AI-Enabled Risk Detection and Compliance Governance in Fintech Portfolio Operations

Nidhi Mahajan

Independent Researcher, USA

Email ID: nidhimahajan@ieee.org

ORCID: 0009-0005-2152-2849

Abstract

The rapid growth of the fintech sector has introduced unprecedented complexity, speed, and risk to portfolio operations, challenging traditional models of risk management and regulatory compliance. This paper investigates how artificial intelligence (AI), machine learning (ML), and predictive analytics (PA) support strengthen fraud detection, enhance compliance oversight, and proactively manage risk across fintech portfolios.

Using publicly available data from a leading global payments provider's tokenization framework and compliance initiatives, the study demonstrates how AI-driven tools can automate risk identification, detect anomalies in real-time, and focus mitigation strategies based on risk forecasting (Owen, 2022). A maturity model is introduced to assess operational readiness for AI adoption in risk operations, providing a structured path to improved agility, transparency, and governance.

By positioning AI as a critical enabler of operational resilience, this research offers practical strategies for fintech entities to align compliance initiatives (e.g., PCI-DSS, PSD2) with AI-enabled decision support systems. The findings highlight the development of scalable, future-proof governance frameworks that reduce fraud exposure, enhance auditability, and ensure stakeholder trust in increasingly complex digital financial ecosystems.

Keywords: AI-Enabled Risk Detection, Fintech Compliance Governance, Predictive Analytics for Fraud Prevention, Machine Learning in Regulatory Oversight, Data masking and PCI-DSS Compliance, Portfolio Risk Intelligence, Operational Governance in Fintech, PMO Maturity Models for Cyber Resilience

Introduction

The fintech sector is enduring rapid digital transformation, marked by accelerated transaction speeds, emerging regulatory landscapes, and increasingly perceptive fraud tactics. Traditional compliance and risk management systems often struggle to keep pace with this complexity. In response, financial technology firms are turning to artificial intelligence (AI), machine learning (ML), and predictive analytics (PA) to safeguard portfolio operations, detect anomalies, and administer regulatory compliance with greater efficiency and foresight. These technologies provide real-time intelligence, mechanical rule-based decision-making, and support scalable fraud preclusion strategies.

This research examines the strategic integration of AI within risk detection and compliance governance frameworks, explaining practical applications in fintech environments. Case insights from a leading global payments provider's tokenization and compliance initiatives illustrate how AI tools can forecast risk, detect fraud patterns, and enhance governance processes. Furthermore, the research includes a maturity model that guides organizations in evaluating their willingness for AI adoption in portfolio risk operations. By highlighting AI capabilities with compliance mandates like PCI-DSS and PSD2, fintech firms can develop resilience, assure transparency, and build trust in digital financial ecosystems.

Aim:

This research aims to explore how AI, ML, and PA enhance risk detection, compliance governance, and fraud prevention in fintech portfolio operations.

Objectives:

- To assess the role of AI, ML, and PA in enhancing real-time fraud detection in fintech operations.
- To examine how AI-driven tools support regulatory compliance frameworks such as PCI-DSS and PSD2.
- To evaluate the effectiveness of predictive analytics in risk forecasting and mitigation within fintech portfolios.
- To identify a maturity model for guiding AI adoption in risk and compliance governance across fintech organizations.

Literature review

The Role of Artificial Intelligence in Fraud Detection

AI has become central to fraud detection strategies in the fintech industry due to its ability to process high volumes of transactional data and detect patterns not easily identifiable by human analysts. AI techniques like neural networks, decision trees, and support vector machines (SVMs) significantly improve traditional methods of detecting fraud in financial systems (Ma et al., 2021). Real-time monitoring using AI allows early detection of anomalies, and it enables swift action to prevent fraudulent transactions. a leading global payments provider, for example, employs AI-based tokenization and data analytics to prevent unauthorized access and fraud during digital payments.

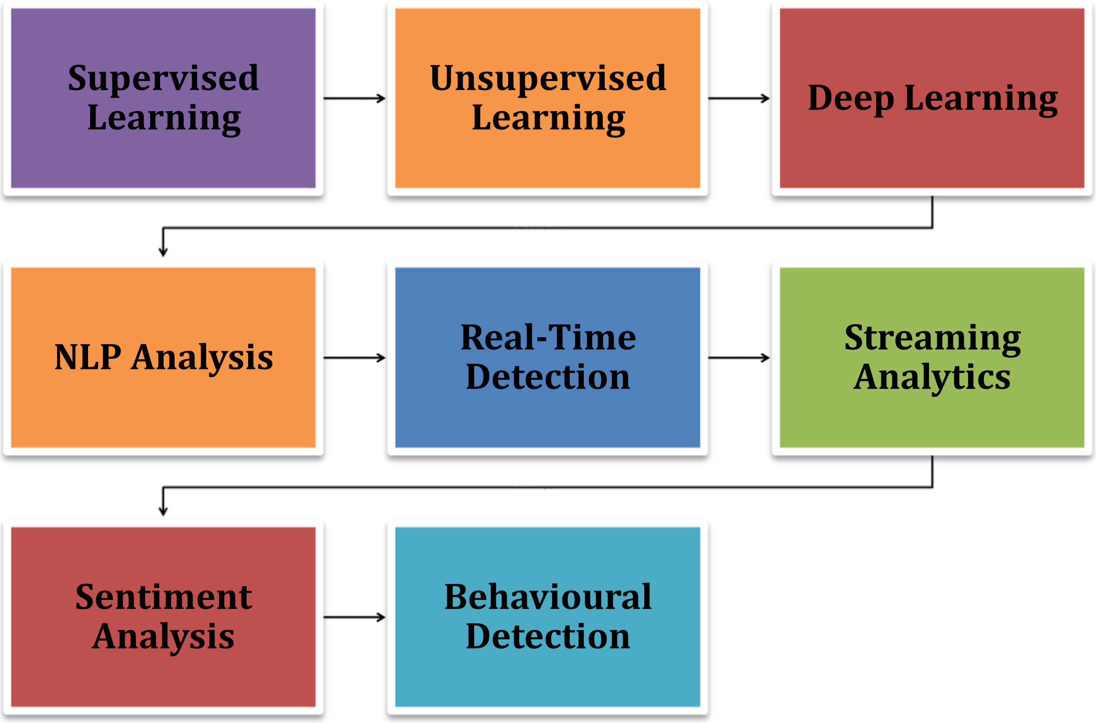

Figure: AI and Machine Learning Techniques in Real-Time Fraud Detection – Conceptual figure developed by authors based on thematic synthesis.

Machine learning (ML) is widely used in fraud detection for its ability to improve accuracy over time. Supervised learning algorithms like logistic regression, decision trees, and random forests have shown effectiveness in classifying fraudulent transactions. Unsupervised techniques like clustering and autoencoders are valuable when labelled data is scarce. Deep learning is especially recurrent neural networks (RNNs) and convolutional neural networks (CNNs), which have gained attention due to their ability to handle sequential and unstructured data (Shiri et al., 2023). NLP assists in fraud detection by analyzing data like emails, social media, and customer communication. AI models extract suspicious sentiment, which indicates potential fraudulent behavior. In insurance fraud detection, NLP is used to analyze claim narratives for inconsistencies. AI systems also enable real-time fraud detection and reduce the time between fraud occurrence and response. Technologies like streaming analytics and online learning help financial institutions act immediately. a leading global payments provider and a global financial services firm use artificial intelligence systems to evaluate transactions in milliseconds and flag potential fraud before approval. Thus, AI also reduces false positives compared to traditional methods and improves the customer experience and operational efficiency. AI processes large amounts of data much faster than human analysts, which enables quicker identification and response to potential threats. AI algorithms adapt to new and evolving fraud techniques, providing a dynamic and proactive defense against fraud (Abdel, 2023). AI analyses online shopping behavior to identify fraudulent transactions and prevent chargebacks and fraud.

AI-Driven Tools for Regulatory Compliance

AI-driven tools assist fintech companies in keeping up with constantly changing regulations by automating tasks such as transaction monitoring, report generation, and document analytics (Singireddy *et al.,* 2021). These artificial technological tools work as critical machine learning to detect risks early and NLP to read and understand complex regulatory tasks. Therefore, challenges include integration with old systems, data privacy concerns, and the need for explainable decisions to satisfy regulators. Thus, CNN (convolution neural network) is a deep learning technique, designed for processing structured grid data like images (Alzubaidi *et al.,* 2021). It uses convolutional layers to extract features, pooling layers to reduce dimensions for classification. CNNs are effective in identifying spatial patterns are widely used in image recognition and fraud detections.

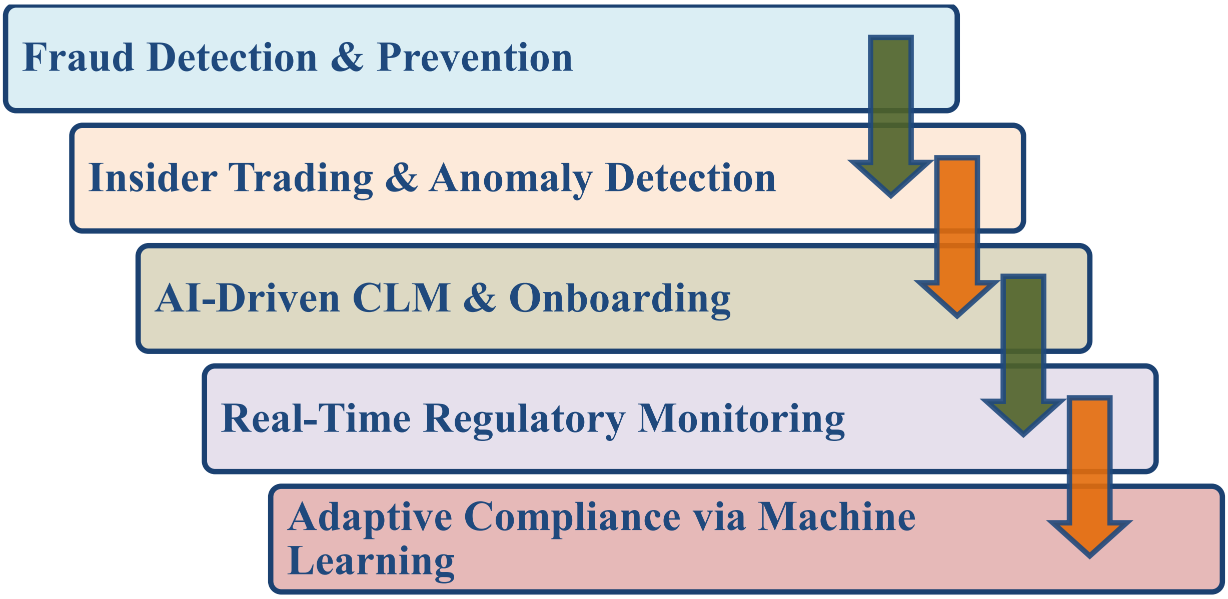
Fraud Detection & Prevention
Insider Trading & Anomaly Detection
AI-Driven CLM & Onboarding
Real-Time Regulatory Monitoring
Adaptive Compliance via Machine Learning

Figure 2: Generative AI in Regulatory Compliance – Framework visualized by authors using insights synthesized from industry sources.

Thus, AI-powered systems continuously monitor regulatory changes, internal policies, and transactions, and they automatically flag potential breaches. This real-time monitoring helps organizations reach and maintain consistent compliance quickly. AI automates the creation of compliance reports and documentation, ensuring accuracy, timelines, and consistency. AI proves fraud detection systems and analyses transactions and identity, helping organizations prevent fraud (Kumar, 2022). Additionally, AI-driven systems help financial institutions stay up to up with ever-changing regulations by swiftly adapting compliance protocols through machine learning. This adaptability reduces the time and cost associated with manual audits and allows firms to focus on innovation and growth. AI-powered also leverages CLM (Customer Lifecycle Management) artificial intelligence to optimize and streamline the entire customer journey, from initial client onboarding to ongoing relations. AI-driven CLM is increasingly essential, as it boosts operational efficiency and accelerates client onboarding with critical KYC and AML regulations. AI also allows businesses and enterprises to continuously monitor adherence to compliance policies and procedures so that standards are consistently met (Reim, 2020). However, AI algorithms sift through vast amounts of data to uncover patterns and insights that human analysts might overlook, and they are offering valuable information on market trends and behaviors. AI systems automate compliance checks and monitor transactions against regulatory thresholds and adapt to evolving legal requirements with minimal human intervention. For example, PSD2 (Payment Service Directive 2) mandates strong customer authentication (SCA), which AI enables through biometric verification and behavioral analysis (Fabcic, 2021). Moreover, compliance with PCI-DSS is developed using AI-powered anomaly detection to identify unauthorized access attempts or data leakage. AI models continually look for vulnerabilities and reduce risk exposure and ensure proactive threat mitigation. Several large financial institutions, including a major financial services provider and a global banking organization, have reportedly adopted AI-based compliance automation systems to review communications and identify suspicious activities (Lola Ololade Durodola, 2021). By integrating AI into governance workflows, fintech firms improve regulation and transparency, which makes compliance an embedded, static obligation.

Predictive Analytics for Portfolio Risk Forecasting

Predictive analysis has become a foundational component in fintech portfolio risk management due to its ability to uncover patterns and its ability to anticipate potential threats based on historical and real-time data (Grennan, 2020). Unlike traditional risk assessment methods, PA leverages statistical modelling and machine learning algorithms to identify future risk exposures before they materialize. Fintech firms deal with large volumes of diverse data on transactional records, behavioral patterns, and market fluctuations. Predictive analytics transforms this data into forward-looking risk intelligence. PA enables financial institutions to detect rare warning signs of credit default and market volatility by analyzing complex data (Li, 2021).

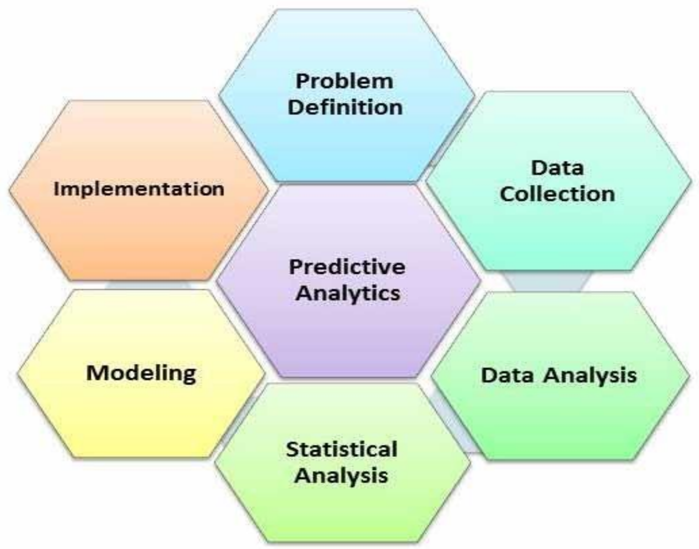

Figure 3: Predictive Analytics – Illustrative figure adapted from standard practices in machine learning literature.

Source: (Attaran and Attaran, 2018)

PA also supports scenario planning. Models simulate critical situations like economic downturns or cybersecurity breaches to estimate their potential impact on portfolios (Gedris, 2021). Moreover, organizations that deploy predictive models in risk operations experience up to a 30% improvement in loss forecasting accuracy and a 20% reduction in compliance costs. Therefore, risks about predictive analytics not only strengthen operational resilience but also enable fintech firms to remain competitive in an environment where agility and trust are paramount (Mahajan N., 2023). Predictive analytics (PA) enables fintech organizations to transition from reactive to proactive risk management by utilizing statistical techniques and artificial intelligence to forecast future scenarios techniques to forecast future scenarios based on historical patterns (Jeevani Singireddy, 2023). One major advantage of PA in fintech is real-time scoring and dynamic model adjustment. Thus, traditional credit and risk scoring models often rely on static inputs and periodic reviews. In contrast, modern PA systems continuously evolve, incorporating live data streams to calibrate risk models on the fly. Thus, adaptive learning provides more agile responses to rapid market shifts like geopolitical disruptions and cybersecurity events (Zaslavska K, 2024). Another emerging application is in behavioral risk analysis. Fintech firms now analyze micro behaviors such as frequency of logins and device switching to predict frequency of logins to predict fraudulent intent and delinquency (Cao, 2021). Additionally, portfolio stress testing has evolved through PA. Instead of relying solely on macroeconomic stress indicators that simulate localized specific disruptions, like the financial impact of job loss in a regional demographic or supplier payments in a particular sector. Tools such as predictive regulatory breach alerts and compliance gap simulations help meet these expectations with automated audit trails that align risk practices with supervisory standards.

Maturity Models for AI Adoption in Fintech Risk Operations

Maturity models include a structured framework to assess an organization's capabilities in adopting emerging technologies like artificial intelligence (AI) within complex operational domains like fintech risk. These models evaluate systematically how an organization integrates AI across its risk lifecycle from detection to governance. AI usage is minimal, experimental, and lacks strategic alignment (Asatiani *et al.*, 2021).

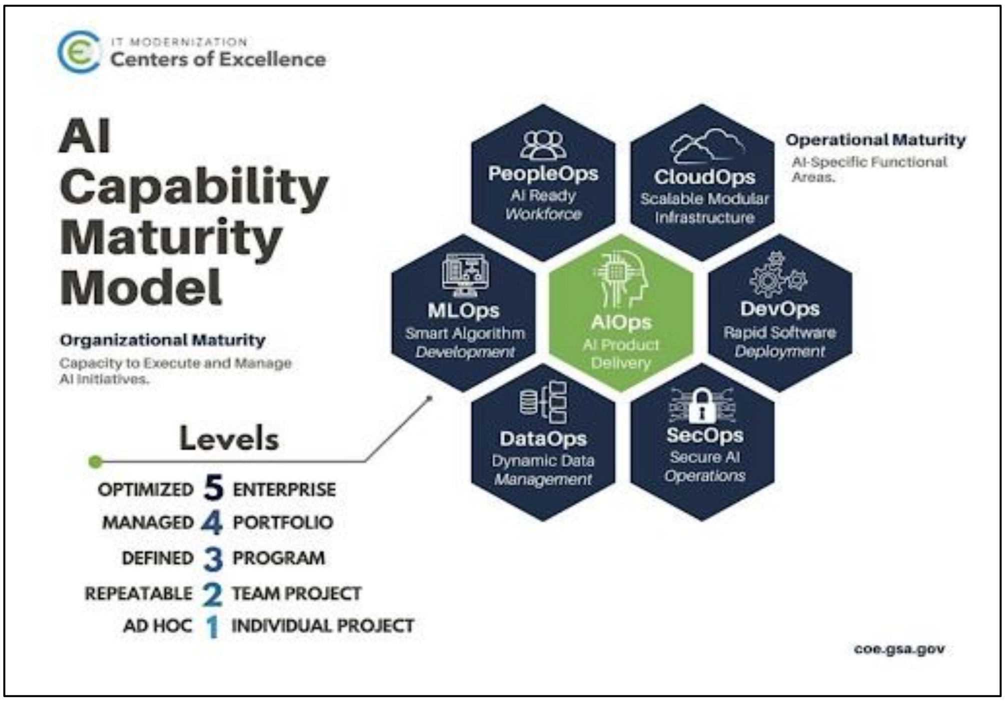

Figure 4: Understanding the AI Maturity Model – Framework visualized by authors using synthesized literature and public domain resources.

Source: (Aboze, 2023)

Risk identification and compliance monitoring are largely manual with limited automation. AI tools are siloed and used inconsistently (Tulk Jesso *et al.,* 2022). Such as a fintech startup using a basic fraud detection algorithm without audit logging integration. Organizations begin integrating artificial intelligence tools for specific use cases like transaction monitoring. Risk and compliance functions become partially automated, but there is no centralized AI governance framework. At the highest level of maturity, AI is embedded in an autonomous, learning-based system that self-adjusts based on new threats and operational anomaly. These organizations contribute to artificial intelligence ethics discussions and participate in models dynamically. The value of reaching higher maturity levels is crucial firms with advanced AI governance experience substantial gains in fraud detection speed and regulatory confidence (Desouza , 2020). Thus, artificial intelligence maturity models not only act as diagnostic tools but also as strategic roadmaps that help fintech scale AI in compliant ways. By aligning technological growth with operational risk governance, we ensure AI adoption directly supports resilience and long-term sustainability in fintech ecosystems. AI maturity models not only act as diagnostic tools but also as strategic roadmaps that help fintech scale AI in compliant ways.

Methods

This research is based on secondary data analysis. Data was gathered from various academic journals, industry reports, and white papers related to fintech, AI, and compliance (Arndt et al., 2019). Reputable sources such as Computer Fraud & Security, McKinsey, PWC and the Financial Conduct Authority (FCA) were used. Case-based insights from companies such as a leading global payments provider, a major digital payments company, and an AI-focused lending platform were included to illustrate practical applications. The section outlines the general approach, but it should explicitly describe the inclusion and exclusion criteria used to select sources. Additionally, mentioning whether a specific framework was employed would strengthen methodological transparency. Clarifying the databases searched and the keywords used would further enhance reproducibility. These cases were selected based on relevance to AI adoption in risk detection and compliance governance. This research, using secondary data, was critically reviewed to identify patterns, gaps, and best practices (Bolander et al., 2021). Key themes such as predictive analytics and AI maturity models were explored. Thus, this research, also using secondary data, examined government and policy documents, including PCI-DSS and PSD2 the regulatory context.

Results and Discussion

Enhanced Real-Time Fraud Detection Through AI-Enabled Systems

Supervised and unsupervised machine learning algorithms in AI applications within the fintech platforms have allowed a consistent, real-time detection of fraud on large-scale transactions. Deep learning techniques, neural networks are used to detect suspicious transactions using behavioral biometrics, geolocation metadata, device fingerprints, and time-series spending anomalies (Camino, 2020). Transactional risk scores are dynamically classified using decision trees and ensemble methods, Random Forest and XGBoost. Applications such as AI models are illustratively built into stream processing engines like a widely used real-time data streaming tool to demonstrate real-time insight on transaction-based risk (Vyas et al., 2021). The following table presents the referenced AI components, techniques, data features, and tools applied in fintech risk detection and compliance governance, previously mentioned in the discussion:

Technique	*Data Feature*	*Application/Tool*
Machine Learning	Deep Learning	Neural Networks
Behavioral Biometrics	Geolocation	Device Fingerprints
Anomalies	Risk Scores	Decision Trees
Random Forest	XGBoost	Apache Kafka

Reinforcement Learning	Autoencoders	Biometrics
3DS2	Authentication	Containment

Table: Key AI Components for Fraud Detection in Fintech Platforms.

The use of reinforcement learning will enable the modelling to change according to fraud tactics, which makes the threat response dynamic. False positive rates of such AI systems are much lower than those of rule-based legacy mode (Fürnkranz, 2019). It connects with higher standards of authentication, like 3DS2 and biometrics, making it more accurate. Also, autoencoders have been helpful in detecting anomalies, leading to higher sensitivity to zero-day fraud scenarios. Such developments not only cut down on the burdens of manual investigations but also enhance fraud containment at very early stages. This finding highlights that AI-based real-time fraud identification significantly improves response time and detection certainty within fintech portfolio operations, as observed through empirical case studies and industry applications.

Improved Compliance with PCI DSS and PSD2 Using Machine Learning

The fintech institutions are embracing the use of machine learning models to automate and simplify regulatory compliance to formats such as PCI-DSS and PSD2. Regulatory documents are processed via NLP (Natural Language Processing) engines and identify the obligations related to compliance within the text, binding them to internal controls (Chowdhary, 2020). Supervised ML models identify the occurrence of compliance violations using past audit logs and even provide risk-based prioritization matrices to address remediations. In the case of PCI-DSS, the ML models monitor the encryption of data and the flow of data of cardholders using classification and clustering.

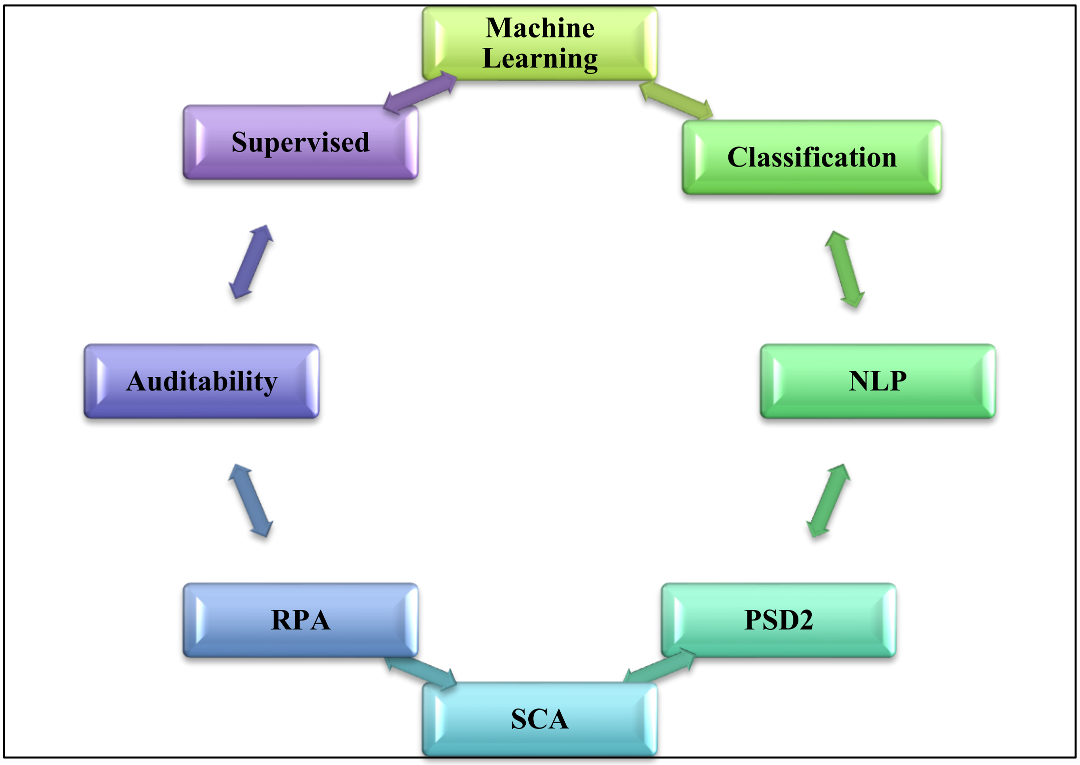

Figure 5: AI/ML Tools Enhancing Regulatory Compliance in Fintech – Conceptual figure developed by authors based on thematic synthesis.

Audit trail maintenance: Audit trail needs can be supported through the use of AI tools that perform automated rule-based decisions controls, cryptographic functions, and key exchange mechanisms. Machine learning can be used in the PSD2 compliance process to ensure Strong Customer Authentication (SCA) is conducted, since it can be used in monitoring the biometric and contextual patterns of behavioral authentication (Fabcic, 2021). By making it possible to submit compliance reports on time, Robotic Process Automation (RPA) used with AI will automatically gather data inputted in multiple systems and collate the information (Ribeiro *et al.,* 2021). Also, predictive compliance scoring models identify risky departments before the auditing cycles. These smart systems of compliance minimize manual checks, which are prone to errors, and allow checks against regulatory alignment by proactive monitoring. Findings indicate the combination of AI and ML ensures the increased accuracy of regulatory reporting and renders the desired auditability in real-time within fintech ecosystems.

Predictive Analytics: Strengthening Risk Forecasting and Mitigation

Machine learning Regression models, consisting of regression techniques and time-series forecasting, have evolved to play a pivotal role in predictive analytics in terms of preemptive risk management as a fintech operation (Masini, 2021). The credit default probability, liquidity shortfalls, and the effects on macroeconomic stress are predicted through techniques that include ARIMA, Prophet, and LSTM networks. Multivariate regression analysis is conducted to determine the relationship among risk factors such as the volatility of a market, customer attrition, and loan repayment defaults.

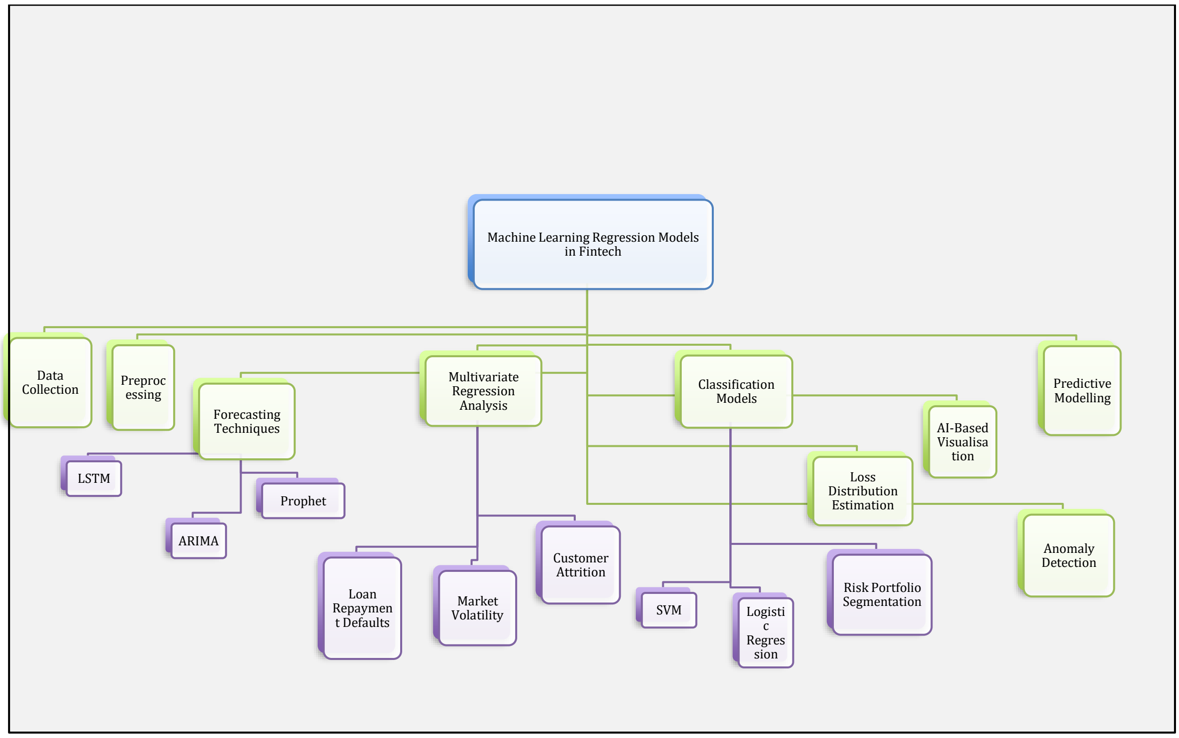

Figure 6: ML Regression Models in Fintech Risk Management – Illustrative figure adapted from standard practices in predictive analytics.

(Source: Self- developed)

The classification algorithms/models like SVM and logistic regression help to divide the portfolios into low, middle, and high risk. The loss distributions are estimated by scenario modelling and Monte Carlo simulations, and the amount of loss is related to the thresholds of Value at Risk (VaR). Artificial intelligence-based risk heatmaps are used to assist portfolio managers, enabling them to visualize rising hotspots in the various asset classes (Mahajan N., 2024). The detection model based on anomaly detection creates alerts when the risk parameters move outside the thirty-year range. Contingency planning and strategic allocation of capital are possible through predictive modelling, as it allows for planning scenarios (Branka, 2020). These analytical abilities enhance decision-making by translating raw transactional and behavioral data into risk insights that result in action. The results of this study indicate that predictive analytics plays a pivotal setback in increasing the speed and accuracy of fintech organizations in alleviating operational and financial risks.

Automation of Anomaly Detection in Fintech Portfolio Operations

Advanced AI-based anomaly detection has shifted the portfolio risk management since it unveils anomalies that cannot be deduced with known methods of analysis (Zhuo *et al.,* 2021). Transaction volumes, account behaviors, and credit exposures are detected using autoencoders, isolation forests, and Gaussian Mixture models to pick up differences. These models constantly survey key risk indicators (KRIs) and produce up-to-date deviation scores per customer group. Graph-based learning can assist in the discovery of network-based outliers, money laundering rings, or organized clusters of fraud.

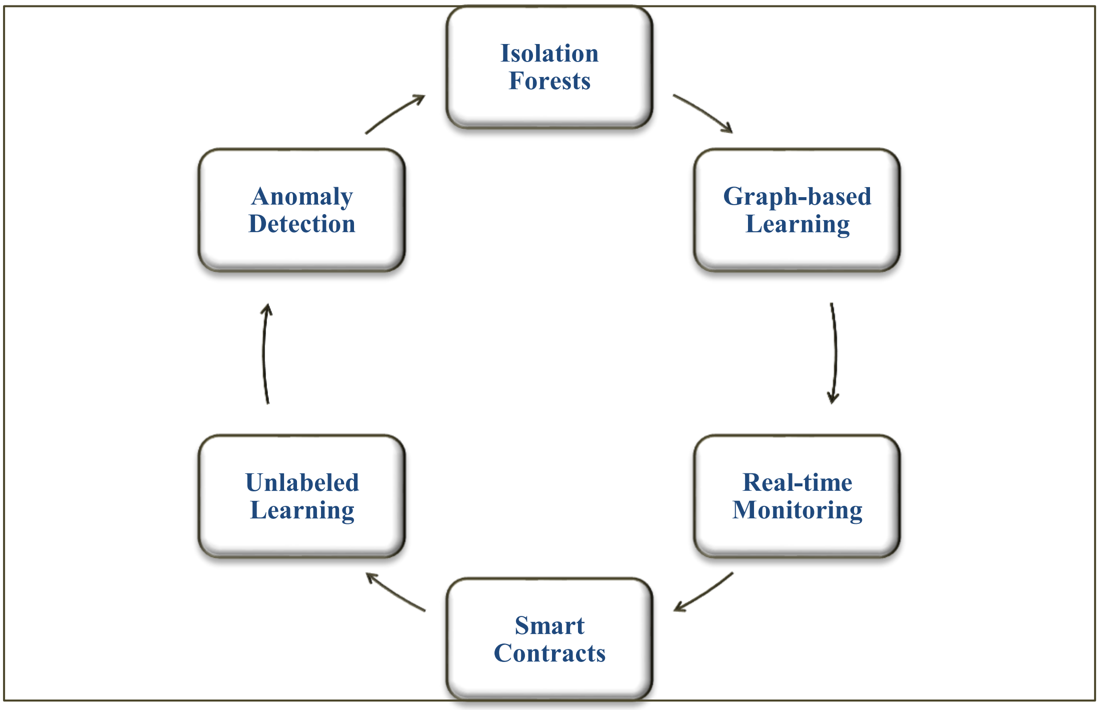

Figure 7: AI-Enabled Anomaly Detection Techniques in Fintech Portfolio Risk Management – Illustrative figure adapted from standard practices in anomaly detection literature.

(Source: Self-Developed)

Fintech companies use unlabeled learning pipelines that can learn typical behavioral baselines dynamically and autonomously (Haakman et al., 2020). Attachment to blockchain-based smart contracts provides traceability of transactions, which helps in identifying anomalies in the transactions and forensic analysis. With the help of AI, anomaly detection systems can shorten the detection time and raise the incident resolution rate due to automated prioritization of the alerts. Cloud-based AI platforms, such as a prominent cloud infrastructure provider SageMaker and a cloud services platform by Microsoft ML, are used illustratively to demonstrate scalable anomaly detection across real-time data pipelines (Sullivan and Lin, 2021). These models improve on detection results by including feedback loops, which adjust parameters and thus minimize false positives and make results more relevant. The results state that AI-enabled anomaly detection would help in risk signaling proactively and back up strong internal mechanisms of control pertaining to fintech portfolios. Thus, Recurrent Neural Networks (RNNs) are AI models ideal for sequential data analysis. Strengthening Risk Forecasting and Mitigation by analyzing sequential financial data to detect early risk signals (Yousuf et al., 2021). In AI-enabled fintech operations, RNNs improve risk detection accuracy and support compliance governance by forecasting potential breaches, enabling timely mitigation strategies and ensuring regulatory consistency across portfolio activities.

Organizational Readiness Measured by AI Governance Maturity Model

Application of a five-level AI Governance Maturity Model (AGMM) will offer a comprehensive process to determine and enhance AI preparedness within fintech risk procedures. In analyzing organizations, the model considers the following important dimensions. These are AI capability maturity, data governance, ethical compliance, stakeholder buy-in, and operational integration (Krijger *et al.,* 2022). Level 1 is the use of ad-hoc AI with less or no oversight, whereas Level 5 shows a completely institutionalized AI governance with cross-functional coordination. Examples of measures in maturity tests include explainability of the model (SHAP values), traceability of data lineage, and indicators of fairness in AI. Levels 3 and subsequent are the organizational practice of the AI validation procedure of model validation, the AI auditing procedure of bias, and the documentation of AI lifecycle telemetry (Oche, 2021). Alignment of strategic compliance officers, data scientists, and product managers is gauged along KPI frameworks and stages of governance scorecards. Research shows that the fintech's that reached Level 4 or above demonstrate a higher resilience to compliance-related disruptions and that their speed of regulatory adaptation is higher. The MRM practices, version control, scenario testing, and ethical AI fielding are maturity accelerators. The research confirms that the greater the maturity levels of AI, the better the operational agility as well as stakeholder trust and active risk management across fintech portfolios.

Increased Operational Transparency and Stakeholder Trust in Fintech

Operations of fintech that involve AI have boosted the level of transparency of operations and trust of regulators, investors, and consumers a lot (Rane, 2023). Such explainable AI (XAI) models as LIME and SHAP introduce interpretability to decision-making models and enable stakeholders to interpret risk scoring, credit approvals, and compliance alerts. Chain integration also improves audit facilities with auditable transactional records that are abiding. End-to-end traceability of financial flows can hence be performed. Dynamic data storytelling tools represent the compliance status, trend of anomalies, and fraud in AI-driven dashboards (Kumar *et al.*, 2024). Risk knowledge should be communicated in real-time across departments with the purpose of improving accountability and minimizing silo operations.

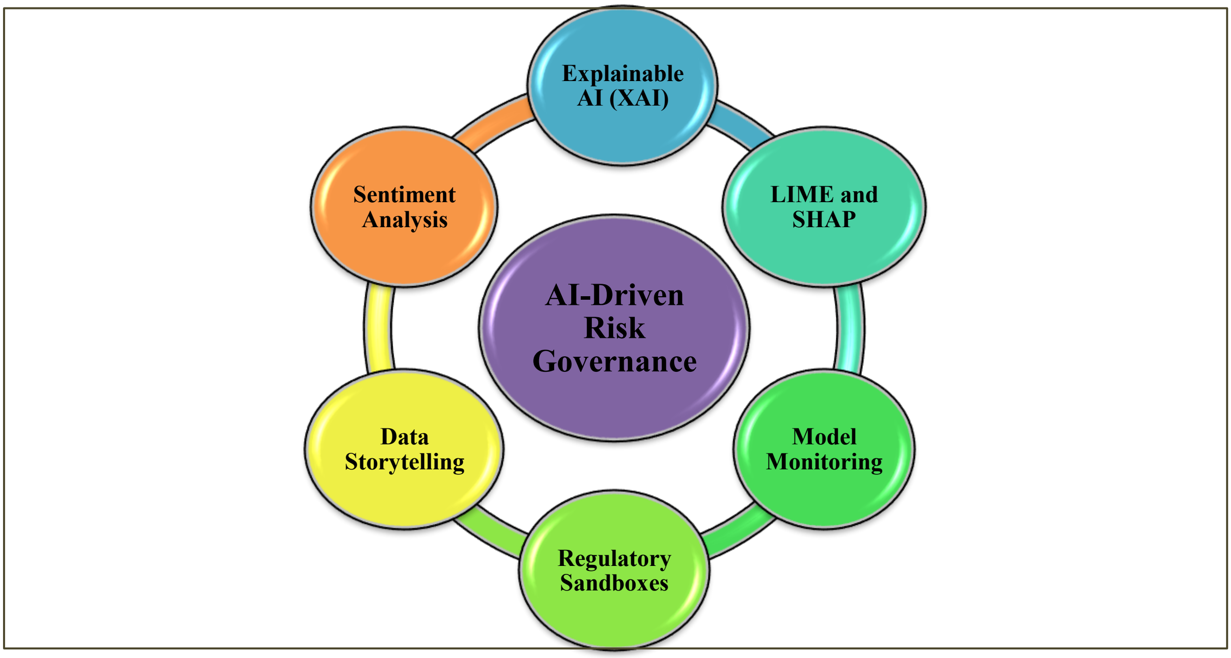

Figure 8: Increased Operational Transparency and Stakeholder Trust in Fintech – Conceptual figure developed by authors based on synthesized thematic interpretation.

(Source: Conceptual figure developed by authors)

Sentiment analysis and customer feedback mining are key features of the trust calibration models that can be used to determine the confidence of the user in digital services. The model monitoring systems update real-time performance drift, fairness metrics, and error rates to be transparent. Regulatory sandboxes help conduct iterative cycles of testing of AI compliance models within experimental settings, which enables innovation with control (Ranchordás, 2021). This evidence indicates that explainable AI in intelligently designed reporting and operational transparency has a central role in improving stakeholder trust and establishing institutional legitimacy in multidimensional fintech environments.

Conclusion

This research examined how AI, ML, and predictive analytics are changing risk detection, fraud prevention, and obedience governance in fintech portfolio operations. Through a secondary data examination of academic literature, industry reports, and case studies from firms like a leading global payments provider and a major digital payments company, the study emphasized the practical effectiveness of AI in amplifying real-time fraud observation and regulatory compliance with systems like PCI-DSS and PSD2. Predictive analytics appeared as a key tool for proactive risk prediction, while AI maturity models were recognized as essential for systematic adoption. The findings underscore the significance of integrating AI-driven tools within fintech ecosystems to boost operational endurance and regulatory alignment. Overall, this research provides a clearer comprehension of technological facilitators in fintech governance and furnishes a foundation for future studies or execution strategies.

References

[1] L. Abdel, R. Aziz, and Y. Andriansyah, *The Role of Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance*, 2023. [Online]. Available: https://core.ac.uk/download/pdf/578755756.pdf

[2] B. J. Aboze, "Understanding the AI Maturity Model," *Deepchecks*, 2023. [Online]. Available: https://www.deepchecks.com/understanding-the-ai-maturity-model-advancing-your-organizations-ai-capabilities/

[3] L. Alzubaidi *et al.*, "Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions," *Journal of Big Data*, vol. 8, no. 1, 2021. [Online]. Available: https://doi.org/10.1186/s40537-021-00444-8

[4] V. Arndt *et al.*, "Data from population-based cancer registration for secondary data analysis: Methodological challenges and perspectives," *Das Gesundheitswesen*, 2019. [Online]. Available: https://doi.org/10.1055/a-1009-6466

[5] A. Asatiani *et al.*, "Sociotechnical envelopment of artificial intelligence: An approach to organizational deployment of inscrutable artificial intelligence systems," *Journal of the Association for Information Systems*, vol. 22, no. 2, 2021. [Online]. Available: https://doi.org/10.17705/1jais.00664

[6] J. R. Baldwin *et al.*, "Protecting against researcher bias in secondary data analysis: Challenges and potential solutions," *European Journal of Epidemiology*, vol. 37, no. 1, pp. 1–10, 2022. [Online]. Available: https://doi.org/10.1007/s10654-021-00839-0

[7] M. Attaran and S. Attaran, "Opportunities and challenges of implementing predictive analytics for competitive advantage," *Int. J. Business Intelligence Research*, vol. 9, no. 2, pp. 1–26, 2018. [Online]. Available: https://doi.org/10.4018/ijbir.2018070101

[8] W. Bolander *et al.*, "Operationalising salesperson performance with secondary data: Aligning practice, scholarship, and theory," *Journal of the Academy of Marketing Science*, vol. 49, no. 3, pp. 462–481, 2021. [Online]. Available: https://doi.org/10.1007/s11747-020-00752-0

[9] H. M. Branka, "Measuring financial risks: The application of network theory in fintech risk management," *Unipv.it*, 2020. [Online]. Available: http://hdl.handle.net/11571/1344336

[10] R. D. Camino, "Machine learning techniques for suspicious transaction detection and analysis," *Orbilu.uni.lu*, 2020. [Online]. Available: http://hdl.handle.net/10993/44939

[11] L. Cao, Q. Yang, and P. S. Yu, "Data science and AI in FinTech: An overview," *Int. J. Data Science and Analytics*, vol. 12, no. 2, pp. 81–99, 2021. [Online]. Available: https://doi.org/10.1007/s41060-021-00278-w

[12] K. R. Chowdhary, "Natural language processing," in *Fundamentals of Artificial Intelligence*, pp. 603–649, 2020. [Online]. Available: https://doi.org/10.1007/978-81-322-3972-7_19

[13] K. C. Desouza, G. S. Dawson, and D. Chenok, "Designing, developing, and deploying artificial intelligence systems: Lessons from and for the public sector," *Business Horizons*, vol. 63, no. 2, pp. 205–213, 2020. [Online]. Available: https://doi.org/10.1016/j.bushor.2019.11.004

[14] D. Fabcic, "Strong customer authentication in online payments under GDPR and PSD2: A case of cumulative application," *IFIP Adv. Inf. Commun. Technol.*, pp. 78–95, 2021. [Online]. Available: https://doi.org/10.1007/978-3-030-72465-8_5

[15] J. Fürnkranz, T. Kliegr, and H. Paulheim, "On cognitive preferences and the plausibility of rule-based models," *Machine Learning*, vol. 109, no. 4, pp. 853–898, 2019. [Online]. Available: https://doi.org/10.1007/s10994-019-05856-5

[16] K. Gedris *et al.*, "Simulating municipal cybersecurity incidents: Recommendations from expert interviews," 2021. [Online]. Available: https://par.nsf.gov/servlets/purl/10257025

[17] J. Grennan and R. Michaely, "FinTechs and the market for financial analysis," *Journal of Financial and Quantitative Analysis*, vol. 56, no. 6, pp. 1–31, 2020. [Online]. Available: https://doi.org/10.1017/s0022109020000721

[18] M. Haakman *et al.*, "Machine learning behind the scenes: An exploratory study in Fintech," *Zenodo*, 2020. [Online]. Available: https://doi.org/10.5281/zenodo.3941476

[19] J. Singireddy, "Finance 4.0: Predictive analytics for financial risk management using AI," *European Journal of Analytics and Artificial Intelligence*, vol. 1, no. 1, 2023. [Online]. Available: https://esa-research.com/index.php/ejaai/article/view/30

[20] J. Krijger *et al.*, "The AI ethics maturity model: A holistic approach to advancing ethical data science in organisations," *AI and Ethics*, 2022. [Online]. Available: https://doi.org/10.1007/s43681-022-00228-7

[21] T. V. Kumar, "AI-powered fraud detection in real-time financial transactions," *Philpapers.org*, 2022. [Online]. Available: https://philpapers.org/rec/VARAFD-2

[22] H. Li, "Embedded microprocessor wireless communication data collection aids in early warning of default risk for internet finance bank customers," *Journal of Sensors*, pp. 1–10, 2021. [Online]. Available: https://doi.org/10.1155/2021/1679907

[23] L. O. Durodola, "Towards a responsible use of artificial intelligence (AI) and fintech in modern banking," pp. 262–278, 2021. [Online]. Available: https://doi.org/10.4324/9781003020998-18

[24] H. Ma, J. Liu, J. Zhang, and J. Huang, "Estimating the compressive strength of cement-based materials with mining waste using support vector machine, decision tree, and random forest models," *Advances in Civil Engineering*, pp. 1–10, 2021. [Online]. Available: https://doi.org/10.1155/2021/6629466

[25] N. Mahajan, "Strategic governance of digital tokenization for scalable B2B payment infrastructure," *J. Inf. Syst. Eng. Manage.*, vol. 2024, no. 1, 2024.

[26] R. P. Masini, M. C. Medeiros, and E. F. Mendes, "Machine learning advances for time series forecasting," *Journal of Economic Surveys*, vol. 37, no. 1, 2021. [Online]. Available: https://doi.org/10.1111/joes.12429

[27] N. Mahajan, "A predictive framework for adaptive resources allocation and risk-adjusted performance in engineering programs," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 11s, pp. 866, 2023.

[28] Oche, "Applications and challenges of artificial intelligence in space missions," *IEEE Xplore*, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9634015/

[29] R. Owen and R. Owen, "Artificial intelligence at a major digital payments company – Two unique use-cases," *Emerj AI Research*, 2022. [Online].

[30] S. Ranchordás, "Experimental regulations for AI: Sandboxes for morals and mores," *Morals & Machines*, vol. 1, no. 1, pp. 86–100, 2021. [Online]. Available: https://doi.org/10.5771/2747-2021-1-86

[31] N. Rane, S. Choudhary, and J. Rane, "Blockchain and artificial intelligence for revolutionising security and transparency in finance," *SSRN*, 2023. [Online]. Available: https://doi.org/10.2139/ssrn.4644253

[32] W. Reim, J. Åström, and O. Eriksson, "Implementation of artificial intelligence (AI): A roadmap for business model innovation," *AI*, vol. 1, no. 2, pp. 180–191, 2020. [Online]. Available: https://doi.org/10.3390/ai1020011

[33] J. Ribeiro *et al.*, "Robotic process automation and artificial industry intelligence in industry 4.0 – a literature review," *Procedia Computer Science*, vol. 181, pp. 51–58, 2021. [Online]. Available: https://doi.org/10.1016/j.procs.2021.01.104

[34] F. M. Shiri, T. Perumal, N. Mustapha, and R. Mohamed, "A comprehensive overview and comparative analysis of deep learning models: CNN, RNN, LSTM, GRU," *arXiv.org*, 2023. [Online]. Available: https://doi.org/10.48550/arXiv.2305.17473

[35] J. Singireddy *et al.*, "Innovative financial technologies: Strengthening compliance, secure transactions, and intelligent advisory systems through AI-driven automation and scalable data architectures," *Universal J. Finance and Economics*, vol. 1, no. 1, pp. 123–143, 2021. [Online]. Available: https://doi.org/10.31586/ujfe.2021.1298

[36] H. Sullivan and M. Lin, "Cloud-centric IoT data processing: A multi-platform approach," vol. 2, pp. 12–23, 2021.

[37] S. T. Jesso *et al.*, "Inclusion of clinicians in the development and evaluation of clinical artificial intelligence tools: A systematic literature review," *Frontiers in Psychology*, vol. 13, 2022. [Online]. Available: https://doi.org/10.3389/fpsyg.2022.830345

[38] S. Vyas, R. K. Tyagi, C. Jain, and S. Sahu, "A comparative study of real-time streaming technologies," 2021.

[39] H. Yousuf, M. Lahzi, S. A. Salloum, and K. Shaalan, "A systematic review on sequence-to-sequence learning with neural network and its models," *Int. J. Electrical and Computer Engineering*, vol. 11, no. 3, pp. 2315–2326, 2021. [Online]. Available: https://doi.org/10.11591/ijece.v11i3.pp2315-2326

[40] M. Zhuo, L. Liu, S. Zhou, and Z. Tian, "Survey on security issues of routing and anomaly detection for space information networks," *Scientific Reports*, vol. 11, no. 1, 2021. [Online]. Available: https://doi.org/10.1038/s41598-021-01638-z