RADemics

Cloud-Based AI Solutions for Secure Payments and Banking Automation

Nabeena Ameen, S. Soorya

B. S. Abdur Rahman Crescent Institute of Science and Technology, Velalar College of Engineering and Technology

Cloud–Based AI Solutions for Secure Payments and Banking Automation

[1]Nabeena Ameen, Assistant Professor (Sel Gr), Information Technology, B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamilnadu, India. nabeena@crescent.education

[2]S. Soorya, Assistant Professor, Department of CSE (Artificial Intelligence and Machine Learning), Velalar College of Engineering and Technology, Erode, Tamil Nadu, India. sooryavcet5@gmail.com

Abstract

The accelerating digitization of financial services has transformed payment infrastructures into highly interconnected, data-intensive ecosystems that demand intelligent, scalable, and secure technological foundations. Cloud-based artificial intelligence solutions have emerged as a strategic enabler for modern banking, facilitating real-time fraud detection, adaptive risk assessment, automated compliance monitoring, and intelligent customer engagement. The convergence of distributed cloud architectures with advanced machine learning models enables high-performance processing of large-scale transactional data while ensuring elasticity, operational resilience, and cost efficiency.

This book chapter critically examines architectural frameworks, AI-driven fraud analytics, adversarial threat mitigation strategies, identity and access governance, and privacy-preserving computational models within secure payment environments. Emphasis is placed on the integration of explainable AI, zero trust security principles, and regulatory compliance mechanisms to address transparency, accountability, and data protection challenges in automated financial systems. The discussion further evaluates performance optimization, scalability strategies, and cybersecurity resilience in cloud-native banking infrastructures.

By synthesizing technological innovation with ethical governance and compliance considerations, this chapter provides a comprehensive roadmap for designing secure, intelligent, and sustainable digital banking ecosystems. The presented insights contribute to scholarly discourse and practical implementation strategies for next-generation financial automation within regulated cloud environments.

Keywords: Cloud Computing, Artificial Intelligence, Secure Payments, Fraud Detection, Zero Trust Security, Banking Automation

Introduction

The global financial ecosystem has undergone a profound transformation driven by rapid digitization, expansion of online payment channels, and growing reliance on data-centric decision-making frameworks [1]. Traditional banking infrastructures, originally designed around centralized processing and rigid legacy systems, encounter significant limitations in addressing

real-time transaction demands and evolving cybersecurity threats [2]. Digital wallets, mobile banking platforms, and cross-border payment systems generate high-velocity data streams that require scalable computational capabilities and adaptive analytics [3]. Cloud computing has emerged as a foundational technology that addresses these operational challenges through distributed architectures, elastic resource provisioning, and high-availability frameworks. Integration of artificial intelligence within these cloud environments further enhances analytical depth, enabling predictive modeling, dynamic risk assessment, and automated process optimization [4]. Financial institutions now operate within ecosystems where resilience, scalability, and intelligent automation define competitive advantage and regulatory compliance. This technological convergence reshapes core banking functions, redefines customer engagement models, and establishes a platform for secure digital transformation [5].

Artificial intelligence contributes significantly to modern payment ecosystems by transforming transactional data into actionable intelligence [6]. Advanced machine learning algorithms analyze patterns across millions of transactions to detect anomalies, predict fraudulent behavior, and evaluate credit risk in near real time [7]. Deep learning architectures process sequential transaction histories to identify subtle deviations that static rule-based systems fail to recognize. Cloud-based deployment of AI models ensures rapid scalability and centralized governance, allowing institutions to update detection mechanisms in response to emerging threat vectors [8]. Data lakes and distributed storage frameworks support continuous ingestion of structured and unstructured financial data, strengthening predictive accuracy [9]. This analytical capability enhances fraud prevention strategies while maintaining seamless customer experiences across digital channels. As transaction volumes expand globally, intelligent automation becomes indispensable for managing operational complexity and ensuring uninterrupted financial services [10].