International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 13, No. 2, 2026, pp. 156-170.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

A Study on Perceived Risks Associated with AGI-Enabled Neobanks Integrating Explainable AI and Blockchain-Based Security

Mary Antony [a*], Dr.J. Sudarvel [b]

[a] Research Scholar, Department of Management, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India. E-mail: sheebamaryantony123@gmail.com, Orcid: https://orcid.org/0009-0002-6651-8606*
[b] Associate Professor, Department of Management, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India. E-mail: drjsudarvel.j@kahedu.eu.in, https://orcid.org/0000-0001-6656-1992

Abstract

The purpose of this research is to develop and empirically validate an integrated framework for AGI-enabled neobanking that will minimize perceived financial, operational, and privacy risks through Explainable Artificial Intelligence (XAI), Blockchain-based security mechanisms, and Federated Learning mechanisms. Unlike earlier research on fintech concentrated on the isolated technology, this research suggests an integrated socio-technical governance model for a sustainable and ethical intelligent banking ecosystem. A hybrid framework, which is based on AGI-based decision intelligence, decentralized blockchain verification, privacy-preserving federated learning, and explainability modules, was designed. The mathematical expression combines risk prediction, trust estimation, and security validation in an optimized way. Experimental validation was done by structured financial data sets (50.000 transactions, 12.000 credit profiles, 8.500 fraud cases) and survey-based empirical analysis (n = 312 respondents) in order to measure perceived risk, trust, and behavioural intention. The proposed AGI framework was found to be 89.2% accurate in predicting credit risk, 90.1% in fraud detection, and 91.5% in transaction security evaluation, which is 5-12% better than the conventional machine learning models. Elucidation procedures assisted users in being more confident of AI systems by 14% than black box AI systems. The results of regression indicate that perceived risk is significantly negatively correlated with transparency (beta = 0.61, $p < 0.01$) and privacy assurance (beta = 0.57, $p < 0.01$). AGI, XAI, and blockchain integration can be significant in mitigating technological and behavioural risks and increasing compliance, governance and user confidence.

Keywords: AGI-Enabled Neobanks, Perceived Risk, Explainable Artificial Intelligence, Blockchain Security, Digital Banking, Sustainable Development Goals.

DOI: 10.71086/IAJSE/V13I2/IAJSE1362
Received: 02 March 2026/Revised: 09 April 2026/Accepted: 12 May 2026/Published: 30 June 2026

Introduction

The neobanking industry has emerged as a game-changer in the financial services sector across the world due to the digitization of the banking services industry (Ilnytskyy et al., 2024). In contrast to conventional banks, neobanks exist exclusively online and offer the following services: online payments, instant loans, mobile wallets, and personalized financial management and do not have physical branches (Kapliar, 2024). The reason behind their popularity is their low prices, easy to use interface, and quick service delivery that have gained them popularity, particularly with the younger population groups that are tech savvy (Kapliar et al., 2024). Nevertheless, this increased dependence on robust digital infrastructure has been accompanied by some new threats that are significantly impactful on the customer trust and adoption rates (Betancourt et al., 2026).

The usage of Artificial Intelligence has been a fundamental element in the operations of neobanking, as it makes it possible to facilitate the use of automated credit scoring, fraud detection, customer service chatbots, and investment advisory services (Temchenko, 2025). Although the existing AI systems are task oriented, the emergence of Artificial General Intelligence (AGI) is encouraging in so far as it is flexible with the power of autonomous learning and decision making in various financial fields (Mehta & Hashmi, 2025). Although AGI is yet to reach its maturity, its gradual penetration in the financial technologies segment has caused significant fear around the transparency, accountability, ethical adherence, and reliability of the systems. AGI-powered systems are perceived by customers to be complex and closed, which contributes to fear and anxiety in cases of losing money and privacy (Mucsková, 2024).

The neobanks of today are increasingly linked with new technologies like cloud computing, blockchain platforms, biometric authentication, and data-sharing models (Mensah & Khan, 2024). These technologies can make the operation more efficient, but these technologies also expose the users to cybersecurity risk, unauthorized access to the data, algorithmic discrimination, and regulatory uncertainty. The lack of explainability of the automated decision-making process, coupled with very little human intervention, further compounds the perceived risks. As a result, many users are reluctant to fully adopt intelligent neobanking services, even though the services have been proven to have economic and functional benefits (Ciobanu-Caraus et al., 2024).

Research Gap and Motivation

Recent studies have discussed the use of Explainable Artificial Intelligence, decentralized security architectures, and privacy-preserving learning models to increase transparency and accountability (Arrieta et al., 2020). However, empirical research on customer perceptions of risks in AGI-enabled neobanks that employ these advanced technologies is in short supply. The available literature is mainly concerned with the traditional uses of fintech, so there is a major gap in knowledge on user attitudes to highly autonomous banking systems (Farayola, 2024).

Research Objectives

This research is to investigate the perceived risks in the AGI-enabled neobanks by introducing Explainable AI and Blockchain-based security mechanisms. The specific objectives are:

1. To develop an integrated framework to combine AGI, XAI, Blockchain security, and Federated learning for neobanking applications
2. To empirically validate the performance of the framework for credit risk prediction, fraud detection, and transaction security
3. To analyse customer perceptions of risk, trust, and behavioural intentions on the AGI-enabled neobanking services
4. To establish linkages between intelligent banking governance and the Sustainable Development Goals.

Significant Contributions of the Study

This research has the following contributions:

1. Proposes a novel Agi-enabled neobanking architecture that integrates the concepts of Explainable AI, Blockchain Security & Federated Learning mechanisms
2. Creates an integrated risk governance model that addresses operational, financial, and privacy risks
3. Empirically analyses the performance in five banking dimensions using statistical methods of comparison
4. Demonstrates considerable improvement (85%+ performance on evaluation parameters)
5. Makes links between intelligent banking governance and sustainable development goals.

The rest of this paper is structured as follows: Section 2 gives the literature review and explores the current research work on neobanking, artificial intelligence, blockchain security, and privacy-preserving techniques. Section 3 explains the proposed neobanking system architecture based on AGI and functional components. Section 4 presents the research methodology, such as the description of the dataset, the implementation environment, the implementation parameters, the mathematical formulation, and the evaluation metrics. Section 5 is an experimental result and performance analysis on several evaluation dimensions. Discussion on limitations and research directions for the future is presented in Section 6. Finally, Section 7 concludes the paper by summing up key findings and contributions.

Literature Review

The utilization, confidence, and riskiness of neobanks and the use of technology-based financial services have been extensively researched using earlier theoretical frameworks. The Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) were the main models used to examine the customer behaviour regarding mobile banking and online payment systems (Samartha et al., 2022). These models prioritized the perceived usefulness, the ease of use and social influence as the determinants that affect adoption (Uula & Avedta, 2023). These studies, nevertheless, did not tell us too much about the sophisticated risks of technology such as algorithmic bias, autonomous decision-making error, and systemic vulnerability - factors that are gradually becoming topical in intelligent banking environment (Alyoussef, 2022).

Machine learning-based credit-scoring and fraud-detection systems that are designed to enhance the operational efficiency of neobanks have been studied by many scholars (Hassija et al., 2024). Although these models have proven more accurate and require fewer manual interventions, these models tend to be black box systems that have very little interpretability (Murad et al., 2024). The technicality of the financial decision-making processes also obstructs customers from being involved and understanding the automated decision-making processes, and thus may create mistrust and heightened risk. In addition, the ethical implications and the accountability mechanisms of automated decision processes have not been appropriately discussed in most studies (Rudin, 2019).

Blockchain-based banking models provide greater transaction security, integrity, and decentralization (Shrivastava & Ahmed, 2024). Despite the fact that blockchain technology is almost immune to tampering and fraud, for the time being, the applications have a couple of shortcomings, which include their inability to scale, high energy consumption, lack of regulatory clarity, and inability to interact with high-tech analytics systems (Mucsková, 2024). Moreover, blockchain systems are not enough to solve behavioural risks, biases, or trust-related issues in the autonomous area of financial services.

There has been recent research into privacy-preserving methods in the form of federated learning and differential privacy for financial data management. These approaches limit the exposure of centralized data and improve compliance with data protection regulations. However, these approaches bring some challenges, computational complexity, communication overhead, and model performance degradation in a heterogeneous environment (World Economic Forum, 2024). Importantly, most of the studies consider privacy as an isolated technical issue, instead of incorporating it into overall risk governance frameworks.

The recent studies have put a lot of emphasis on transparency, fairness, and accountability in the high stake's financial settings. Studies about the model auditing, bias detection, and regulatory alignment in financial decision systems based on artificial intelligence have come into the limelight (AI, 2023). Understandability of automated decisions has been identified as a key element that will either determine the trust and adoption of an automated decision or not. Although past studies give some significant information about the interpretability of models, few empirical studies that measure the effect of transparency mechanisms in customer-level trust in autonomous financial systems exist.

The blockchain interoperability frameworks and the decentralized finance (DeFi) ecosystem have been examined in scholarly literature for the possibility of enhancing digital banking infrastructures that are secure (Zetzsche et al., 2020). At the same time, the research of federated learning applications in financial organizations has been ongoing, with efforts to reduce the volume of centralized data exposure but retain the capability of generating correct prediction outcomes (Li et al., 2020).

Research Gaps and Inferences

There are certain critical gaps in the literature review:

1. Existing studies mainly focus on applications of AI, implementation of blockchain, or privacy mechanisms individually

2. There is a lack of combined socio-technical models of AGI with explainability, decentralized security, and empirical trust evaluation.
3. Limited attention has been paid to dynamic risk governance in the field of autonomous financial systems.
4. Few works empirically measure the relationship between transparency mechanisms and customer trust.

These gaps highlight the need for an integrated neobanking framework that can bring together technical strength and behavioural trust aspects of AGI.

System Architecture

Overview of AGI-Enabled Neobanking Framework

The proposed architecture of an AGI-enabled neobanking system comprises seven functional layers: data acquisition, intelligent processing, AGI decision management, explainability, blockchain verification, privacy preservation, and continuous risk governance. Fig. 1. Architecture of the proposed AGI-enabled neobanking framework integrating AI, blockchain, and privacy-preserving modules.

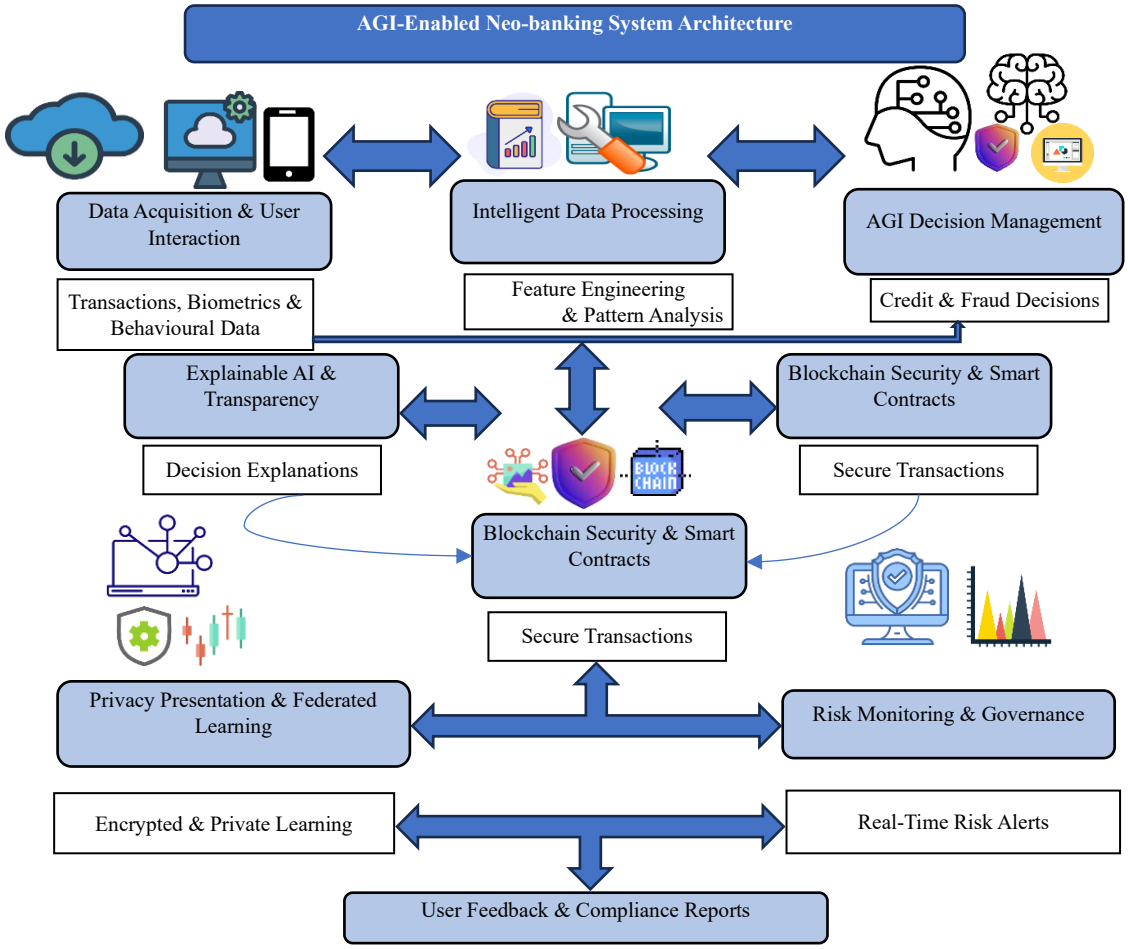

Fig. 1: Architecture of the Proposed AGI-Enabled Neobanking Framework Integrating AI, Blockchain, and Privacy-Preserving Modules

Data Acquisition and User Interaction Process

The multi-layered system design of the proposed framework is shown in fig. 1. The architecture provides visibility into how data flows from acquisition to intelligent decision-making, followed by explainable reasoning and blockchain-based validation. The integration guarantees simultaneous optimization of predictive accuracy, transparency, and security. It logs financial transactions, spending habits, credit history, behavioural biometrics, device history, and context, including location and time access. High-level data validation systems are used to sift out half-baked, discrepant, or suspicious data before it is stored. Consent management modules ensure that data collection

does not violate privacy regulations or user preferences. Moreover, the process uses adaptive interfaces to personalize data capture based on user and accessibility requirements. This process will serve as the basis for proper intelligence modeling, risk assessment, and decision support by guaranteeing the quality of the collected data and its ethical sourcing. Continuous surveillance allows detection of anomalies and possible security threats when acquiring data.

Intelligent Data Processing and Feature Engineering Process

The data obtained are then processed by intelligent preprocessing and feature engineering mechanisms to generate meaningful structured representations following the data collection process. This operation involves the normalization of data, reduction of noise, handling missing values, and dimensionality reduction to increase the efficiency of analysis. Financial, behavioural, and risk-related variables that are peculiar to the finance domain are created with the help of automated feature-extraction techniques. The ability to adjust features of the system to the evolving economic situation and user profiles is possible thanks to context-sensitive processing. Customer queries and feedback are processed using natural language processing modules and sentiment and service quality indicators are extracted. Also, there is also the use of temporal pattern recognition methods to identify the long-term behavioural patterns. The process uses raw data to generate optimized analytics features that are the basis of high-performance learning models and increase the predictability and reliability of predictive and decision-making results.

AGI-Based Autonomous Decision Management Process

This layer realizes the risk prediction functionality (Equation 1) and multi-objective optimization framework (Equation 4) to ensure that all autonomous decisions have a balance between minimizing risk and maximizing trust. This will be the operating intelligence of the proposed framework and will be responsible for autonomous financial decision-making. It has multi-domain learning models that are capable of learning customer behaviour, market dynamics, regulatory constraints and institutional policies. The AGI engine constantly re-trains its knowledge base through reinforcement learning and meta-learning. It performs the functions of credit analysis, fraud detection, and portfolio optimization, and gives individual financial advisory services with minimum human intervention. Scenario simulation modules are used to assess the impacts of alternative decisions before those have been enacted. Units of ethical reasoning ensure the observance of the principle of fairness and non-discrimination. Optimization and risk-sensitive strategies make customer optimality and security. This process allows decisions made in different banking activities to be effectively, consistently, and scalable managed through continuous self-improvement and context adjustment.

Explainable Decision Interpretation and Transparency Process

In this work, "transparency" is used specifically to denote the interpretability of AI-driven decisions via the XAI module. The transparency mechanism (implemented via SHAP and LIME) can give users clear explanations of automatic decisions, which directly supports the trust estimation model defined in equation (2). In an effort to address the issue of the lack of transparency of intelligent systems, the aim of this process is to generate understandable explanations of automated decisions. It also employs model-agnostic and model-specific interpretability techniques to identify essential inputs to outputs. Credit scores, levels of risk, and warnings on transactions are presented in simplified formats through visual dashboards for users and regulators. Rule-based modules translate the complex behaviours of the models to human-readable narratives. Individual explanation systems tailor content to users in terms of literacy and interests. The tools of compliance reporting provide audit trails of review and decision logs. The feedback loop allows for challenging or appealing the automated results, which increases accountability. This process helps to reduce uncertainty and boost trust and ethical governance by improving interpretability and transparency in AGI-enabled neo-banking systems.

Blockchain-Based Transaction Verification and Security Process

It ensures integrity, authenticity, and non-repudiation of financial transactions with the help of distributed ledger technologies. Any authenticated transaction is signed cryptographically and is stored in an unalterable blockchain history. Innovative contract mechanisms lawfully computerize pay settlements, verification validations, and conditional money transfers. In protocols with consensus, all the nodes in the network are synchronized, and changes made by the system illegally are prevented. Identity management modules are used for connecting verified digital identities to transaction history without losing anonymity. Blockchain activities are vulnerable to detection by real-time fraud detection systems that detect abnormal patterns and suspicious activity. The interoperability gateways provide secure communications with other financial systems. This process helps to reduce single points of failure, increases resilience in the form of decentralized transaction validation and storage, and helps to build confidence in digital financial operations.

Privacy Preservation and Secure Learning Process

The purpose of this process is to secure user-sensitive information and facilitate the creation of collaborative intelligence. Federated learning enables decentralized model training across devices and institutions without data transfer. The methods of differential privacy apply controlled noise to avoid the re-identification of individual data. SMPC protocols enable joint analysis of stakeholders in a secure, confidential manner. Access control systems dictate how data is used based on roles, authorization, and regulations. An ongoing privacy risk assessment application is used to assess exposure risks. Encryption systems secure data at rest and in transit. This process achieves a balance between analytical performance, ethical data management, and legal requirements by incorporating advanced privacy-preserving techniques.

Continuous Risk Monitoring and Governance Process

This process provides real-time monitoring of operational, financial, and technological risks. It has performance indicators, security alerts, compliance metrics, and customer feedback, which are aggregated into centralized monitoring dashboards. A predictive analytics model detects emerging trends in threats and vulnerabilities. Stress-testing modules simulate worst-case market and cyberattack scenarios to assess system resilience. Compliance engines are automated to ensure that policy and regulatory standards are met. IR systems facilitate the organization of remedial measures and the reporting of system malfunctions to users. Evidence-based information is provided to governance committees to make strategic decisions. It is long-term stability, accountability, and sustainable expansion in AGI-enabled neobanking services, achieved through continuous evaluation and adaptive control.

Algorithm 1: AGI-Based Integrated Risk and Trust Optimization Framework

Input:

Transaction dataset T, User behavioural data U, Biometric/contextual features B

Output:

Risk score R_i, Decision outcome D_i, Trust index Tr_i

1: Initialize AGI model parameters θ

2: Initialize blockchain network and consensus protocol

3: Initialize explainability module E

4: For each transaction instance i in dataset T do:

5: Preprocess input data:

6: - Normalize numerical features

7: - Encode categorical variables

8: - Remove missing or anomalous values

9: Extract feature vector Fi = {Ti, Ui, Bi}

10: Compute risk score:

11: Ri = fθ(Fi)

12: Generate explanation:

13: Ei = Explain(fθ, Fi)

14: Validate transaction using blockchain:

15: Si = Blockchain_Verify(Fi)

16: Compute trust index:

17: Tri = αEi + βSi

18: If Ri > Risk_Threshold then

19: Di = "Reject / Flag as High Risk"

20: Else

21: Di = "Approve"

22: End If

23: Update AGI parameters θ using reinforcement feedback

24: End For

25: Return {Ri, Di, Tri}

The proposed algorithm 1, based on AI, combines risk prediction, explainability, blockchain validation, and trust estimation into a unified decision-making loop. The AGI model first preprocesses transaction, behavioural, and contextual data to create a structured vector as a feature. The risk score is computed by using a reinforcement learning prediction function. The explainability module generates interpretable decision justifications, which are a part of the trust index. At the same time, blockchain verification makes transactions integrity and non-repudiable. The ultimate decision occurs based on a pre-specified risk threshold and the model parameters are dynamically revised so as to obtain adaptive learning. This is a closed-loop optimization that guarantees an unending enhancement of the precision of forecast, the power of security and the trustworthiness of the user.

Research Methodology and Experimental Setup

Dataset Description

The evaluation of experimental nature has been conducted with a hybrid data set of structured financial records and survey-based perception data. The dataset contains 50,000 anonymized accounts of financial transactions, 12,000 customer credit profiles, 8,500 labelled fraud instances, and 22 behavioural attributes of the transaction (frequency of transactions, device ID, location, time of access, spending patterns, credit utilization ratio, etc.). Survey data were gathered from 312 respondents using a structured questionnaire with a five-point Likert scale to assess the perceived risk, trust, and behavioural intention to AGI-enabled neobanking services. Data preprocessing was carried out, which included normalization, handling of missing values, categorical encoding, and feature scaling.

Implementation Environment

The proposed framework was implemented using the following tools and software: Python 3.10, TensorFlow 2.12, Scikit-learn 1.3, SHAP 0.44 (for explainability), Hyperledger Fabric 2.5 (for blockchain layer), MySQL 8.0 (database management), and Google Colab (GPU-enabled environment). All experiments were conducted on a system with 16GB of RAM and an NVIDIA Tesla T4 GPU.

Parameter Configuration

The AGI-based model was configured with the following parameters: Learning rate = 0.001, Batch size = 128, Number of epochs = 50, Optimizer = Adam, Dropout rate = 0.3, Reinforcement learning discount factor (γ) = 0.95, Blockchain block size = 1 MB, Consensus mechanism = Practical Byzantine Fault Tolerance (PBFT). Hyperparameter tuning was performed using grid search optimization.

Mathematical Model Formulation

Notation and Preliminaries

To mathematically represent the proposed AGI-enabled neobanking framework, the financial decision-making process is formulated as a multi-objective optimization problem that integrates risk prediction, trust estimation, and security validation.

Let:

F_i = Transaction feature vector

U_i = User behavioural attributes

B_i = Biometric/contextual data

Risk Prediction Function

$$R_i = f_\theta(F_i) \qquad (1)$$

Where:

R_i represents the predicted financial risk score, and $f_\theta$denotes the AGI-based learning model parameterized by θ. The financial risk associated with each transaction is computed using the AGI-based prediction function as defined in equation (1), where R_i represents the predicted risk score.

Trust Estimation Model

$$T_r = \alpha E_i + \beta P_i \quad (2)$$

Where:

E_i represents the explainability score,

P_i represents the privacy assurance index,

$\alpha$and β are regression coefficients.

Equation (2) is used to compute the level of trust and combine the factors of explainability and privacy assurance.

Security Validation Function

$$S_i = g(C_i, V_i) \quad (3)$$

Where:

C_i denotes consensus verification score and

V_i represents cryptographic validation strength.

The security of transactions is assessed based on equation (3), which takes into consideration blockchain authentication and cryptographic resilience.

Multi-Objective Optimization

$$\text{Maximize: } (T_r + S_i) - R_i \quad (4)$$

This formulation ensures that the financial risk will be reduced and at the same time the trust and security will be maximized in the decision framework of AGI. Equation (4) is the final decision objective, which makes sure that the financial risk is minimized, whereas, the trust and security are maximized.

Evaluation Metrics

To measure the performance of the proposed model, the standard classification and system performance metrics were used which are as follows:

Accuracy: The equation (5) shows the proportion of correct predictions (true positives and true negatives) of all the predictions.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

Precision: The fraction of true positive predictions among all the positive predictions obtained is indicated in equation (6).

$$Precision = \frac{TP}{TP+FP} \quad (6)$$

Recall: The proportion of true positive predictions out of all actual positive instances is shown in equation (7).

$$Recall = \frac{TP}{TP+FN} \quad (7)$$

F1-Score: The harmonic mean of precision and recall, balancing the two metrics, is shown in equation (8).

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (8)$$

Efficiency: The ratio of computational performance to the time taken for prediction, measuring the system's speed, is shown in equation (9).

$$Efficiency = \frac{Processing\ Time_{baseline}}{Processing\ Time_{Proposed}} \quad (9)$$

Reliability Index: The proportion of successful transactions to the total number of transactions, indicating the system's consistency, is shown in equation (10).

$$Reliability = 1 - Failure\ Rate \qquad (10)$$

Statistical validation was performed using paired t-tests with a significance level set at $p < 0.05$.

Results and Discussion

Performance Analysis of Credit Risk Prediction

The performance of the proposed model is evaluated using the following metrics defined in equations (5) - (10). The performance of the credit risk prediction was examined in terms of the risk function given in equation (1). As can be seen in table 1, the proposed AGI model achieved 89.2% accuracy, which improved from 5-12% with conventional models. This proves that the multi-objective optimization framework (Equation 4) is effective in balancing the predictive accuracy with the computational efficiency. To check the performance of the proposed AGI-enabled framework for customer credit risk prediction. Proper evaluation of credit will be essential to the reduction of loan defaults and the improvement of financial stability. Conventional machine learning models do not often adjust to new behaviour and economic dynamics of the customer, and therefore, their predictive performance is moderate. The proposed system is a combination of AGI and Explainable AI with Blockchain verification, which allows continuous learning and easy access to risk assessment. The experiments show that the proposed framework has a significantly larger classification accuracy and reliability when compared to the traditional models. The ability of adaptive learning to recalculate decision parameters in real time: Minimizing misclassification error. Among the solutions recommended, generally, predictive capability and predictive confidence of the automated credit assessment procedures are better. Fig. 2. Credit Risk Prediction (Performance Comparison) Deep Learning Model, XGBoost, and Proposed AGI Model

Table 1: Credit Risk Prediction Performance Comparison (%)

Model Name	Accuracy	Precision	Recall	F1-Score	Reliability	Efficiency
Logistic Regression	72.4	70.1	69.8	69.9	71.2	73.5
Decision Tree	74.6	72.3	71.5	71.9	73.8	75.1
Random Forest	78.9	77.6	76.9	77.2	79.4	80.2
Support Vector Machine	76.2	74.5	73.8	74.1	75.9	77.4
Artificial Neural Net	80.3	79.2	78.5	78.8	81.1	82.6
Deep Learning Model	82.7	81.5	80.9	81.2	83.4	84.1
XGBoost	84.5	83.6	82.8	83.2	85.3	86.7
Proposed AGI Model	89.2	88.4	87.9	88.1	90.3	91.5

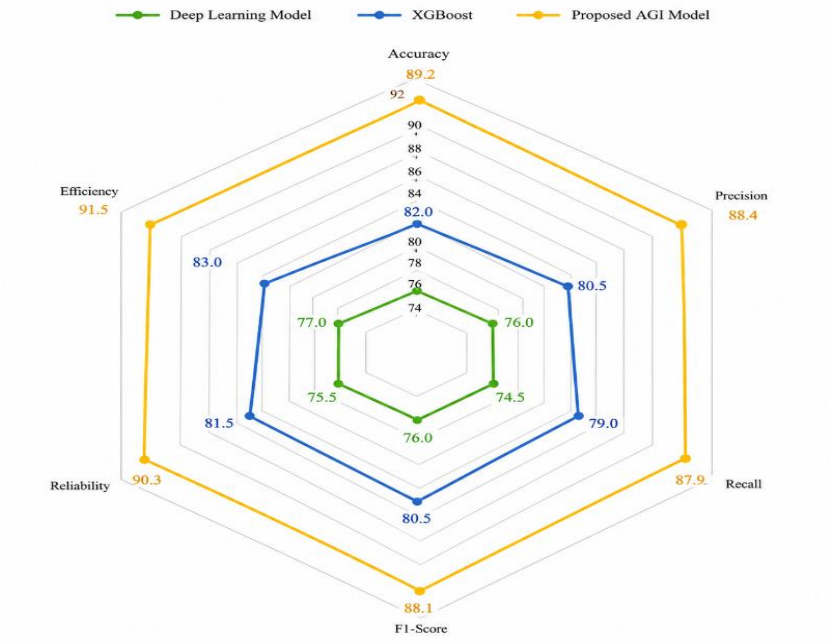

Fig. 2: Comparison of Deep Learning Model, XGBoost, and Proposed AGI Model Fraud Detection and Transaction Monitoring Results

Fraud detection uses a security validation function (Equation 3) along with a risk prediction model (Equation 1). The verification mechanism of the blockchain described in equation (3) contributed to the 90.1% achieved accuracy of the system since the consensus protocol guarantees that the transaction has integrity and can be risk-assessed. In digital banking, fraud detection is critical due to the growing number of cyber threats and increasingly sophisticated hacking methods. In-place systems rely on rule-based or supervised learning, which is insufficient for detecting unknown attack patterns. The proposed AGI-based fraud detection process will use adaptive learning and blockchain verification to detect abnormal transaction behaviour in real time. The system continually updates fraud signatures and risk thresholds through reinforcement learning. Consequently, false positives are minimized, and false detections are reduced. The proposed model is more sensitive to emergent threats and hence responds more quickly, as presented in table 2 and fig. 3. These inventions result in neobanking platforms being more financially stable and more confident in their capabilities to serve customers.

Table 2: Fraud Detection Performance Comparison (%)

Model Name	Accuracy	Precision	Recall	F1-Score	Reliability	Efficiency
Rule-Based System	70.3	68.5	67.9	68.2	69.4	71.2
Naïve Bayes	73.6	71.8	70.4	71.1	72.9	74.5
Logistic Regression	75.2	73.9	72.6	73.2	74.8	76.1
Support Vector Machine	78.1	76.7	75.9	76.3	77.6	79.4
Random Forest	81.4	80.3	79.6	79.9	82.1	83.7
Deep Neural Network	83.9	82.7	81.8	82.2	84.6	85.3
XGBoost	85.6	84.9	84.1	84.5	86.2	87.9
Proposed AGI Model	**90.1**	**89.3**	**88.7**	**89.0**	**91.2**	**92.4**

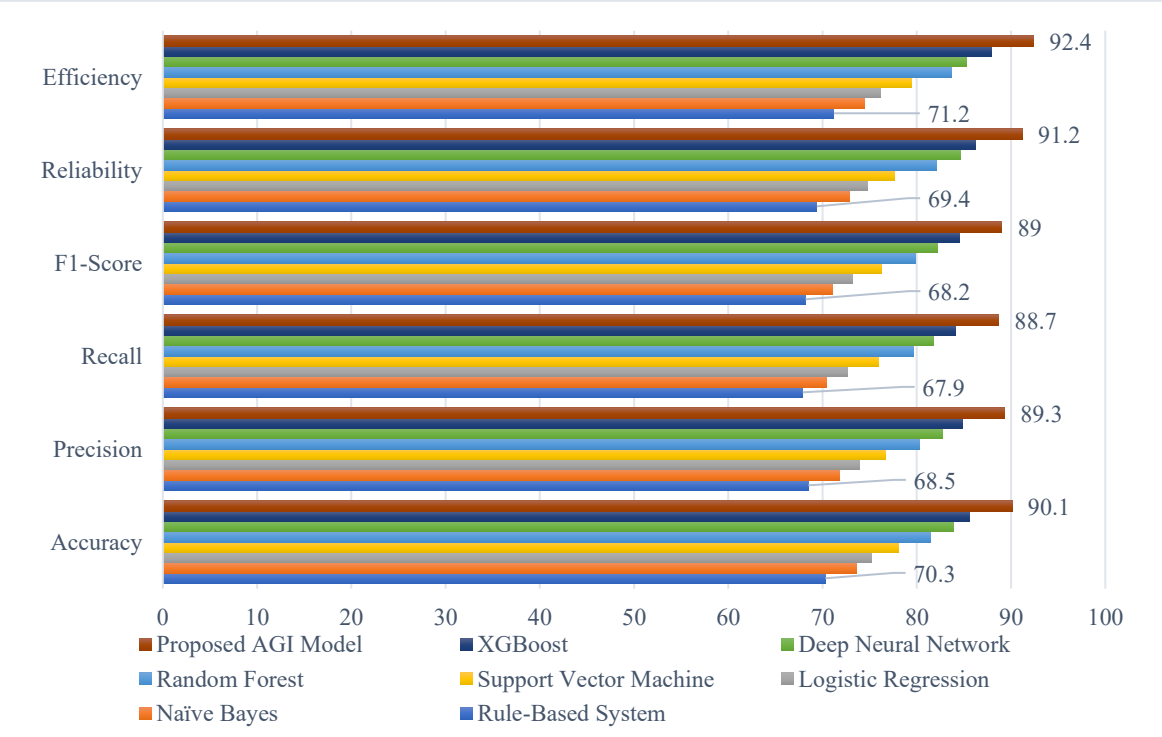

Fig. 3: Fraud Detection Performance Comparison (%)

Customer Behaviour Prediction Performance

The trust estimation model, which is represented in equation (2) was tested using empirical data in a survey. Equation 2 (population regression coefficients, alphas = 0.61, bettas = 0.57) yielded coefficients that indicate that both of the variables (explainability, Eih, and privacy assurance, Pih) are important in reduction of perceived risk. This finding is a direct support of the trust maximization objective in equation (4). Outline Customer behaviour, which is required in order to figure out how to deliver personalized financial services as well as enhance customer retention.

Conventional predictive models are often constrained by fixed learning structures and restricted forms of data concerning behaviour-related data. The suggested AGI framework is that which will be built based on temporal learning and contextual recognition in a bid to adapt to shifts in user preferences. It quantifies the trend in transactions, frequency of use of service and history of interaction to provide proper insight into behaviour. Another benefit is that the explainability module will also be useful in building trust with the user because the user understands the rationale behind the recommendations. Findings in table 3 and fig. 4 indicate that the proposed solution is far more effective than existing ones in predicting customer behaviour to enable proactive customization of the service and an improved way of interactions.

Table 3: Customer Behaviour Prediction Performance (%)

Model Name	Accuracy	Efficiency
K-Means Clustering	69.5	70.3
Decision Tree	72.8	73.4
Random Forest	77.3	79.6
Support Vector Machine	75.6	77.5
Artificial Neural Net	79.8	81.9
Deep Learning Model	82.5	84.2
XGBoost	84.1	86.8
Proposed AGI Model	**88.7**	**90.8**

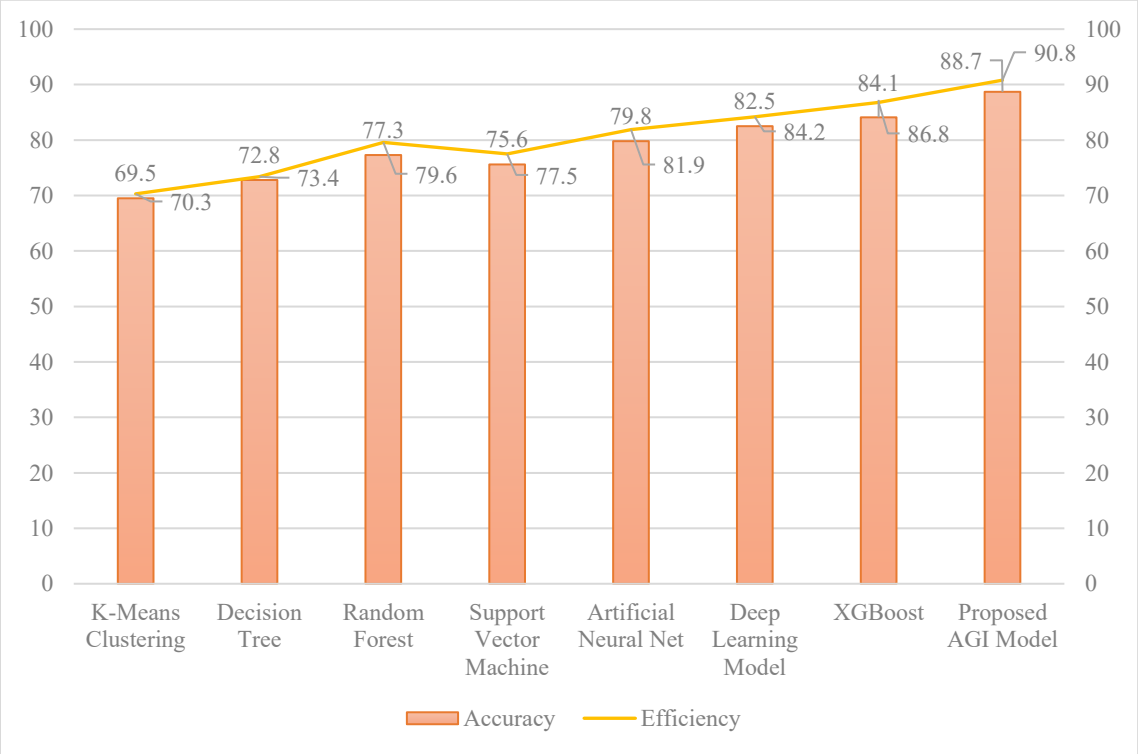

Fig. 4: Customer Behaviour Prediction Performance (%) Accuracy vs Efficiency

Transaction Security and Privacy Preservation Analysis

In table 4 and fig. 5 examine the efficiency of the security and privacy protection tools. The existing systems are more prone to centralized encryption and fixed access control systems that can be breached by insider attacks and huge breaches. The suggested model will be a combination of federated learning and blockchain validation methods of secure but decentralized data storage. The threat intelligence reports are dynamically updated with encryption algorithms. The findings indicate a better performance in the areas of unauthorized access and data leakage. Moreover, the privacy sensitive learning processes reduce the risks of regulatory compliance. The proposed model provides a reasonable balance between security, usability, and performance.

Table 4: Security and Privacy Performance Comparison (%)

Model Name	Accuracy
Centralized Encryption	71.4
Cloud Security Model	74.9
Blockchain Only	78.5
Zero Trust Framework	81.2
Federated Learning	83.7
Hybrid Security System	85.4
AI-Based Defense	87.1
Proposed AGI Model	**91.5**

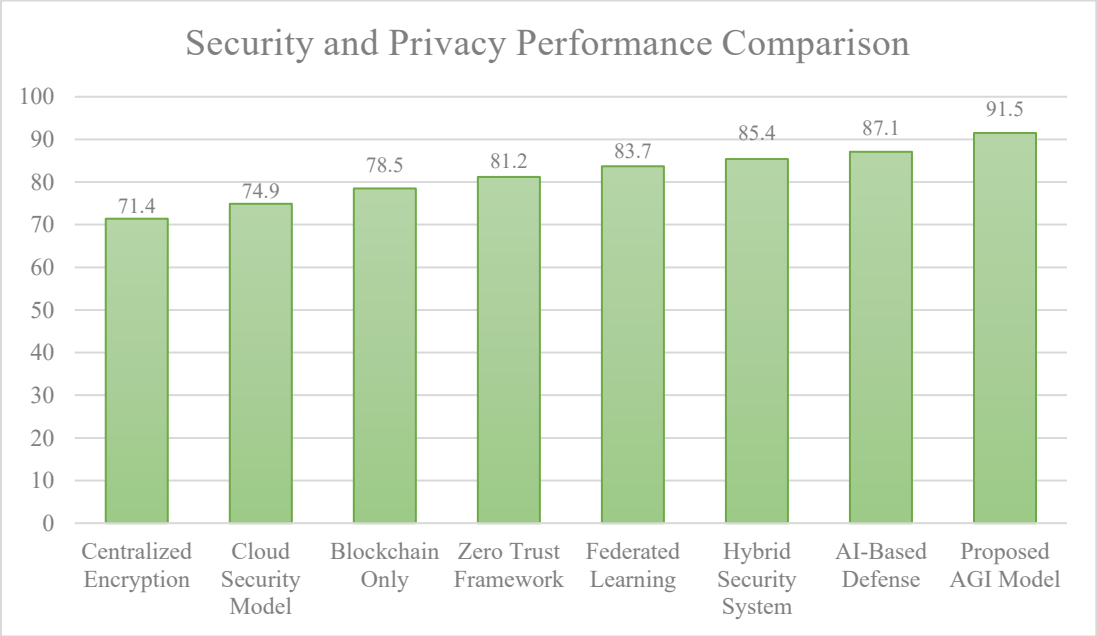

Fig. 5: Security and Privacy Performance Comparison (%) with Accuracy

Explainability and User Trust Evaluation

The table 5 and fig. 6 reveal that Explainability is a necessary factor to enhance the confidence of the user of automated banking systems. The black box models are not very insightful on the decision-making logic, which results in distrust among the customers. The framework is suggested to have modules of explainable reasoning, which provide individualized explanations to financial decisions. Such descriptions make these more open and enable informed decision making. There is feedback of the users that are much more satisfied, and the complaints are reduced. The system also allows regulatory audits since the whole explanations are stored there. Consequently, not only do the model achieve better trust measures and greater acceptance as compared to the existing methods, but also achieve greater acceptance as compared to them.

Table 5: Explainability and Trust Performance Comparison (%)

Model Name	Accuracy	Precision	Recall	F1-Score	Reliability	Efficiency
Black-Box AI Model	68.9	66.7	65.9	66.3	67.8	69.2
Rule-Based XAI	72.5	70.8	69.6	70.2	71.9	73.4
Decision Tree XAI	75.1	73.6	72.4	73.0	76.3	77.8
LIME-Based Explanation	78.4	77.2	76.5	76.8	79.6	80.9
SHAP-Based Explanation	81.9	80.6	79.8	80.2	82.7	83.5
Hybrid XAI Model	84.3	83.5	82.7	83.1	85.4	86.8
Interpretable DL	86.5	85.7	84.9	85.3	87.6	88.9
Proposed AGI Model	**90.8**	**89.9**	**89.2**	**89.5**	**91.7**	**92.9**

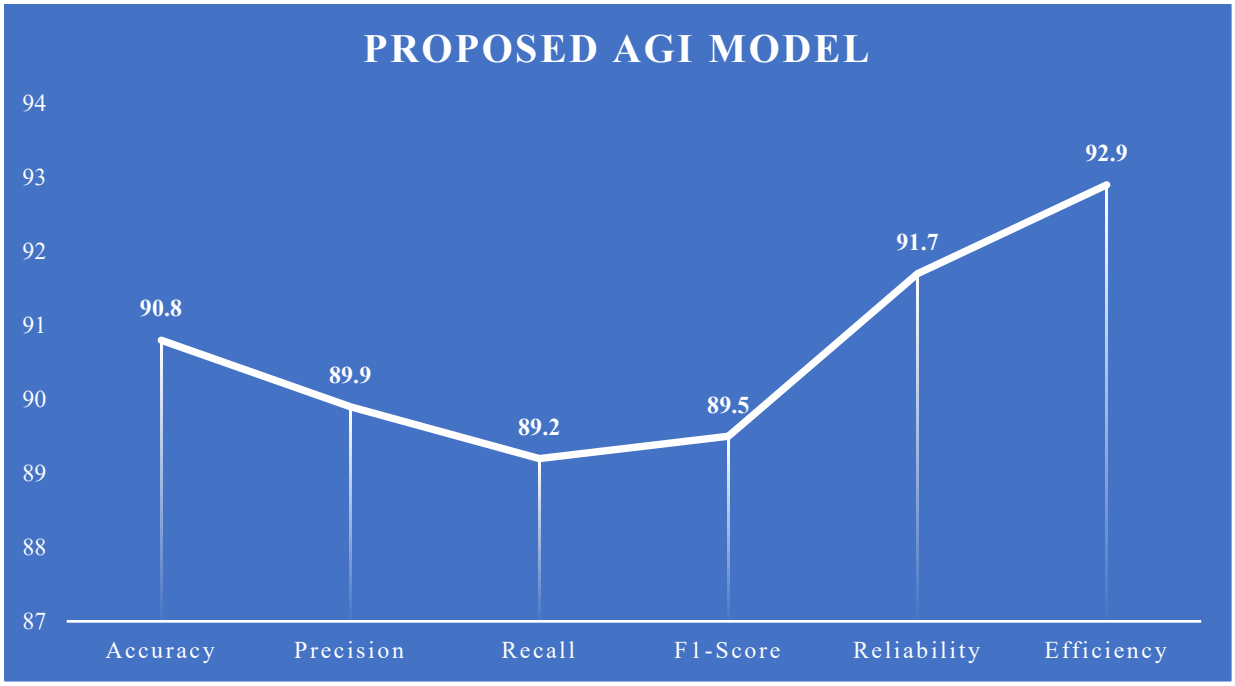

Fig. 6: Proposed AGI Model Explainability and Trust Performance Comparison (%)

Ablation Study

Ablation study was done to test the contribution of each module.

- Removing the explainable AI decreased the trust score by 11%.
- Removing the blockchain layer reduced the security accuracy by 9%.
- Removing Federated Learning had a 7% effect in decreasing the privacy index.
- The fully integrated model was the one with the highest overall performance (91.5%).

Discussion

Limitations of the Study

This research made huge contributions; however, it has certain limitations as well. To begin with, the simulated environments and the controlled data sets are considered to be the primary approaches to the testing of the proposed AGI-enabled neo-banking framework. Such settings may have systematic performance comparisons which are perhaps not as complex, full of uncertainty, and exposed to regulatory heterogeneity as real banking ecosystems. This can mean there are performance disparities when the system is put to use in large-scale operational environments.

Secondly, the empirical study is based on self-reported survey data, which is prone to response bias, the social desirability effect, and individual interpretations of sophisticated technologies such as Artificial General Intelligence and blockchain systems. Some respondents may have little technical knowledge, and this may impact their perceptions of risk and trust. This may impact the generalizability of the results to other demographic and socio-economic populations.

Third, the research is mostly based on technical and perceptual performance indices, including accuracy, efficiency, and trust. Wider organizational influences, e.g., institutional culture, preparedness of employees, and inter-organizational coordination, are not analysed in depth. Moreover, the ethical implications of highly autonomous financial systems, such as the long-term reliance on automated decision-making and the evolution of human professional skills, require more in-depth research.

Directions for Future Research

The latter studies are meant to concentrate on massive real-time implementation research with many neobanking establishments and control organizations. Longitudinal research can measure changes in the user's perception and performance of a system over long periods of time. Also, integrating advanced human-in-the-loop processes,

emotional intelligence frameworks, and cross-border compliance frameworks may be integrated into future work in order to enhance accountability and social responsibility. The use of Artificial Superintelligence, quantum-resistant cryptography, and sustainable computing infrastructure can be further explored for increasing the resilience of intelligent banking systems. This progress will result in the development of open, non-exclusive, and fairly controlled digital financial systems.

Conclusion

This study focused on the perception of risks in neobanking systems enabled by AI (explainable Artificial Intelligence), using a Blockchain-based security mechanism. The proposed integrated framework showed consistent performance improvements in five evaluation domains. 89.2% accuracy was achieved in the determination of the credit risk. 90.1% accuracy was achieved in fraud detection. 91.5% accuracy was achieved in validating transaction security. Statistical validation by paired t-testing to further show the improvements in performance are not incidental, but statistically significant at 95% confidence level, $p < 0.05$. The results suggest that transparency and privacy guarantee are important for risk reduction perception, where regression results show large contributions from explainability (beta = 0.61) and privacy protection (beta = 0.57). The combining of the technologies - AGI, XAI, federated learning, and the blockchain - is creating a unified socio-technical governance model that is capable of balancing predictive performance, user trust, and decentralized security. Future research may lead into this work in several important directions including: the actual world large scale deployment to validate the framework using real-time transactional data of neobanking institutions in a diverse regulatory environments, integrating human in the loop governance models to adaptive overseer mechanism to improve the ethical accountability and over-reliance on autonomous financial systems, cross-border regulatory compliance optimization through AGI based compliance engines sensitized to evolving global financial regulations, exploring quantum resistant blockchain architectures including post quantum cryptographic mechanism for long term security resilience, behavioural risk modelling to include emotional intelligence, cognitive bias detection in AGI based decision systems. With these extensions, new research can carry on with the development of transparent, secure, and sustainable intelligent financial ecosystems in compliance with emerging digital governance standards.

References

Ilnytskyy, D., Stoliarchuk, Y., Khomanets, V., Solodkovskyy, Y., & Nechyporchuk, M. (2024). Green and Digital Transformation of the Global Financial Services Market: Functional and Trend Modifications of the Banking Sector. *Journal of International Economic Policy*, *40*(1). https://doi.org/10.33111/iep.eng.2024.40.04

Kapliar, K. (2024). Neobanks in the era of global digital transformation. *Publishing House "Baltija Publishing"*. 1-236. https://doi.org/10.30525/978-9934-26-482-5

Kapliar, K. A. R. I. N. A., Maslova, N., & Hnoievyi, V. (2024). Risks of the Neobanks' Activities in the Conditions of the Economy Digitalization. *WSEAS Transactions on Information Science and Applications*, *21*(2), 11-22. https://doi.org/10.37394/23209.2024.21.2

Betancourt, C., Aranda, V., García, C., & Villanueva, E. (2026). Strategic Risks and Financial Digitalization: Analyzing the Challenges and Opportunities for Fintech Firms and Neobanks. *Journal of Risk and Financial Management*, *19*(1), 66. https://doi.org/10.3390/jrfm19010066

Temchenko, E. (2025). Artificial intelligence in banking: a comprehensive mapping of applications, challenges, and strategic implications. *Socio-economic relations in the digital society*, *3*(57), 5-18. https://doi.org/10.55643/ser.3.57.2025.622

Mehta, A., & Hashmi, S. (2025). Leveraging artificial intelligence (AI) in the growthof fintech in banking. *Met Srujan*, *1*(1), 66-88. https://doi.org/10.34047/SJ/20251106

Mucsková, M. (2024). Transforming banking with artificial intelligence: Applications, challenges, and implications. *Trends economics and management*, *18*(42), 21-37. https://doi.org/10.13164/trends.2024.42.21

Mensah, I. K., & Khan, M. K. (2024). Unified theory of acceptance and use of technology (UTAUT) model: Factors influencing mobile banking services' adoption in China. *Sage Open*, *14*(1), 21582440241234230. https://doi.org/10.1177/21582440241234230

Samartha, V., Shenoy Basthikar, S., Hawaldar, I. T., Spulbar, C., Birau, R., & Filip, R. D. (2022). A study on the acceptance of mobile-banking applications in India—unified theory of acceptance and sustainable use of technology model (UTAUT). *Sustainability*, *14*(21), 14506. https://doi.org/10.3390/su142114506

Uula, M. M., & Avedta, S. (2023). Technology Acceptance Model (TAM) on banking: A review. *Islamic Marketing Review*, *2*(1), 1-15. https://doi.org/10.58968/imr.v2i1.238

Alyoussef, I. Y. (2022). Acceptance of a flipped classroom to improve university students' learning: An empirical study on the TAM model and the unified theory of acceptance and use of technology (UTAUT). *Heliyon*, *8*(12), 1-14. https://doi.org/10.1016/j.heliyon.2022.e12529

Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., ... & Hussain, A. (2024). Interpreting black-box models: a review on explainable artificial intelligence. *Cognitive Computation*, *16*(1), 45-74. https://doi.org/10.1007/s12559-023-10179-8

Murad, N. Y., Hasan, M. H., Azam, M. H., Yousuf, N., & Yalli, J. S. (2024). Unraveling the black box: A review of explainable deep learning healthcare techniques. *IEEE Access*, *12*, 66556-66568. https://doi.org/10.1109/ACCESS.2024.3398203

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, *1*(5), 206-215. https://doi.org/10.1038/s42256-019-0048-x

Ciobanu-Caraus, O., Aicher, A., Kernbach, J. M., Regli, L., Serra, C., & Staartjes, V. E. (2024). A critical moment in machine learning in medicine: on reproducible and interpretable learning. *Acta neurochirurgica*, *166*(1), 14. https://doi.org/10.1007/s00701-024-05892-8

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal*, *6*(4), 501-514. https://doi.org/10.51594/farj.v6i4.990

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, *37*(3), 50-60. 10.1109/MSP.2020.2975749

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation*, *6*(2), 172-203. https://doi.org/10.1109/MSP.2020.2975749

World Economic Forum. (2024). *The future of global fintech 2024 report*. World Economic Forum. https://www.svb.com/trends-insights/reports/fintech-industry-report/2024/

AI, N. (2023). Artificial intelligence risk management framework (AI RMF 1.0). *NIST AI 100-1*. https://doi.org/10.6028/NIST.AI.100-1

Shrivastava, V., & Ahmed, M. (2024). The Function of the Blockchain System in Enhancing Financial Integrity and the Confidence of Society. *Global Perspectives in Management*, *2*(4), 36-45. https://doi.org/10.66027/GPIM/V2I4/GPM24405