly detection, data security, and interpretability in anti-fraud systems. This review synthesizes contributions, focusing on the merging of blockchain, hybrid cloud, and AI for the detection of financial fraud. Key approaches, advantages, limitations, and open challenges, such as interoperability, regulatory compliance, and scalability bottlenecks, are critically analyzed. The study also highlights future opportunities, including federated learning and quantum-ready architectures, to support secure, efficient, and trustworthy financial ecosystems.

Keywords: Financial Fraud Detection, Blockchain Technology, Hybrid Cloud Computing, Artificial Intelligence, Federated Learning, Explainable AI, Quantum-Inspired Security, Scalable Systems..

I. INTRODUCTION

The rapid digital transformation of financial services has revolutionized the way individuals and organizations conduct transactions. Online banking, mobile payments, and digital currencies have provided unparalleled convenience and speed; however, they have also introduced new risks, particularly in the realm of financial fraud. Cybercriminals increasingly exploit vulnerabilities in payment infrastructures, resulting in fraudulent activities such as credit card abuse, phishing, identity theft, and money laundering. The global impact of such activities is immense, with financial fraud losses estimated to be in the billions of dollars annually, posing serious threats to both customers and institutions [4,18].

Conventional fraud detection systems typically depend on centralized architectures and rule-based models. Systems capable of recognizing established deceit patterns typically achieve success, but they often encounter difficulties with scalability, adaptability, and responsiveness in rapidly changing environments [5,19]. The explosive growth of financial transactions, coupled with the sophistication of adversarial attacks, renders many traditional mechanisms inadequate. Moreover, centralized infrastructures suffer from single points of failure and heightened privacy concerns, which further limit their reliability in large-scale, digital-first ecosystems [2,6].

Emerging technologies such as blockchain, hybrid cloud computing, and artificial intelligence (AI) are increasingly seen as promising enablers for next-generation fraud detection frameworks. Blockchain introduces decentralization, immutability, and transparency into financial systems, enabling tamper-proof record-keeping and fostering enhanced trust among stakeholders

[10,13]. Hybrid cloud systems offer flexibility, scalability, and distributed data management, enabling monitoring of big transactions by combining the security of private clouds with the efficiency of public clouds [12,17]. Artificial intelligence and machine learning algorithms, particularly deep learning and federated learning models, provide advanced anomaly detection capabilities, allowing systems to detect novel fraud patterns without extensive manual intervention [20,38].

The convergence of blockchain, hybrid cloud, and AI has the potential to redefine financial fraud detection. For example, blockchain-enhanced federated learning frameworks preserve data privacy by enabling collaborative model training across institutions without exposing sensitive data, while hybrid cloud infrastructures ensure the computational scalability necessary for fraud detection [18,30]. Furthermore, explainable AI techniques are increasingly being integrated to improve interpretability, a critical requirement in financial decision-making processes where accountability and transparency are paramount [36,38].

Despite these advances, the integration of these technologies remains at a relatively early stage and faces significant challenges. Interoperability across blockchain platforms, compliance with diverse regulatory standards, and the high computational costs associated with AI training in distributed cloud environments are major hurdles [29,37]. Furthermore,whileblockchain, Given the increasing sophistication of fraudsters and the limitations of current systems, there is an urgent need for a systematic review of the latest advances in this area. Although several studies have individually examined blockchain, cloud computing, or AI-based fraud detection, few works provide a comprehensive synthesis of their combined application in financial systems [3,28]. This paper addresses this gap by analyzing and categorizing, offering an integrated perspective on secure and scalable fraud detection using blockchain and hybrid cloud technologies.

II. REVIEW METHODOLOGY

This study follows a systematic literature review (SLR) approach to examine recent research on secure and scalable real-time financial fraud detection using blockchain, hybrid cloud computing, and artificial intelligence. The methodology ensures transparency, rigor, and reproducibility in the review process.

Relevant studies were retrieved from established academic databases, including IEEE Xplore, SpringerLink, Elsevier Science Direct, Google Scholar, MDPI, and Wiley Online Library. The literature search employed combinations of keywords such as financial fraud detection, blockchain technology, hybrid cloud computing, artificial intelligence, federated learning, *and* privacy-preserving fraud detection.

Only peer-reviewed journal articles, conference papers, and high-quality review studies published between 2021 and 2025 were considered. Articles unrelated to financial systems, non- technical publications, and duplicate studies were excluded.

The selected literature was systematically analyzed and classified based on employed technologies; fraud detection approaches, scalability, privacy mechanisms, performance metrics, and reported limitations. This structured analysis facilitated a critical comparison of existing solutions and supported the identification of research gaps and emerging trends in financial fraud detection.

III. BACKGROUND AND FUNDAMENTALS

3.1 Financial Fraud Landscape

Financial systems have undergone significant digital transformation, which has greatly increased the scope and complexity of fraudulent activities. Common types of fraud include credit card fraud, phishing attacks, identity theft, money laundering, and synthetic account fraud, all of which exploit vulnerabilities in online banking, e-commerce, and digital payment infrastructures. These fraudulent schemes often utilize advanced technologies, such as malware, deepfakes, and Botnets, to bypass conventional detection mechanisms [4,18].

Globally, financial fraud results in billions of dollars in annual losses, undermining consumer trust and threatening economic stability. For example, credit card fraud has seen a sharp increase due to the rise of digital transactions and contactless payments, while money laundering exploits weak regulatory compliance across jurisdictions [6, 19]. The increasing reliance on cross-border transactions, coupled with high transaction volumes, amplifies the scale of risk and necessitates more intelligent and scalable detection systems [5,37].

Conventional fraud detection methods depend on rule-based frameworks and historical transaction analysis. While effective against previously observed fraud patterns, they fail against adaptive, evolving attacks that disguise themselves within legitimate transaction flows [2,29]. These limitations highlight the pressing need for scalable, and intelligent detection mechanisms capable of responding to evolving financial crime strategies.

3.2 Blockchain Overview

Blockchain technology has emerged as a critical enabler forsecure financial ecosystems. Its core features, decentralization, immutability, consensus-driven validation, and transparency make it suitable for building tamper-resistant systems [3,13]. In fraud detection, blockchain facilitates the reliable documentation of logs across, guaranteeing that no individual party can modify documents without notice [10,28].

The technology is broadly classified into public blockchains (e.g., Bitcoin, Ethereum) and permission blockchains (e.g., Hyperledger Fabric, Corda). In corporate settings, permission blockchains offer faster processing, enhanced privacy, and are more suitable for financial applications than public blockchains, which are hindered by slow processing speeds and scalability limitations, resulting in restricted open participation and transparency [12, 15].

Blockchain technology-enabled smart contracts can automatically verify transactions, thereby prevent deceit and facilitate secure collaboration with federated learning frameworks that ensure customer confidentiality and simplify data exchange between institutions, safeguarding sensitive customer data [18, 30]. These features make blockchain a robust foundation for secure and collaborative fraud detection ecosystems.

3.3 Hybrid Cloud Overview

Hybrid cloud computing combines public cloud scalability with private cloud security, offering a flexible infrastructure for handling large-scale, sensitive financial data. Public clouds provide flexibility and cost advantages, in contrast to private clouds, which ensure compliance with regulations, security, and management supervision. Meanwhile, hybrid cloud systems reconcile the conflicting requirements for speed, expandability, and security [12,17].

For fraud detection, hybrid clouds enable the processing of vast transactional datasets across distributed environments. Financial institutions can deploy machine learning models in the cloud for rapid fraud detection while maintaining sensitive data in private nodes to ensure compliance with regulations such as GDPR and PCI-DSS [15,19]. Moreover, hybrid cloud infrastructures support interoperability with blockchain networks, enhancing both transparency and trustworthiness [28,36].

The adoption of hybrid cloud in fraud detection also enables the deployment of federated learning models, where institutions collaboratively train algorithms without exposing raw data. This approach not only enhances privacy preservation but also improves fraud detection accuracy by leveraging cross-institutional knowledge [20,38]. Despite these advantages, hybrid clouds face challenges such as latency management, secure orchestration of resources, and protection against advanced cyber attacks, requiring continuous innovation in architecture and governance.

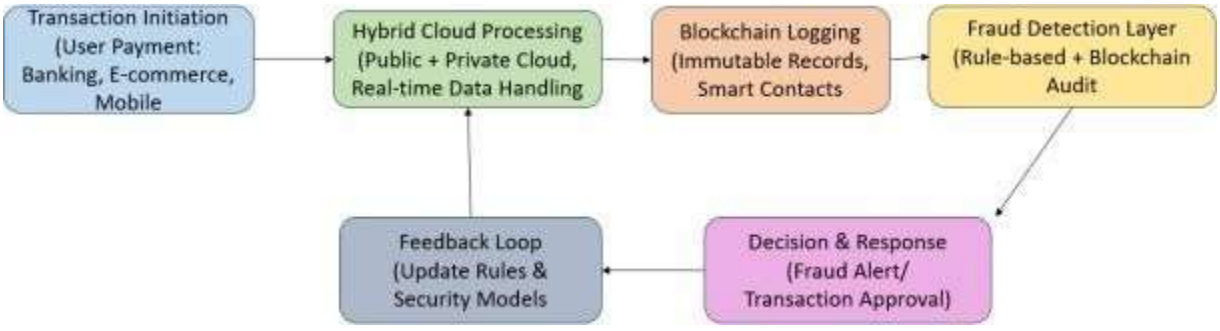

Fig.1.Work flow of Blockchain + Hybrid Cloud-Enabled Fraud Detection Lifecycle

IV. LITERATURE REVIEW

4.1 Real-World Implementations

Blockchain and hybrid cloud technologies have gradually moved from theory to practical deployments in financial fraud detection. Early studies focused on cloud-only models that leveraged machine learning for anomaly detection. For example, [2] proposed a cloud-based fraud detection framework using recurrent neural networks (RNNs) that demonstrated scalability in transaction monitoring. Building on this, [6] integrated long short-term memory (LSTM) networks with cloud infrastructure, enabling sequential modeling of transaction information.

Financial institutions find hybrid frameworks particularly appealing because they can effectively balance privacy and scalability. This approach was applied in [18] by utilizing blockchain-enhanced federated learning to detect credit card fraud across multiple banks, enabling data privacy while facilitating model updates. Similarly, [13] systematically reviewed blockchain-FL integration for cryptocurrency fraud detection, highlighting its potential for cross-exchange collaboration without direct data sharing.

Beyond prototypes, large-scale systems have been explored using big data platforms [27]. A PySpark-XGBoost pipeline demonstrates the possibility of processing extensive transaction data [29], integrating hybrid machine learning with blockchain auditing to enable scalable and comprehensible fraud analysis for digital transactions. While these implementations demonstrate real-world feasibility, most remain in pilot or experimental phases, and few have been validated under production-grade transaction volumes.

4.2 Challenges and Adoption Barriers

Despite the progress, significant challenges hinder the wide spread adoption of blockchain-cloud fraud detection systems. A primary limitation is scalability. Blockchain consensus mechanisms, while ensuring security and immutability, introduce latency that restricts processing [3,4].Hybrid cloud infrastructures offer elasticity but often struggle with network bottlenecks when handling high-volume, distributed fraud detection tasks [17,28].

Privacy and security risks also persist. While federated learning offers a mechanism for data sharing without exposing raw records, it introduces communication over heads and vulnerabilities to model inversion or poisoning attacks [13,23]. Similarly, storing sensitive metadata on public blockchains can conflict with privacy regulations, raising compliance concerns [12].

Interoperability between diverse systems poses another barrier. Financial institutions often operate across multiple cloud vendors and private infrastructures, and integrating these with blockchain platforms such as Hyperledger or Ethereum is still immature [15,28]. Furthermore, cross-border collaboration requires adherence to heterogeneous regulatory frameworks, complicating deployment.

Resource consumption is also a critical challenge. Big data-driven fraud detection frameworks, such as XGBoost and ensemble models, demand extensive computing power and incur high operational costs [27]. This establishes obstacles for small and medium-sized enterprises (SMEs) that have limited resources for large-scale deployments [36]. Finally, the lack of explain ability in deep learning-driven fraud detection models hinders regulator acceptance, as black-box systems conflict with accountability requirements [25].

4.3 Real-World Implementations

Blockchain and hybrid cloud technologies have gradually moved from theory to practical deployments in financial fraud detection. Early studies focused on cloud-only models that leveraged machine learning for anomaly detection. For example, [2] proposed a cloud-based fraud detection framework using recurrent neural networks (RNNs) that demonstrated scalability in transaction monitoring. Building on this, [6] integrated long short-term memory (LSTM) networks with cloud infrastructure, enabling sequential modeling of transaction information.

Financial institutions find hybrid frameworks particularly appealing because they can effectively balance privacy and scalability. This was applied in [18] by using blockchain-enhanced federated learning to detect credit card fraud across multiple banks, allowing for data privacy while model updates were shared. Similarly, [13] systematically reviewed blockchain-FL integration for cryptocurrency fraud detection, highlighting its potential for cross-exchange collaboration without direct data sharing.

Beyond prototypes, large-scale systems have been explored using big data platforms [27]. A PySpark-XGBoost pipeline demonstrates the possibility of processing extensive transaction data [29], integrating hybrid machine learning with blockchain auditing to enable scalable and comprehensible fraud analysis for digital transactions. While these implementations demonstrate real-world feasibility, most remain in pilot or experimental phases, and few have been validated under production-grade transaction volumes.

4.4 Integration with Emerging Technologies

To overcome these barriers, researchers are exploring integrations with advanced AI and cryptographic techniques. The integration of machine learning and blockchain technology improves process monitoring and predictive capabilities, as demonstrated by secure anomaly detection in machine learning-blockchain integration [4] and theoretical models that link blockchain and machine learning to prevent fraudulent transactions [11].

Federated learning with blockchain is a second direction, which tackles privacy concerns in collaborative fraud detection. Research has demonstrated in [18,13] that incorporating FL with blockchain provides data integrity, along with enhancements such as homomorphic encryption and secure aggregation, which have been implemented to mitigate risks [20, 24]. However, these solutions still struggle with communication costs and non-IID (non-independent and identically distributed) data challenges [23].

Complex relationships are being identified using graph neural networks to combat fraud rings, and studies have shown that incorporating quantum-inspired GNNs improves scalability, as seen in reference [32]. Studies have also been conducted by [31], and ongoing research is focused on speeding up federated learning through the development of quantum-enhanced models, as mentioned in [30]. Although promising, the sere mainataconceptualor early experimental stage. Another emerging direction is Explainable AI (XAI), which ensures compliance and interpretability in fraud detection [25]. Applied ensemble learning with XAI for blockchain-based fraud analytics [38]. Integrated XAI with federated learning for transparent decision-making.

Finally, studies are exploring edge-cloud integration for low-latency detection. The Peer study on blockchain - FL for industrial IoT suggests that extending hybrid cloud to the network edge could enable responses, a concept relevant for fraud detection in financial microtransactions.

4.5 Research Gaps and Trends

Despite these advances, several research gaps persist. First, few studies validate their systems at production scale, especially in financial ecosystems processing millions of daily transactions [19,27]. Second, blockchain throughput limitations and consensus overheads continue to hinder adoption unless hybrid anchoring techniques are applied [12,28]. Third, interoperability challenges between heterogeneous cloud providers and blockchain frameworks remain unresolved [15,28]. Fourth, while explainable AI methods are emerging, most are not tailored to regulatory audit standards, leaving compliance concerns unaddressed [25,38].

Another gap lies in the cross-border deployment of fraud detection systems, which requires standardized frameworks for compliance and collaboration across jurisdictions [13]. Current models are often region-specific, limiting global applicability. Finally, while quantum-enhanced and privacy-preserving approaches show promise, they are still in the exploratory phase, requiring further validation before deployment [30,32]

TABLE I:

COMPARISON OF EXISTING RESEARCH

Year	Model / Approach	Contribution	Strength	Limitation
2021[1]	Blockchain+ AI pipeline	Early blockchain-enabled frame work for secure Fraud detection	An integrity- and immutability-capable real-time detection systemwaslaunched.	Limited through put for large-scale data
2022[4]	ML+ Blockchain (Sensors)	Combinedsupervised ML with blockchain for auditability	Improved transparency and tamper-resistance	Poor scalability on-chain

2022[3]	Blockchainfor financial services	Comprehensive review of blockchain use cases in finance	Offers a classification of applications	Lacked a real-time fraud detection focus
2023[6]	LSTM+Cloud computing	Designed a scalable LSTM-based fraud detection	Effective for sequential transaction data	Evaluated only on small datasets
2023[9]	Blockchain+ AI(Fintech)	Dual approach to mitigate fintech fraud	Enhances resilience Via decentralization	Communication overhead in deployment
2024[13]	Blockchain+ Federated Learning	Systematic review for cryptocurrency fraud detection	Supports privacy-preserving training	FL aggregation faces challenges with non-independently and identically distributed data.
2024[18]	Blockchain+ FL for credit card fraud	Incentive-based FL mechanism	Encourages participation+ trust	High network communication cost
2025[27]	Big Data+ XG Boost+ Py Spark	Large-scale credit card fraud detection pipeline	Demonstrated scalability in the cloud	High resource consumption
2025[31]	GNN-based blockchain analysis	Dynamic feature fusion for fraud detection	Captures complex transaction graphs	Requires large labelled graph datasets

Although existing research demonstrates significant progress in financial fraud detection, each approach presents distinct strengths and limitations. Cloud-based machine learning models, such as Random Forest and XGBoost, as well as deep learning techniques like LSTM, achieve high detection accuracy and support real-time analysis. However, these centralized models raise concerns regarding data privacy and single-point failures.

Blockchain-based frameworks enhance transparency, immutability, and auditability of financial transactions, making them effective against data tampering and insider attacks. Nevertheless, blockchain systems often introduce latency and scalability constraints due to consensus mechanisms and on-chain processing.

Federated learning-based fraud detection addresses privacy concerns by enabling decentralized model training without sharing raw transaction data. Despite its advantages, federated learning suffers from communication overhead, slow convergence, and performance degradation in non-IID data environments.

Hybrid cloud architectures combine the security of private clouds with the scalability of public clouds, offering a balanced solution for large-scale fraud detection. However, such architectures increase system complexity and require careful orchestration and compliance management. These limitations indicate that no single approach is sufficient, motivating integrated frameworks that jointly address scalability, privacy, and real-time performance.

V. FUTURE SCOPE

While blockchain and hybrid cloud integration for financial fraud detection have advanced significantly, multiple avenues remain open for research and development. Future work can leverage the latest advances in scalable architectures, privacy-preserving learning, graph-based analytics, and explainability to build production-ready systems.

5.1 High-Performance and Scalable Frameworks

Current blockchain deployments in fraud detection still suffer from latency and throughput bottlenecks. Future systems should adopt big data-driven hybrid cloud pipelines (e.g., PySpark-XGBoost) that balance volume and velocity of financial transactions[27].Similarly, lightweight consensus mechanisms and hybrid anchoring approaches can reduce blockchain overhead while maintaining immutability [28,29].

5.2 Federated and Privacy-Preserving Learning

Privacy remains central to financial applications. Future research must extend federated learning with secure aggregation and homomorphic encryption, ensuring both compliance and resilience against poisoning or inversion attacks [30, 34]. Combining blockchain audit trails with quantum-enhanced FL offers a promising path toward higher accuracy and faster convergence under non-IID data distributions [40].

5.3 Graph-Aware and Specialized Models

Traditional anomaly detection struggles with coordinated fraud rings. Future work should explore graph neural networks (GNNs) and dynamic feature fusion to capture transaction relationships and evolving fraud strategies [31,32]. In parallel, mixture-of-experts architectures can provide specialization across transaction types, maintaining scalability while reducing false positives [35].

5.4 Explainability and Regulatory Compliance

For adoption in real-world finance, models must be transparent and auditable. Integrating explainable AI (XAI) with federated and blockchain frameworks can provide both interpretability and tamper-proof audit trails [38]. This will be crucial in meeting regulatory standards and building institutional trust.

5.5 Edge-Cloud Integration and Real-Time Inference

As financial transactions increasingly occur at the edge through mobile payments, IoT devices, and micro transactions, future systems should adopt edge cloud hybrid deployments. This would allow low-latency inference at the edge, with suspicious transactions escalated to cloud-scale models for deeper analysis [34].

5.6 Toward Production-Grade Deployments

Finally, future research must move beyond simulations and small pilots. Emphasis should be placed on stress-testing hybrid blockchain-cloud frameworks under realistic transaction loads, performing cross-institution validations, and conducting longitudinal evaluations that track system reliability and adaptability over time. Such steps are essential for bridging the gap between academic prototypes and industry-ready solutions.

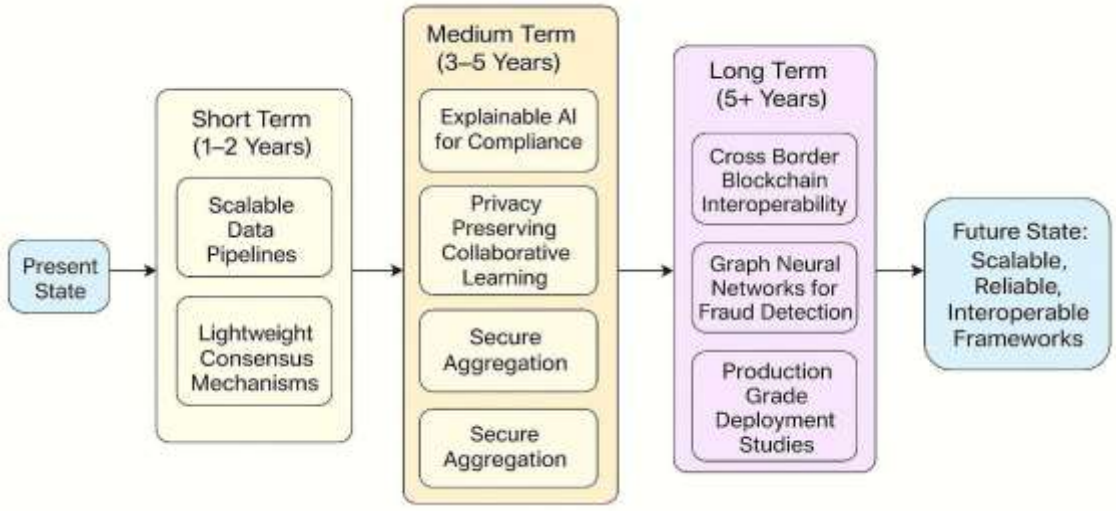

Fig.2. Future Research Road map for Blockchain–Hybrid Cloud Fraud Detection

VI. CONCLUSION

This review examined the function of blockchain and hybrid cloud technologies in enabling secure, scalable, and real-time financial fraud detection. Traditional approaches often face challenges of scalability, latency, and limited transparency, which are critical in high-volume financial systems. Blockchain provides immutability and decentralization to ensure trust, while hybrid cloud infrastructures deliver the computational elasticity required for real-time fraud detection at scale. The surveyed works demonstrate a clear shift from basic blockchain-enabled integrity checks toward integrated frameworks that combine machine learning, federated learning, and graph-based models with blockchain support. Hybrid cloud platforms further strengthen these systems by enabling containerized, high-throughput data pipelines. Together, these approaches reflect a growing movement toward multi-technology convergence to combat increasingly sophisticated fraud threats. Blockchain-federated learning frameworks face communication over head, graph neural networks require large labelled datasets, and big data pipe lines often demand high resource consumption. Most studies have also been validated only in controlled environments, limiting insights into real-world deployment.

REFERENCES

[1] H. Rehan, "Leveraging AI and Cloud Computing for Real-Time Fraud Detection in Financial Systems," Journal of Science & Technology, vol. 2, no. 5, pp. 127–134, 2021.

[2] V. R. Kumar, "Scalable Financial Fraud Detection System Employing Recurrent Neural Networks and Cloud Computing," IJERST, vol. 18, no. 3, pp. 36–42, 2022.

[3] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A Review of Blockchain Technology Applications for Financial Services," BenchCouncil Transactions, vol. 2, p. 100073, 2022.

[4] R. Ashfaq, et al., "An Efficient Machine Learning and Blockchain Mechanism for Financial Fraud Detection," Sensors, vol. 22, no. 19, p. 7162, 2022.

[5] J. Samuel, "Enhancing Financial Fraud Detection with AI and Cloud-Based Big Data Analytics: Security Implications," WJAETS, vol. 9, no. 2, pp. 417–434, 2023.

[6] S. Boyapati, C. Vasamsetty, R. P. Nippatla, et al., "Scalable Fraud Detection in Financial Transactions Using LSTM and Cloud Computing," Journal of Computer Science, vol. 11, no. 2, pp. 70–79, 2023.

[7] McCall, "Toward Intelligent Financial Security: Real-Time Fraud Detection via AI-Enabled Cloud Orchestration," Research, 2023. [Online]. H. Zhang, J. Hong, F. Dong, S. Drew, L. Xue, and J. Zhou, "A Privacy-Preserving Hybrid

[8] Federated Learning Framework for Financial Crime Detection," arXiv preprint, 2023.

[9] N. Kassetty, "Blockchain and AI in Fintech: A Dual Approach to Fraud Mitigation," Journal of Contemporary Management & Marketing, 2023.

[10] K. Lui, "Enhancing AI-Based Financial Fraud Detection with Blockchain Integration," IJHMP, 2023.

[11] H. O. Bello, et al., "Integrating Machine Learning and Blockchain: Conceptual Frameworks for Fraud Detection and Prevention," WJARR, vol. 23, no. 1, pp. 56–68, 2024.

[12] M. Malempati, "Leveraging Cloud Computing Architectures to Enhance Scalability and Security in Finance," EAJSE, vol. 1, no. 1, 2024.

[13] A. Ahmed and O. O. Alabi, "Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review," IEEE Access, vol. 12, 2024.

[14] J. K. R. Burugulla, "The Future of Digital Financial Security: Integrating AI, Cloud, and Big Data," MSW Management Journal, vol. 34, no. 2, pp. 711–730, 2024.

[15] U. Shankar and G. V. Radhakrishnan, "Cloud + Blockchain for Enhanced Financial Security," Library Progress International, vol. 44, no. 3, pp. 24752–24760, 2024.

[16] S. B. Masud, et al., "Blockchain + Machine Learning for Fraud Detection in Data Privacy and Security," Pakistan Journal of Life & Social Sciences, vol. 22, no. 2, 2024.

[17] D. V. Talati, "Scalable AI & Data Processing Strategies for Hybrid Cloud," WJARR, vol. 10, no. 3, pp. 482–492, 2024.

[18] T. Baabdullah, A. Alzahrani, D. B. Rawat, and C. Liu, "Federated Learning and Blockchain for Credit Card Fraud Detection," Future Internet, vol. 16, no. 6, p. 196, 2024.

[19] S. R. Subramaniam and R. Bandam, "AI-Powered Fraud Detection Across Hybrid Cloud," IJSRA, vol. 13, no. 1, pp. 3517–3528, 2024.

[20] MDPI, "Blockchain-Based Trusted Federated Learning with Pre-Trained Models," Electronics, vol. 12, no. 9, p. 2068, 2024.

[21] Wiley, "Federated Learning with Blockchain and Homomorphic Encryption," Wiley/Hindawi, 2024.

[22] ScienceDirect, "Privacy in Blockchain-FL Systems: Architectures, Attacks, Defences," Computer Communications, 2024.

[23] ScienceDirect, "CoPiFL: Collusion-Resistant FL Scheme Using Blockchain + HE," Applied Soft Computing, 2024.

[24] Frontiers, "FedNIC: Privacy-Preserving FL with Homomorphic Encryption," Frontier in Computer Science, 2024.

[25] S. S. Taher, et al., "Fraud Detection in Blockchain with Ensemble Learning + XAI," ETASR, 2024.

[26] A. A. Shakeabubakor, "Real-Time Fraud Detection with ML + Cloud Data Warehousing," IJISAE, 2024.

[27] L. Theodorakopoulos, et al., "Big Data-Driven ML for Scalable Credit Card Fraud Detection (PySpark, XGBoost)," Electronics, vol. 14, no. 1754, 2025.

[28] W. Ahmed, "Blockchain Integration in Modern Cloud Computing: A Survey," Premier JDS, vol. 2, p. 100003, 2025.

[29] S. Diyasi, A. Ghosh, and D. Dey, "Hybrid Machine Learning for Blockchain Fraud Detection," IJSSIC, vol. 2, no. 1, pp. 14–30, 2025.

[30] Sawaika, S. Krishna, T. Tomar, et al., "Privacy-Preserving Federated Framework with Quantum Learning," arXiv preprint, Jul. 2025.

[31] S. Zhang, L. Song, and Y. Wang, "Dynamic Feature Fusion for Blockchain Fraud Detection," arXiv preprint, Jan. 2025.

[32] L. D'Amico, et al., "Blockchain Network Analysis using Quantum-Inspired GNNs," arXiv preprint, Aug. 2025.

[33] H. Rahmati, "Federated Learning-Driven Cybersecurity Framework for IoT," arXiv preprint, 2025.

[34] Springer, "Blockchain + Federated Learning for Industrial IoT," Peer J Computer & Engineering, 2025.

[35] D. Vallarino, "Mixture-of-Experts Deep Learning for Fraud Detection," arXiv preprint, 2025.

[36] R. Seshakagari and A. Nathan, "AI-Augmented Fraud Detection for Digital Payments," IJCLI, 2025.

[37] G. Moura, et al., "AI in Financial Fraud Prevention: Bibliometric Study," JRFM, vol. 18, no. 6, p. 323, 2025.

[38] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Explainable AI + Federated Learning for Fraud Detection," JRFM, vol. 18, no. 4, p. 179, 2025.

[39] IEEE, "Secure Blockchain Architectures for Real-Time Transaction Processing," IEEEAccess, vol. 13, pp. 112345–112360, 2025. Springer, "Hybrid Cloud-Based Fraud Analytics with Blockchain Integration," Cluster Computing, 2025