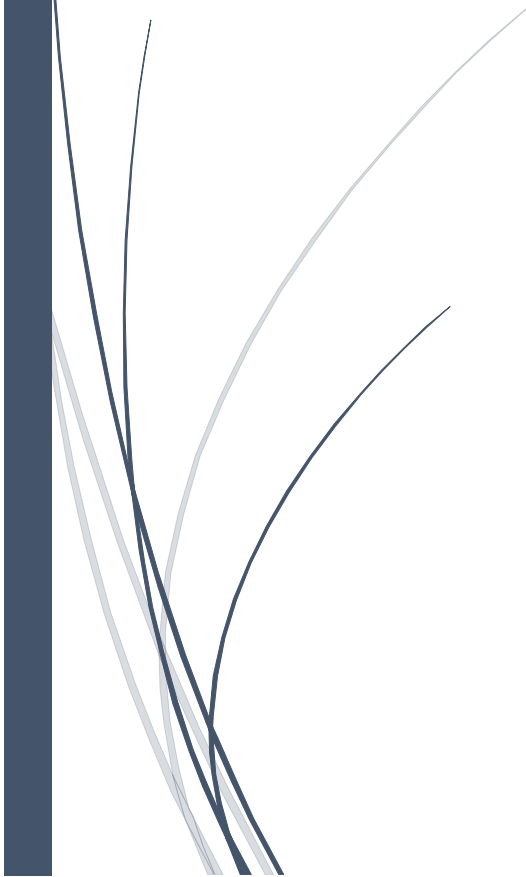


The logo for RADemics, featuring a dark blue vertical bar on the left and a blue arrow pointing right with the text "RADemics" inside.

RADemics

Blockchain and Artificial Intelligence Synergy for Secure Digital Transactions

An abstract graphic consisting of several thin, curved lines in dark blue and light grey, originating from the bottom left and extending upwards and to the right.

[Kavitha A Karkera, Jyoti Prasad Patra](#)
Nagarjuna Degree College, Nigam Institute of
Engineering and Technology NIET

Blockchain and Artificial Intelligence Synergy for Secure Digital Transactions

¹Kavitha A Karkera, Associate Professor, Dept of MBA, Nagarjuna Degree College, Bengaluru, Karnataka State, India. kavitaashwin@gmail.com

²Jyoti Prasad Patra, Principal, Nigam Institute of Engineering and Technology NIET, UG PG Diploma Engineering, Mundali, Cuttack Odisha India. jpp42003@yahoo.co.in

Abstract

Rapid digital transformation across financial, e-commerce, and decentralized platforms has amplified the need for secure, transparent, and resilient transaction systems. Conventional security mechanisms often fail to address sophisticated cyber threats, identity fraud, and evolving attack patterns, highlighting the necessity for integrated technological solutions. The convergence of Blockchain and Artificial Intelligence (AI) establishes a robust framework that combines immutable, decentralized ledger structures with adaptive, intelligent analytics. Blockchain ensures transactional integrity, data provenance, and decentralized trust, while AI facilitates real-time anomaly detection, predictive risk scoring, and automated decision-making. This synergy enhances digital identity management, strengthens access control, and mitigates fraud by enabling continuous monitoring, behavioral analysis, and transparent verification processes. Applications extend to secure payments, smart contracts, cross-border transactions, and decentralized finance ecosystems, demonstrating improved operational efficiency, scalability, and resilience. The chapter also explores privacy-preserving computation, federated learning, and explainable AI frameworks to ensure ethical and accountable deployment of intelligent transaction systems. By integrating structural security with predictive intelligence, Blockchain-aided AI frameworks establish a next-generation foundation for secure digital transactions, fostering trust, regulatory compliance, and systemic reliability across global digital networks.

Keywords: Blockchain, Artificial Intelligence, Digital Transactions, Fraud Detection, Secure Identity Management, Smart Contracts.

Introduction

The ongoing digital revolution has transformed transactional ecosystems across financial services, e-commerce platforms, healthcare networks, and decentralized governance systems [1]. Increasingly complex digital infrastructures handle massive volumes of data and transactions on a daily basis, requiring robust mechanisms to maintain security, transparency, and operational integrity [2]. Traditional centralized security systems are often inadequate, exposing platforms to vulnerabilities such as identity theft, transaction fraud, unauthorized data access, and system manipulation. The rise of sophisticated cyber threats, including coordinated multi-stage attacks and adaptive malware, further exacerbates these risks, highlighting the critical need for advanced technological solutions [3]. The integration of Blockchain and Artificial Intelligence (AI) represents a strategic approach to address these challenges. Blockchain provides immutable, distributed ledgers and decentralized consensus mechanisms, ensuring transaction integrity and

verifiability [4]. AI contributes intelligent data analysis, predictive modeling, and anomaly detection, enabling proactive identification of fraudulent or suspicious activities. The convergence of these technologies offers a multi-layered security architecture capable of adapting to dynamic threat landscapes while maintaining operational efficiency. By combining structural robustness with real-time intelligence, Blockchain-aided AI systems establish a foundation for secure digital transaction frameworks capable of supporting high-volume, decentralized environments without compromising trust or performance [5].

Digital transaction environments generate vast amounts of structured and unstructured data, including payment records, identity credentials, device information, and behavioral patterns [6]. The sheer scale and diversity of this data present significant challenges for maintaining secure interactions, particularly in distributed networks where single points of failure can compromise entire systems [7]. Traditional security mechanisms rely on static rules, predefined thresholds, and signature-based detection methods, which are often unable to identify novel attack vectors or subtle deviations in user behavior. The integration of AI into Blockchain-based infrastructures addresses these challenges by providing adaptive, learning-driven capabilities [8]. Machine learning models analyze historical and real-time transaction data, identifying anomalous patterns, suspicious activities, and potential fraud with increasing accuracy over time. Deep learning algorithms enhance the ability to detect multi-stage, coordinated attacks that span multiple nodes or platforms, while reinforcement learning optimizes automated decision-making processes for dynamic environments. In parallel, Blockchain ensures that all transaction records used for AI analysis remain tamper-proof, verifiable, and auditable [9]. This combination not only strengthens security but also enhances transparency, allowing stakeholders to trace every transaction through an immutable ledger while leveraging intelligent insights to mitigate risks proactively. The complementary capabilities of these technologies provide a resilient, adaptive framework for managing threats in high-volume, real-time digital ecosystems [10].