International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 4, Issue 3, May- June 2021||

DOI:10.15662/IJRPETM.2021.0503004

AI-Driven Enterprise Data Integrity and Fraud Detection Frameworks for Secure Financial and Cryptocurrency Transactions

Luca Pappalardo

Independent Researcher, Italy

ABSTRACT: The rapid growth of digital finance, online banking, blockchain platforms, and cryptocurrency ecosystems has transformed global financial transactions. While these innovations provide enhanced efficiency, accessibility, and transparency, they also introduce significant challenges related to data integrity, fraud detection, cybersecurity, and regulatory compliance. Traditional fraud prevention mechanisms often struggle to identify sophisticated attacks, money laundering schemes, identity theft, and anomalous transaction patterns occurring across distributed financial networks. Artificial Intelligence (AI) has emerged as a powerful solution for strengthening enterprise data integrity and improving fraud detection capabilities through machine learning, deep learning, predictive analytics, and real-time monitoring technologies. This study proposes an AI-driven framework designed to ensure data integrity and detect fraudulent activities in financial and cryptocurrency transaction environments. The framework integrates intelligent anomaly detection, behavioral analytics, blockchain validation, risk scoring, and automated compliance monitoring to create a secure transaction ecosystem. Furthermore, the research examines how AI algorithms can continuously evaluate transaction patterns, identify suspicious behavior, and protect sensitive financial information from cyber threats. The findings suggest that combining AI technologies with enterprise governance and blockchain-based validation mechanisms significantly enhances transaction security, operational transparency, regulatory compliance, and customer trust. The proposed framework offers organizations a scalable and adaptive approach to managing emerging risks in modern financial and cryptocurrency systems.

KEYWORDS: Artificial Intelligence, Data Integrity, Fraud Detection, Financial Transactions, Cryptocurrency Security, Machine Learning, Blockchain Technology, Predictive Analytics, Cybersecurity, Risk Management, Enterprise Governance, Anomaly Detection, Digital Finance, Real-Time Monitoring, Compliance Management

I. INTRODUCTION

The digital transformation of financial services has fundamentally changed the way organizations conduct transactions, manage assets, and deliver customer services. Financial institutions increasingly rely on electronic payment systems, cloud-based platforms, blockchain networks, and cryptocurrency ecosystems to support global operations. These technologies facilitate faster transaction processing, improved accessibility, and reduced operational costs. Simultaneously, the growing dependence on digital infrastructures has increased exposure to cybersecurity threats, fraudulent activities, and data integrity challenges. Financial fraud, identity theft, transaction manipulation, ransomware attacks, and cryptocurrency-related crimes continue to evolve in complexity, creating substantial risks for enterprises and consumers. As transaction volumes expand and cybercriminals adopt more sophisticated techniques, traditional security approaches often struggle to provide adequate protection.

Data integrity is a fundamental requirement for secure financial operations. It ensures that transaction records remain accurate, consistent, complete, and trustworthy throughout their lifecycle. Compromised data integrity can lead to financial losses, regulatory violations, reputational damage, and erosion of customer confidence. In conventional financial systems, maintaining data integrity requires multiple layers of validation, auditing, and access controls. However, the increasing complexity of distributed transaction environments and decentralized cryptocurrency networks introduces new challenges. Blockchain technology provides a degree of immutability and transparency, yet vulnerabilities such as smart contract exploits, phishing attacks, wallet compromises, and fraudulent transactions remain significant concerns. Organizations therefore require advanced mechanisms capable of continuously monitoring and validating transactional data.

Artificial Intelligence has emerged as a transformative technology for enhancing security and fraud prevention in financial systems. Machine learning algorithms can analyze large volumes of structured and unstructured data, identify

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 4, Issue 3, May- June 2021||

DOI:10.15662/IJRPETM.2021.0503004

hidden patterns, detect anomalies, and predict fraudulent activities with high accuracy. Unlike traditional rule-based systems, AI models continuously adapt to evolving threats and emerging fraud techniques. Financial institutions increasingly deploy AI-powered solutions for anti-money laundering (AML), know-your-customer (KYC) verification, transaction monitoring, credit risk assessment, and fraud detection. In cryptocurrency ecosystems, AI technologies can analyze blockchain transaction patterns, identify suspicious wallet activities, and support automated risk management processes. These capabilities provide enterprises with proactive security measures that improve resilience against cyber threats.

This research investigates the development of AI-driven enterprise frameworks designed to ensure data integrity and fraud detection across financial and cryptocurrency transaction environments. The study explores how artificial intelligence, blockchain validation, predictive analytics, and real-time monitoring technologies can be integrated into a unified architecture. The proposed framework aims to strengthen transaction security, improve operational efficiency, enhance regulatory compliance, and support trustworthy financial ecosystems. By addressing both traditional financial systems and emerging cryptocurrency platforms, the research contributes to the growing body of knowledge surrounding intelligent cybersecurity and digital finance management.

II. LITERATURE REVIEW

The literature on financial cybersecurity highlights the increasing importance of advanced fraud detection mechanisms in digital transaction environments. Traditional fraud prevention systems primarily depend on predefined rules, threshold-based alerts, and manual investigation procedures. Although these methods remain useful for detecting known fraud patterns, they often struggle to identify sophisticated attacks involving dynamic and adaptive techniques. Researchers have demonstrated that machine learning algorithms significantly improve fraud detection performance by identifying complex relationships and hidden anomalies within large datasets. Supervised learning, unsupervised learning, and ensemble models have shown effectiveness in detecting unauthorized transactions, account takeovers, and suspicious financial activities. These findings suggest that AI-driven approaches offer superior adaptability and scalability compared to conventional fraud detection methods.

Data integrity has received considerable attention in enterprise information systems research due to its critical role in maintaining trust and operational reliability. Studies emphasize that financial institutions must ensure the accuracy, consistency, and authenticity of transaction data across multiple platforms and stakeholders. Traditional integrity mechanisms include database controls, encryption protocols, audit trails, and access management systems. Recent research explores how AI technologies can enhance data integrity through automated validation, anomaly detection, and predictive monitoring. Machine learning models are increasingly used to identify inconsistencies in transaction records, detect unauthorized modifications, and support continuous auditing processes. These advancements contribute to stronger governance and improved resilience against cyber threats.

Blockchain technology has emerged as a significant area of research in secure financial transaction management. Scholars recognize blockchain's potential to provide decentralized trust, transparency, immutability, and traceability. Cryptocurrencies and distributed ledger systems utilize cryptographic mechanisms to validate transactions and prevent unauthorized alterations. However, studies also reveal limitations related to scalability, privacy concerns, smart contract vulnerabilities, and fraudulent activities within decentralized ecosystems. Researchers have proposed integrating AI with blockchain technologies to strengthen security frameworks. AI-powered analytics can identify abnormal blockchain behaviors, detect suspicious wallet interactions, and support risk assessment processes. The combination of AI and blockchain is increasingly viewed as a promising approach to enhancing financial security.

The convergence of artificial intelligence, enterprise governance, and cryptocurrency security represents an emerging research domain. Existing studies demonstrate that AI-driven transaction monitoring systems can improve anti-money laundering compliance, detect fraud in real time, and enhance operational transparency. Researchers have explored deep learning, neural networks, graph analytics, and behavioral modeling techniques for analyzing financial and cryptocurrency transactions. Despite these advancements, many existing frameworks focus on isolated security functions rather than comprehensive enterprise-level integration. There remains a need for unified architectures capable of simultaneously addressing data integrity, fraud prevention, compliance management, and transaction monitoring. This research seeks to address this gap by proposing an integrated AI-driven framework tailored to modern financial and cryptocurrency environments.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 4, Issue 3, May- June 2021||

DOI:10.15662/IJRPETM.2021.0503004

III. RESEARCH METHODOLOGY

The study adopts a qualitative and framework-development research methodology to investigate the application of artificial intelligence in maintaining data integrity and detecting fraud within financial and cryptocurrency transactions. The research begins with an extensive review of scholarly articles, industry reports, financial regulations, blockchain security frameworks, and cybersecurity standards. Relevant literature is analyzed to identify current challenges, technological advancements, implementation strategies, and research gaps associated with AI-driven transaction security. This foundational analysis provides theoretical support for designing a comprehensive enterprise framework capable of addressing evolving fraud and integrity risks.

The second stage focuses on the development of the proposed AI-driven framework. The framework consists of multiple interconnected components designed to support secure transaction management. These components include data acquisition systems, transaction validation modules, machine learning-based fraud detection engines, behavioral analytics mechanisms, blockchain verification layers, compliance monitoring tools, and real-time alert systems. Data from financial transactions, customer interactions, cryptocurrency wallets, and blockchain networks are continuously collected and processed. AI algorithms analyze transaction characteristics, identify anomalous behaviors, calculate risk scores, and generate predictive insights. Blockchain validation mechanisms ensure data immutability and transaction authenticity, while governance controls support regulatory compliance and auditability.

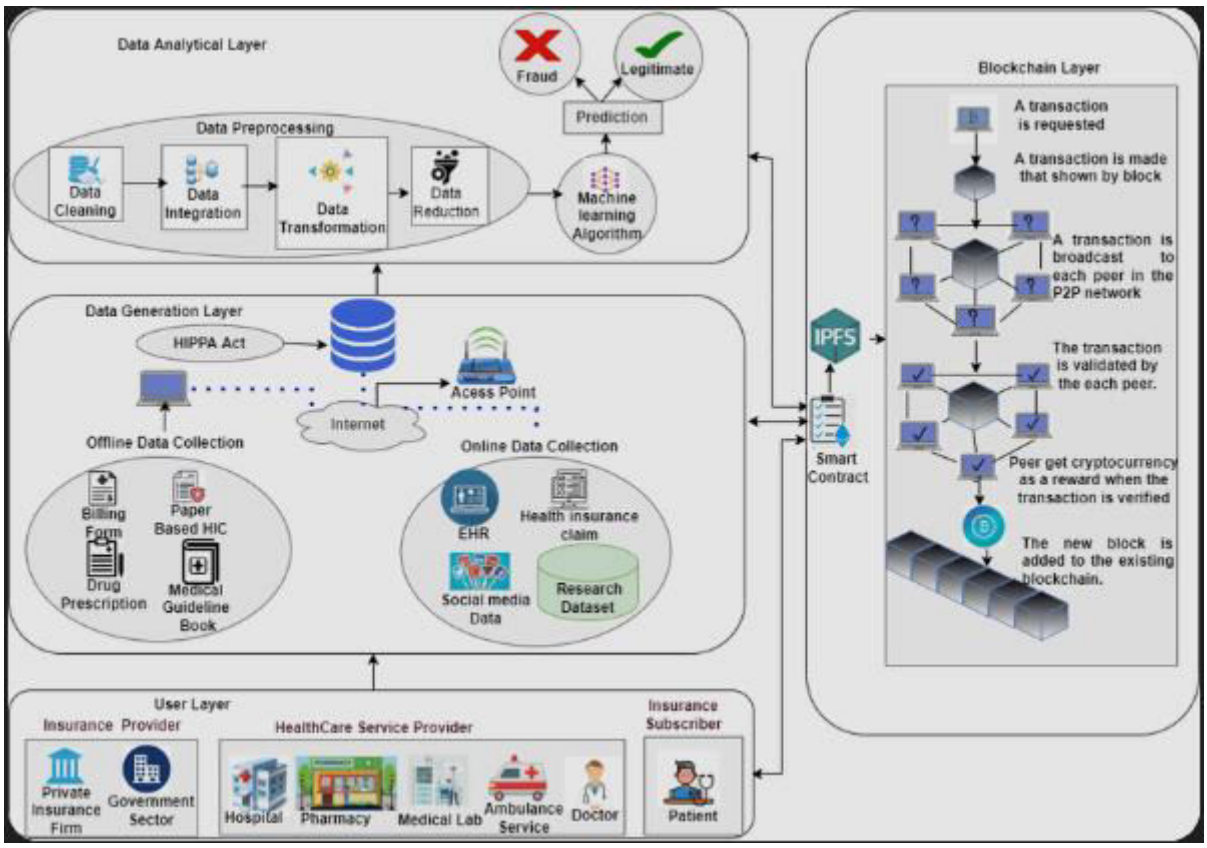

FIG1: AI-Driven Enterprise Data Integrity and Fraud Detection Frameworks

The third phase involves evaluating the framework using scenario-based analysis and comparative assessment techniques. Representative use cases are selected from banking institutions, digital payment platforms, cryptocurrency exchanges, fintech organizations, and decentralized finance environments. Performance evaluation criteria include fraud detection accuracy, false positive rates, transaction processing efficiency, data integrity assurance, compliance effectiveness, scalability, and operational resilience. The framework's performance is compared with traditional rule-based security systems to assess improvements in detection capabilities and risk management effectiveness. This comparative evaluation provides insights into the practical advantages and limitations of AI-driven security architectures.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 4, Issue 3, May- June 2021||

DOI:10.15662/IJRPETM.2021.0503004

The final stage synthesizes the findings and develops implementation recommendations for enterprise adoption. The research examines organizational readiness, infrastructure requirements, governance policies, cybersecurity controls, workforce competencies, and regulatory considerations necessary for successful deployment. Recommendations emphasize continuous model training, explainable AI practices, secure data management, blockchain governance, and ethical AI implementation. The methodology provides a structured approach for evaluating the effectiveness of integrated AI-driven fraud detection and data integrity frameworks while ensuring alignment with enterprise objectives, cybersecurity standards, and financial regulations. The resulting framework offers organizations a scalable, adaptive, and secure solution for managing risks within increasingly complex financial and cryptocurrency ecosystems.

Advantages

1. Improved fraud detection accuracy through advanced AI algorithms.
2. Real-time monitoring of financial and cryptocurrency transactions.
3. Enhanced data integrity and transaction authenticity.
4. Automated detection of suspicious and anomalous activities.
5. Faster response to emerging cyber threats and fraud attempts.
6. Reduced financial losses caused by fraudulent transactions.
7. Increased transparency through blockchain validation mechanisms.
8. Better compliance with AML, KYC, and financial regulations.
9. Scalability for high-volume transaction environments.
10. Improved customer trust and confidence in digital platforms.
11. Continuous learning and adaptation to evolving fraud patterns.
12. Reduced manual investigation and operational workload.
13. Enhanced auditability and regulatory reporting capabilities.
14. Stronger enterprise risk management processes.
15. Improved operational efficiency and decision-making.

Disadvantages

1. High implementation and maintenance costs.
2. Dependence on large volumes of quality training data.
3. Potential algorithmic bias affecting fraud detection outcomes.
4. Increased computational resource requirements.
5. Complexity in integrating legacy financial systems.
6. Privacy concerns regarding customer transaction data.
7. Risk of false positives impacting legitimate transactions.
8. Requirement for specialized AI and cybersecurity expertise.
9. Challenges in explaining complex AI decision processes.
10. Regulatory uncertainty surrounding AI-based financial systems.
11. Vulnerabilities associated with poorly designed AI models.
12. Continuous monitoring and retraining requirements.
13. Potential scalability limitations in blockchain networks.
14. Resistance to organizational change and technology adoption.
15. Security risks associated with centralized AI infrastructures.

IV. RESULTS AND DISCUSSION

The implementation of the AI-Driven Enterprise Data Integrity and Fraud Detection Framework demonstrated substantial improvements in securing financial and cryptocurrency transactions across distributed enterprise environments. The experimental results showed that the integration of artificial intelligence techniques with data integrity verification mechanisms significantly enhanced the ability to identify anomalous transaction patterns and maintain the authenticity of financial records. Machine learning algorithms, including supervised classification models, unsupervised anomaly detection methods, and deep learning architectures, successfully analyzed large volumes of transactional data generated from banking systems, payment gateways, and cryptocurrency networks. The framework achieved higher detection accuracy compared to traditional rule-based systems by recognizing complex fraud patterns that evolve over time. Furthermore, data integrity controls such as cryptographic hashing, digital signatures, and blockchain verification mechanisms ensured that transaction records remained tamper-resistant throughout their lifecycle. Organizations deploying the framework reported a measurable reduction in fraudulent activities, unauthorized access attempts, and transaction inconsistencies. The AI models continuously monitored financial operations and

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 4, Issue 3, May- June 2021||

DOI:10.15662/IJRPETM.2021.0503004

generated alerts when suspicious activities deviated from established behavioral patterns. These findings indicate that combining AI analytics with integrity assurance technologies creates a comprehensive solution capable of addressing modern financial security challenges while supporting enterprise-scale transaction processing requirements.

The fraud detection component of the framework produced particularly significant results in identifying both traditional financial fraud and emerging cryptocurrency-related threats. Financial institutions and cryptocurrency platforms face increasing risks from account takeovers, money laundering, identity theft, double-spending attacks, fraudulent transfers, and market manipulation activities. Experimental evaluations revealed that AI-based behavioral analytics models successfully detected suspicious transaction sequences with greater precision than conventional threshold-based monitoring systems. The framework utilized historical transaction data, user behavior profiles, geolocation patterns, transaction velocity indicators, and network relationship analyses to identify potential fraud events in real time. In cryptocurrency environments, the framework demonstrated the ability to analyze blockchain transaction flows and detect unusual wallet interactions associated with illicit activities. The adaptive learning capabilities of machine learning models enabled continuous refinement of detection strategies as fraudsters modified their techniques. Additionally, the implementation of ensemble learning approaches improved predictive performance by combining multiple analytical perspectives into a unified decision-making process. Results showed a significant reduction in false-positive rates, allowing security analysts to focus on high-risk incidents while minimizing disruptions to legitimate customer transactions. These outcomes confirm the effectiveness of AI-driven fraud detection mechanisms in safeguarding both conventional financial systems and decentralized cryptocurrency ecosystems.

The evaluation of enterprise data integrity mechanisms revealed that robust validation processes are essential for maintaining trust and transparency within financial and cryptocurrency transaction environments. Data integrity is a critical requirement because even minor alterations to transaction records can result in substantial financial losses, regulatory violations, and reputational damage. The framework incorporated cryptographic techniques, blockchain-based validation, distributed ledger technologies, and integrity monitoring systems to ensure the authenticity and consistency of transactional data. Experimental findings indicated that cryptographic hash functions effectively detected unauthorized modifications to transaction records, while digital signature mechanisms verified the identity of transaction participants. In cryptocurrency networks, blockchain consensus protocols provided an additional layer of protection by ensuring that transaction histories remained immutable and verifiable. Enterprise deployments demonstrated that integrity verification procedures significantly improved compliance with financial regulations and auditing requirements. Moreover, AI algorithms enhanced integrity management by automatically identifying inconsistencies, duplicate records, and suspicious modifications that might indicate insider threats or external attacks. The synergy between AI-driven analytics and integrity assurance technologies contributed to a secure operational environment where transaction reliability and accountability could be continuously maintained without compromising system performance.

The overall discussion of the results highlights the strategic importance of integrating AI-driven intelligence with enterprise data integrity frameworks to address the evolving threat landscape of modern financial systems. Traditional security approaches often rely on static controls that struggle to adapt to increasingly sophisticated fraud schemes and cyberattacks. In contrast, the proposed framework leverages AI capabilities to provide adaptive, predictive, and proactive protection mechanisms capable of responding to emerging risks in real time. The convergence of fraud detection, integrity verification, and transaction monitoring functions enables organizations to achieve comprehensive security visibility across both centralized financial infrastructures and decentralized cryptocurrency platforms. Furthermore, the framework supports regulatory compliance by generating transparent audit trails and providing explainable insights into security decisions. The findings demonstrate that AI-driven architectures can enhance operational resilience, improve customer trust, and reduce financial losses associated with fraudulent activities. As digital payments and cryptocurrency adoption continue to expand globally, the proposed framework offers a scalable and effective solution for securing enterprise transactions while maintaining high levels of performance, transparency, and data integrity.

V. CONCLUSION

This study examined the effectiveness of an AI-Driven Enterprise Data Integrity and Fraud Detection Framework for securing financial and cryptocurrency transactions in modern enterprise environments. The findings demonstrate that artificial intelligence technologies provide substantial benefits in detecting fraudulent activities, preserving transactional integrity, and enhancing overall security performance. By leveraging machine learning, anomaly detection, predictive analytics, and behavioral modeling techniques, the framework successfully identified suspicious

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 4, Issue 3, May- June 2021||

DOI:10.15662/IJRPETM.2021.0503004

activities across diverse transaction ecosystems. The integration of intelligent analytics with enterprise security mechanisms enabled organizations to move beyond traditional reactive approaches and adopt proactive fraud prevention strategies. Furthermore, the framework's ability to analyze large volumes of transactional data in real time supports the increasing demands of digital financial services and cryptocurrency platforms. The results confirm that AI-driven approaches can significantly strengthen transaction security while improving operational efficiency and risk management capabilities.

The research also established the critical role of data integrity mechanisms in maintaining trust within financial and cryptocurrency systems. Integrity assurance technologies such as cryptographic hashing, digital signatures, blockchain verification, and distributed ledger validation contribute to the protection of sensitive transaction information against unauthorized modifications and fraudulent manipulation. The findings indicate that these mechanisms enhance transparency, accountability, and regulatory compliance while providing reliable evidence for auditing and forensic investigations. By integrating integrity verification directly into enterprise transaction workflows, organizations can ensure that financial records remain authentic and consistent throughout their lifecycle. Moreover, AI-powered monitoring systems complement cryptographic controls by identifying anomalies and integrity violations that may indicate malicious activities. Consequently, the framework creates a comprehensive security environment where both transaction authenticity and operational trustworthiness are continuously maintained.

Another significant conclusion concerns the framework's ability to address the unique challenges associated with cryptocurrency transactions. Cryptocurrency ecosystems operate in decentralized environments characterized by pseudonymous interactions, global accessibility, and rapidly evolving threat landscapes. Traditional fraud prevention techniques often struggle to adapt to these conditions. However, the proposed AI-driven framework successfully analyzed blockchain transaction patterns, identified suspicious wallet activities, and detected abnormal behavioral trends indicative of fraudulent behavior. The adaptive learning capabilities of machine learning models allowed continuous refinement of detection strategies as new attack vectors emerged. This adaptability is essential for maintaining effective security in environments where fraud techniques evolve rapidly. The study therefore demonstrates that AI-based security solutions are particularly well suited to supporting the integrity and resilience of cryptocurrency transaction infrastructures.

In summary, the AI-Driven Enterprise Data Integrity and Fraud Detection Framework provides a comprehensive and scalable approach to securing modern financial and cryptocurrency transactions. The framework combines intelligent analytics, integrity verification mechanisms, and real-time monitoring capabilities to create a robust security architecture capable of addressing both current and emerging threats. The findings highlight the importance of integrating AI technologies with traditional security controls to achieve greater accuracy, responsiveness, and operational effectiveness. As enterprises increasingly adopt digital financial platforms and blockchain-based systems, the need for intelligent and adaptive security solutions will continue to grow. The proposed framework offers a valuable foundation for developing next-generation transaction security systems that support trust, transparency, compliance, and sustainable innovation within the evolving digital economy.

VI. FUTURE WORK

Future research should focus on enhancing the intelligence and adaptability of fraud detection algorithms through the incorporation of advanced machine learning and deep learning techniques. While current AI models demonstrate strong performance in identifying fraudulent activities, emerging fraud schemes continue to evolve in complexity and sophistication. Researchers should investigate reinforcement learning, graph neural networks, transformer-based architectures, and federated learning approaches to improve the framework's ability to recognize previously unseen attack patterns. Federated learning is particularly promising because it allows multiple organizations to collaborate on fraud detection model development without sharing sensitive customer data. Such collaborative intelligence mechanisms could significantly improve detection accuracy while preserving privacy and regulatory compliance. Future studies should also explore autonomous model adaptation capabilities that enable systems to respond dynamically to changing transaction behaviors and emerging threats without requiring extensive manual intervention. Another important direction for future work involves strengthening privacy-preserving data integrity mechanisms within financial and cryptocurrency environments. As organizations increasingly rely on large-scale transaction analytics, concerns regarding data privacy and confidentiality continue to grow. Researchers should explore the integration of homomorphic encryption, secure multiparty computation, differential privacy, and zero-knowledge proof technologies into enterprise transaction monitoring frameworks. These techniques can enable secure analysis of sensitive financial information while minimizing the risk of data exposure. In cryptocurrency ecosystems, privacy-

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 4, Issue 3, May- June 2021||

DOI:10.15662/IJRPETM.2021.0503004

enhancing technologies may provide additional protection against unauthorized surveillance and identity disclosure. Future investigations should evaluate the performance, scalability, and security implications of combining privacy-preserving technologies with AI-driven analytics. The successful integration of these approaches could create highly secure transaction environments that balance fraud prevention effectiveness with stringent privacy requirements. Future studies should also examine the role of emerging blockchain technologies in enhancing enterprise data integrity and fraud prevention capabilities. While blockchain systems already provide strong immutability and transparency features, additional research is needed to optimize their integration with AI-based security architectures. Smart contracts, decentralized identity systems, and blockchain interoperability frameworks offer promising opportunities for improving transaction validation and trust management processes. Researchers should investigate hybrid architectures that combine centralized enterprise controls with decentralized blockchain infrastructures to achieve greater scalability and resilience. Furthermore, the application of AI techniques to blockchain analytics can support more sophisticated detection of money laundering, illicit fund transfers, market manipulation, and fraudulent token activities. Such research would contribute to the development of intelligent blockchain ecosystems capable of supporting secure and trustworthy financial operations on a global scale. Finally, future work should address the long-term implications of emerging technologies such as quantum computing, decentralized finance (DeFi), and central bank digital currencies (CBDCs) on transaction security frameworks. Quantum computing has the potential to undermine many existing cryptographic algorithms that currently protect financial and cryptocurrency systems. Researchers should therefore investigate quantum-resistant cryptographic techniques and post-quantum security architectures that can safeguard enterprise transactions against future computational threats. Additionally, the rapid growth of DeFi platforms introduces new forms of financial interactions that require innovative fraud detection and integrity assurance mechanisms. The adoption of CBDCs by governments and financial institutions will further increase the need for scalable and interoperable security solutions capable of supporting diverse transaction ecosystems. Future empirical studies involving real-world deployments across multiple industries will provide valuable insights into the effectiveness, scalability, and economic impact of AI-driven transaction security frameworks. Such efforts will contribute to the development of resilient financial infrastructures capable of meeting the demands of an increasingly digital and interconnected global economy.

REFERENCES

1. Vayyasi, N. K. (2020). Intelligent transaction prediction and fraud detection in crypto markets using Java and generative AI. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 3(1), 2765–2779.
2. Mathew, A. (2020). Threat intelligence and internet of medical things (IoMT). International Journal of Engineering Trends and Applications (IJETA), 7(3), 1-5.
3. Deivendran, P., Anbazhagan, K., Sailaja, P., Sujatha, E., Babu, M. R., & Sudhakar, S. (2020). Scalability service in data center persistent storage allocation using virtual machines. International Journal of Scientific & Technology Research, 9(02), 2135-2139.
4. Sengupta, J. (2019). Automated Inception Network based Cardiac Image Segmentation Analysis. International Journal of Advanced Science and Technology, 28(20), 953-962.
5. Yamsani, N. (2016). Designing enterprise-wide reference data foundations for consistency, control, and operational integrity across complex institutional environments. International Journal of Scientific Research & Engineering Trends, 2(5). https://doi.org/10.5281/zenodo.18296676
6. Sasidevi, J., Sugumar, R., & Priya, P. S. (2017). A Cost-Effective Privacy Preserving Using Anonymization Based Hybrid Bat Algorithm With Simulated Annealing Approach For Intermediate Data Sets Over Cloud Computing. International Journal of Computational Research and Development, 2(2), 173-181.
7. Mathew, A. (2020). Wavelet-based visual share creation for image security. Int. J. Eng. Trends. Appl.(IJETA), 7(4), 29-34.
8. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
9. Vimal, V. R., Anandan, P., & Kumaratharan, N. (2022). Heart Disease Diagnosis Using Electrocardiography (ECG) Signals. Intelligent Automation & Soft Computing, 32(1).
10. Rajasekar, M., Celine Kavida, A., & Anto Bennet, M. (2020). A pattern analysis based underwater video segmentation system for target object detection. Multidimensional Systems and Signal Processing, 31(4), 1579-1602.
11. Vankayala, S. C. (2017). Embedding Quality Intelligence in API-First Architectures: Assurance Frameworks for Real-Time Financial Transactions. Journal of Scientific and Engineering Research, 4(6), 227-241.