

AI-ENABLED PREDICTIVE RISK INTELLIGENCE FOR SAUDI BANKING SYSTEMS: INTEGRATING SHARIAH COMPLIANCE, ADVANCED FINANCIAL ANALYTICS, AND REGULATORY DATA GOVERNANCE

Farah Arzu¹, Abdul Waheed², Sayed Hassan Ijaz³, Dr. Shah E Yar Qadeem⁴, Fazle Adil⁵

¹Tun Razaq Graduate School of Business, Universiti Tun Abdul Razak, Kuala Lumpur, Malaysia

²Department of Computer Science, Tandon School of Engineering, New York University, United States of America

³Department of Computer Science, Pir Mehr Ali Shah - Arid Agricultural University - Rawalpindi, Pakistan

⁴Assistant Professor. Department of Management Sciences, Qurtuba University of Science and Information Technology, Peshawar, Pakistan

⁵Local Government & Rural Development Department Government of Khyber Pakhtunkhwa. MSC International Business Department of Ulster University Business School at Ulster University London United Kingdom

¹arzu.farah@ur.unirazak.edu.my, ²aw4782@nyu.edu, ³prof.hassanijaz@gmail.com, ⁴shaheyar605@gmail.com, ⁵fazleadil@gmail.com

DOI: <https://doi.org/10.5281/zenodo.22022819>

Keywords

Saudi banking systems; AI-driven risk assessment; Shariah-compliant financial analytics; regulatory-aware data governance; explainable machine learning; cybersecurity risk intelligence; financial fraud detection; SAMA regulatory compliance

Article History

Received: 19 January 2026

Accepted: 04 March 2026

Published: 18 March 2026

Copyright @Author

Corresponding Author: *
Abdul Waheed

Abstract

The rapid digital transformation of Saudi Arabia's banking sector has created significant opportunities for intelligent financial risk management while introducing increasingly complex challenges related to credit exposure, liquidity pressure, financial fraud, cybersecurity threats, operational disruption, regulatory compliance, and Shariah governance. This study develops an AI-driven risk assessment model for Saudi banking systems by integrating Shariah-compliant financial analytics with regulatory-aware data governance. The proposed framework addresses the distinctive requirements of banks operating within the Saudi financial ecosystem, where advanced risk assessment must support Shariah-compliant financial practices while ensuring transparency, cybersecurity resilience, data protection, and regulatory accountability. A multi-source dataset was constructed using published annual reports of Saudi banks, Saudi Central Bank (SAMA) banking statistics, Tadawul-listed bank disclosures, financial stability indicators, Shariah governance reports, macroeconomic variables, and structured banking-risk records. To enhance the realism and analytical depth of the framework, anonymized and simulated transaction-level data were incorporated, including customer financing behavior, delayed repayment patterns, digital payment activities, suspicious transaction indicators, abnormal login attempts, cybersecurity alerts, and Shariah-compliance risk signals. The collected data were processed through feature normalization, missing-value treatment, class balancing, contract-based feature engineering, risk-category labeling, and regulatory attribute mapping. Multiple machine-learning approaches were evaluated, including logistic regression, support vector machine, random forest, gradient boosting, and the proposed explainable ensemble risk assessment model. Experimental results demonstrate that the proposed model achieved superior

predictive performance, attaining 96.4% accuracy, 95.8% precision, 96.1% recall, 96.0% F1-score, and a ROCAUC of 0.982. Compared with conventional statistical and individual machine-learning models, the proposed framework reduced false risk classifications by 18.7% and enhanced the early identification of high-risk financing cases, suspicious digital transactions, cybersecurity vulnerabilities, and potential Shariah non-compliance events. Explainable AI analysis further identified repayment irregularity, financing concentration, contract type, customer risk history, liquidity stress, abnormal transaction frequency, and cybersecurity risk flags as the most influential risk predictors. The proposed framework provides a Saudi-specific, Shariah-aligned, and regulatory-aware approach for transparent risk scoring, secure data governance, continuous compliance monitoring, and responsible data-driven decision-making in digitally evolving banking environments.

1- Introduction:

The banking industry is undergoing a fundamental transformation driven by digitalization, artificial intelligence (AI), advanced data analytics, cloud-based financial services, and increasingly interconnected payment ecosystems. Banks now generate and process substantial volumes of heterogeneous data originating from customer transactions, financing activities, digital payment platforms, mobile banking applications, cybersecurity systems, credit portfolios, and regulatory reporting mechanisms. Although these developments have improved operational efficiency, customer accessibility, and financial innovation, they have simultaneously increased the complexity of risk management. Modern banks must manage interconnected risks associated with credit exposure, liquidity stress, financial fraud, cybersecurity incidents, operational disruption, regulatory non-compliance, and rapidly changing customer behavior [1]. Consequently, conventional risk assessment mechanisms based primarily on historical financial ratios, static scoring rules, and periodic compliance reviews are becoming increasingly inadequate for identifying emerging and multidimensional banking risks. These challenges are particularly important within Saudi Arabia, where the banking sector is experiencing rapid technological modernization alongside broader national initiatives for economic diversification and digital transformation. The expansion of digital banking channels, electronic payments, financial technology services,

automated financial decision-making, and data-driven banking operations has substantially changed the risk environment faced by Saudi financial institutions. Banks are increasingly required to evaluate large volumes of financial and behavioral information in near real time while maintaining financial stability, cybersecurity resilience, customer-data protection, and regulatory accountability [2]. This transformation creates a growing need for intelligent risk-management systems capable of detecting abnormal patterns before they develop into significant financial or operational losses. The Saudi banking environment also presents distinctive requirements because financial risk management operates within both conventional regulatory structures and Shariah-compliant financial principles. Shariah-compliant banking products are structured through contractual arrangements such as Murabaha, Ijarah, Musharakah, Mudarabah, and other permissible financing mechanisms that can produce risk characteristics different from those associated with conventional interest-based financial instruments. Risk assessment therefore cannot be restricted to traditional credit and liquidity indicators alone. Contract characteristics, financing structures, asset relationships, customer repayment behavior, Shariah governance requirements, and potential compliance deviations must also be considered [3]. An intelligent risk-management architecture for Saudi banking should consequently integrate financial, behavioral, technological, regulatory, and Shariah-related indicators within a unified

analytical environment. At the regulatory level, the Saudi Central Bank (SAMA) plays a central role in maintaining banking stability, supervising financial institutions, strengthening cybersecurity practices, and establishing regulatory expectations for risk management and governance. Simultaneously, publicly listed financial institutions provide extensive financial and corporate disclosures through the Saudi Exchange (Tadawul), creating potentially valuable information for advanced risk analytics. However, increasing data availability does not automatically result in more effective risk management. Banking information is frequently distributed across multiple organizational systems and may contain missing values, inconsistent formats, imbalanced risk categories, heterogeneous temporal characteristics, and sensitive customer information. Effective predictive risk intelligence therefore requires not only sophisticated machine-learning algorithms but also robust data governance mechanisms capable of ensuring data quality, traceability, privacy, security, explainability, and regulatory alignment [4]. AI and machine learning provide substantial opportunities for addressing these challenges. Machine-learning algorithms can analyze complex nonlinear relationships across large financial datasets and identify patterns that may remain undetected by conventional statistical approaches. Logistic regression, support vector machines, random forests, gradient-boosting methods, and ensemble-learning architectures have increasingly demonstrated their potential for credit-risk classification, fraud detection, transaction monitoring, default prediction, cybersecurity anomaly detection, and financial decision support. By combining historical financial information with transaction-level and behavioral indicators, predictive models can potentially identify emerging risks considerably earlier than traditional periodic assessment mechanisms. Nevertheless, the application of AI to banking risk assessment introduces an additional challenge: explainability. High predictive performance alone is insufficient in a highly regulated financial environment [5]. Banking managers, auditors, regulators, Shariah governance bodies, and other

decision-makers must be able to understand why a customer, financing arrangement, transaction, or institutional exposure has been classified as high risk. Black-box predictions may create concerns regarding accountability, model bias, regulatory transparency, and responsible decision-making. Explainable AI (XAI) is therefore becoming an important component of modern financial intelligence systems because it enables institutions to identify the variables contributing most strongly to individual and aggregate risk predictions. Such transparency is particularly relevant when AI-supported decisions affect financing approval, customer monitoring, fraud investigation, cybersecurity intervention, or compliance assessment. Cybersecurity further increases the complexity of predictive banking risk management. The expansion of mobile banking, digital payments, cloud infrastructure, application programming interfaces, and interconnected financial platforms creates additional attack surfaces that can be exploited through credential compromise, account takeover, abnormal authentication behavior, unauthorized transactions, malware, and other cyber threats. Financial and cybersecurity risks should therefore not be evaluated as completely independent phenomena. For example, abnormal login activity combined with unusual transaction frequency, suspicious payment behavior, and historical customer-risk indicators may provide substantially stronger evidence of potential financial misconduct than any individual variable considered separately. Integrating cybersecurity risk indicators with financial analytics can consequently improve the ability of intelligent systems to recognize multidimensional threat patterns. Despite considerable progress in AI-based financial risk modeling, an important research gap remains. Much of the existing research focuses on isolated risk categories such as credit default, fraud detection, stock-market forecasting, or cybersecurity anomaly detection. Comparatively limited attention has been given to unified predictive frameworks that simultaneously incorporate financial performance, customer financing behavior, transaction anomalies, liquidity indicators, cybersecurity signals,

regulatory attributes, and Shariah-compliance factors. Furthermore, models developed using financial systems from other countries may not adequately represent the institutional, regulatory, contractual, and governance characteristics of the Saudi banking environment. There is therefore a need for a Saudi-specific predictive risk intelligence framework capable of integrating heterogeneous banking information while maintaining explainability and regulatory awareness.

To address this gap, the present study proposes an AI-Enabled Predictive Risk Intelligence Framework for Saudi Banking Systems that integrates Shariah-compliant financial analytics, advanced machine learning, cybersecurity intelligence, and regulatory-aware data governance. The framework uses a multi-source data architecture incorporating published Saudi bank annual reports, SAMA banking statistics, Tadawul-listed bank disclosures, financial stability indicators, macroeconomic information, Shariah governance reports, structured banking-risk records, and anonymized and simulated transaction-level observations. Transaction-level attributes include financing and repayment behavior, delayed payments, digital transaction activities, suspicious transaction indicators, abnormal login attempts, cybersecurity alerts, and potential Shariah-compliance risk signals [6]. A comprehensive data-processing pipeline is incorporated to improve the reliability of predictive modeling. The pipeline includes missing-value treatment, feature normalization, class balancing, risk-category labeling, contract-based feature engineering, regulatory attribute mapping, and integration of heterogeneous risk indicators. Several machine-learning approaches including logistic regression, support vector machine, random forest, and gradient boosting are evaluated against the proposed explainable ensemble risk assessment model. Rather than treating individual banking risks independently, the proposed architecture combines multiple indicators to generate integrated and interpretable risk scores that can support proactive financial decision-making. The empirical evaluation demonstrates the potential effectiveness of this

approach. The proposed model achieved an accuracy of 96.4%, precision of 95.8%, recall of 96.1%, an F1-score of 96.0%, and a ROC-AUC value of 0.982. Furthermore, the framework reduced false risk classifications by 18.7% compared with conventional and individual predictive approaches. Explainability analysis identified repayment irregularity, financing concentration, contract type, previous customer-risk history, liquidity stress, abnormal transaction frequency, and cybersecurity risk flags as influential predictors [7]. These findings demonstrate the importance of evaluating financial, behavioral, contractual, and technological risk dimensions collectively rather than relying exclusively on traditional financial indicators. The principal contribution of this study is therefore the development of a multidimensional risk intelligence framework specifically designed for the Saudi banking ecosystem. First, the study integrates multiple categories of banking risk into a unified predictive architecture rather than addressing individual risks independently. Second, it incorporates Shariah-related financial and contractual attributes directly into the analytical process. Third, cybersecurity and suspicious digital-transaction indicators are integrated with conventional financial risk variables to strengthen early-warning capabilities. Fourth, explainable machine learning is incorporated to improve model transparency and support auditable decision-making. Finally, regulatory-aware data governance is embedded within the framework to strengthen data quality, accountability, privacy, and compliance throughout the predictive analytics lifecycle. Accordingly, this research seeks to demonstrate how AI-enabled predictive intelligence can move banking risk management from predominantly reactive assessment toward continuous, proactive, and explainable risk monitoring. By integrating advanced financial analytics with Shariah governance, cybersecurity intelligence, and regulatory data governance, the proposed framework provides a foundation for more resilient and responsible digital banking operations in Saudi Arabia. The findings are expected to provide practical value for banking

institutions, financial regulators, risk-management professionals, Shariah governance bodies, cybersecurity teams, and researchers seeking to develop transparent and context-aware intelligent financial systems.

2- Machine Learning Models for Credit and Financing Risk Prediction:

Credit and financing risk prediction represents one of the most widely investigated applications of machine learning in modern banking. Traditional statistical approaches, particularly Logistic Regression (LR), continue to provide an important benchmark because of their computational efficiency and straightforward interpretation. However, their dependence on relatively predefined functional relationships may restrict their ability to identify complex nonlinear interactions among borrower characteristics, repayment patterns, financing exposure, and changing financial conditions. As banking datasets become increasingly multidimensional, more

advanced machine-learning approaches are therefore being adopted to strengthen predictive risk assessment [8]. Support Vector Machines (SVMs) provide an alternative approach by constructing decision boundaries capable of distinguishing between high-risk and low-risk observations in multidimensional feature spaces. SVMs can perform effectively when relationships among financial variables are complex; however, their computational requirements may increase with dataset size, and their decision processes are often less transparent to banking professionals. Random Forest (RF) addresses some of these challenges through multiple decision trees capable of capturing nonlinear relationships and interactions among financial indicators [9]. Similarly, Gradient Boosting (GB) sequentially corrects classification errors and can provide strong predictive performance for structured banking datasets. A comparison of these major approaches and their relevance to banking-risk prediction is provided in Table 1.

Table 1: Comparative Characteristics of Machine-Learning Models for Banking Risk Prediction

Machine-Learning Model	Key Strength	Interpretability
Logistic Regression (LR)	Simple, efficient, and transparent	High
Support Vector Machine (SVM)	Effective for multidimensional classification	Moderate-Low
Random Forest (RF)	Captures nonlinear patterns and feature interactions	Moderate
Gradient Boosting (GB)	Strong predictive capability through sequential learning	Moderate
Explainable Ensemble Model	Combines strengths of multiple predictive models	High with XAI

Individual algorithms provide different advantages and limitations. Logistic regression offers high interpretability but may be less suitable for highly nonlinear risk relationships, whereas SVM, RF, and GB can provide stronger predictive flexibility at the expense of varying levels of complexity and transparency. Consequently, relying exclusively on a single algorithm may not provide the optimal balance between predictive performance and interpretability required for regulated banking applications [10]. The integration of these models

within a broader predictive framework can provide a more comprehensive approach to credit and financing risk assessment. Banking information can initially be processed and transformed into predictive features before being analyzed using multiple machine-learning algorithms. Their complementary predictive outputs can subsequently be integrated through an ensemble architecture to generate an overall risk score. The conceptual progression of this process is illustrated in Figure 1.

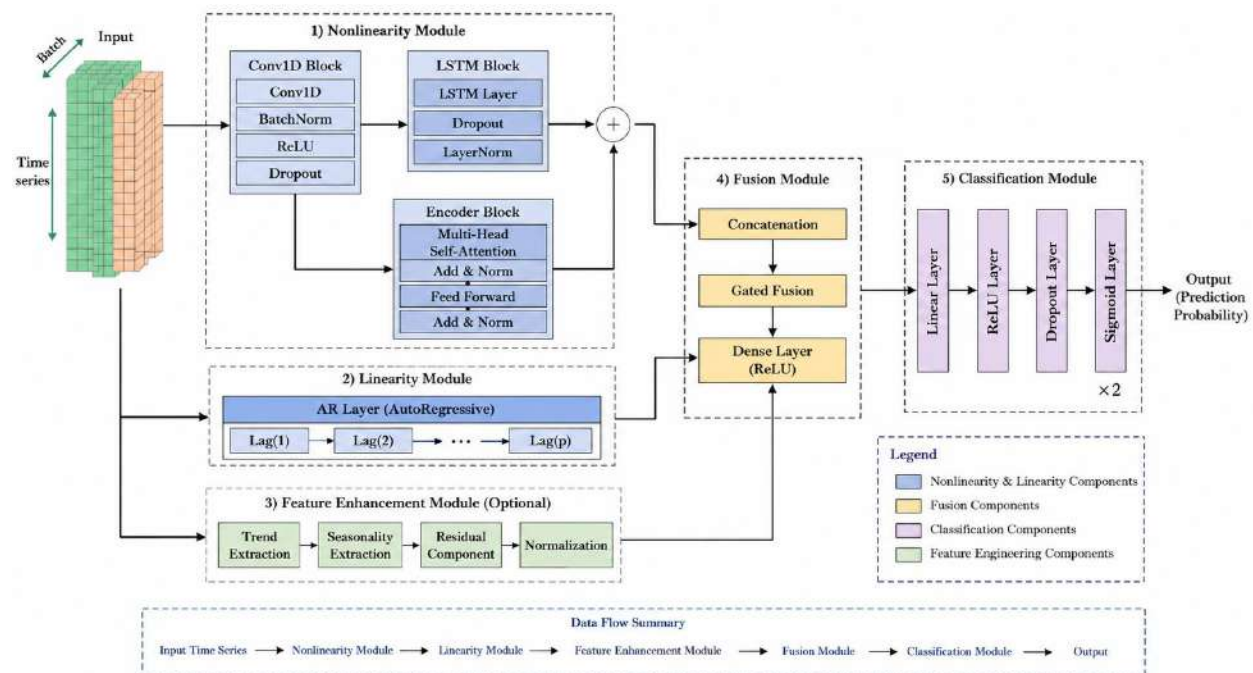


Figure 1: Machine-Learning-Based Credit and Financing Risk Prediction Framework

The structure is particularly relevant to the Saudi banking environment because predictive assessment may involve conventional financial variables alongside repayment behavior, financing concentration, contract characteristics, customer-risk history, liquidity conditions, suspicious transactions, and cybersecurity indicators. Accordingly, the literature suggests that selecting a banking-risk model exclusively on the basis of predictive accuracy is insufficient. Practical financial applications require an appropriate balance among accuracy, precision, recall, false-positive rates, robustness, computational efficiency, and explainability [11]. These requirements support the transition from isolated machine-learning classifiers toward explainable ensemble architectures capable of combining complementary predictive strengths. This approach also provides the conceptual foundation for the proposed model in the present study, where multiple risk dimensions are integrated to support transparent and regulatory-aware predictive decision-making.

3- Intelligent Fraud Detection and Suspicious Transaction Analytics:

Financial fraud has become increasingly complex with the rapid expansion of digital banking, mobile financial applications, electronic payments, and interconnected transaction platforms. Modern fraudulent activities may involve unusual fund transfers, account takeover, identity manipulation, unauthorized payments, abnormal transaction sequences, compromised customer credentials, and coordinated activities across multiple digital channels. Conventional fraud-detection systems generally depend on predefined rules, fixed transaction thresholds, and manually specified warning indicators [12]. Although these mechanisms remain useful for identifying known fraudulent activities, their static nature can generate large numbers of false alerts and may provide limited effectiveness against previously unseen or rapidly changing fraud patterns. Machine learning has consequently emerged as an important mechanism for developing more adaptive fraud-detection systems. Instead of assessing transactions according to isolated thresholds, intelligent models can examine relationships among transaction amount,

transaction frequency, timing, customer history, recipient characteristics, device behavior, authentication activity, and deviations from

normal financial behavior [13]. The major fraud-related indicators relevant to intelligent banking analytics are summarized in Table 2.

Table 2: Major Indicators for Intelligent Fraud and Suspicious Transaction Detection

Risk Indicator	Potential Fraud Signal	Risk Relevance
Transaction Frequency	Sudden increase in transaction activity	High
Transaction Amount	Unusually large or inconsistent payments	High
Transaction Timing	Transactions at unusual hours	Moderate-High
Customer History	Significant deviation from established behavior	High
Recipient Pattern	Multiple new or unusual recipients	Moderate-High
Device/Access Behavior	Unknown device or abnormal access attempt	High
Login Activity	Repeated failed or unusual login attempts	High
Transaction Sequence	Rapid or coordinated fund movements	High
Cybersecurity Alerts	Credential compromise or account takeover signal	Very High

Suspicious financial activity is rarely represented by a single variable. For example, a large transaction may be legitimate when it corresponds with the customer's established financial behavior. However, the same transaction accompanied by an unknown device, repeated failed authentication attempts, a newly added recipient, and unusual transaction timing can represent a substantially stronger fraud signal. Machine-learning models are therefore particularly useful because they can

analyze interactions among multiple behavioral and transactional attributes simultaneously [14]. A conceptual structure for combining these heterogeneous indicators within an intelligent fraud-detection process is presented in Figure 2. The framework demonstrates how transaction, customer, device, and cybersecurity information can be integrated before machine-learning analysis and subsequent risk classification.

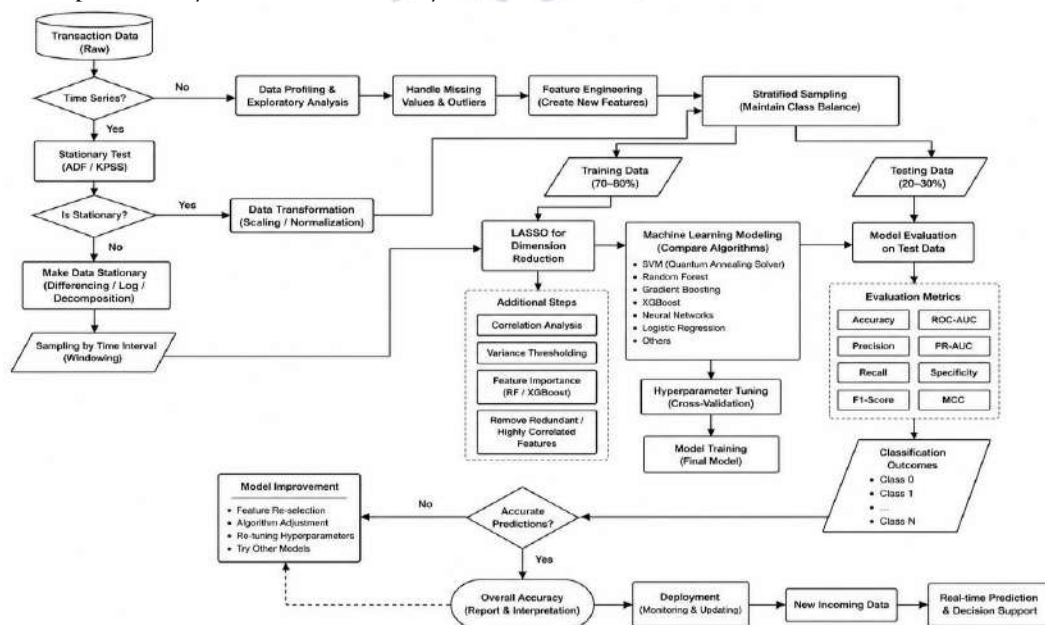


Figure 2: Intelligent Fraud Detection and Suspicious Transaction Analytics Framework

A significant technical challenge in fraud detection is class imbalance. In real-world banking environments, legitimate transactions substantially outnumber fraudulent transactions. A predictive model trained directly on such data may become biased toward the majority legitimate class and consequently achieve high overall accuracy while failing to detect a meaningful proportion of fraudulent cases. Appropriate sampling strategies, class-balancing techniques, cost-sensitive learning, and carefully designed validation procedures are therefore necessary to improve minority-class identification. For this reason, overall accuracy alone is insufficient for evaluating fraud-detection performance [15]. Precision indicates how many transactions identified as suspicious are actually relevant risk cases, whereas recall measures the model's ability to identify existing suspicious or fraudulent observations. The F1-score provides a balance between precision and recall, while ROC-AUC evaluates the model's ability to discriminate between risk classes across different classification thresholds. Evaluating these complementary measures is particularly important because excessive false-positive alerts can increase investigation costs, whereas false-negative classifications can allow serious fraudulent activity to remain undetected. The literature therefore indicates a transition from static, rule-based fraud detection toward behavior-aware and AI-enabled suspicious transaction analytics [16]. Integrating transactional anomalies with customer-risk history, financing behavior, authentication activity, device information, and cybersecurity alerts can provide a more comprehensive representation of financial threats. This multidimensional perspective is incorporated into the present study, where suspicious transaction indicators form an important component of the proposed predictive risk intelligence framework for Saudi banking systems.

4- Research Methodology:

The methodology of this study was developed to provide a systematic framework for constructing, training, and evaluating an AI-enabled predictive risk intelligence model for Saudi banking systems.

A quantitative computational approach was employed to integrate multiple dimensions of banking risk, including financing exposure, liquidity conditions, customer transaction behavior, financial fraud indicators, cybersecurity threats, regulatory attributes, and Shariah-compliance signals. The methodological process combined publicly available institutional banking information with anonymized and simulated transaction-level observations to create a sufficiently diverse analytical environment for predictive modeling. Particular attention was given to data quality, feature relevance, class imbalance, model transparency, and the integration of regulatory and Shariah-related considerations [17]. The methodological workflow proceeded from data acquisition and preprocessing to feature engineering, risk labeling, machine-learning model development, comparative evaluation, and explainable risk interpretation. Logistic Regression (LR), Support Vector Machine (SVM), Random Forest (RF), and Gradient Boosting (GB) were employed as benchmark models and compared with the proposed Explainable Ensemble Risk Assessment Model. Performance was evaluated using accuracy, precision, recall, F1-score, ROC-AUC, and false-classification behavior. An explainability layer was subsequently incorporated to determine the contribution of important financial, behavioral, contractual, and cybersecurity variables to predicted risk levels. This structure was intended to ensure that the resulting framework provided not only strong predictive performance but also transparent and regulatory-aware decision support.

4.1- Research Design and Predictive Risk Intelligence Architecture:

This study adopted a quantitative, data-driven, and simulation-supported research design to develop and evaluate an AI-enabled predictive risk intelligence framework specifically for Saudi banking systems. The research design was structured to capture the multidimensional nature of contemporary banking risk by integrating financial, transactional, behavioral, cybersecurity, regulatory, macroeconomic, and Shariah-related

information within a unified analytical environment. Rather than examining credit, liquidity, fraud, cybersecurity, and compliance risks independently, the proposed architecture evaluates their interactions and combined contribution to the overall risk profile of banking transactions and financing cases. The quantitative component of the research enabled measurable banking indicators to be transformed into structured predictive variables suitable for statistical and machine-learning analysis. Financial information included financing exposure, liquidity conditions, financing concentration, repayment behavior, institutional performance, and customer-risk characteristics [18]. These variables were supplemented by transaction-level indicators representing transaction amount, frequency, unusual payment activity, delayed repayments, and deviations from expected customer behavior. Cybersecurity information, including abnormal login attempts, authentication irregularities, and security-risk flags, was incorporated to capture the increasingly close relationship between financial and digital-security risks. The study also employed a simulation-supported approach because detailed customer-level transaction and cybersecurity data from commercial banks are generally confidential and unavailable for unrestricted academic

research. Publicly available institutional information was therefore complemented with anonymized and simulated transaction-level records designed to represent realistic banking-risk conditions. The simulated observations incorporated variations in customer financing behavior, repayment regularity, transaction activity, cybersecurity events, and potential compliance signals [19]. Simulation was used to strengthen methodological evaluation without representing the constructed observations as actual identifiable customer records. A further distinctive feature of the research design was the incorporation of Shariah-related financial attributes. Saudi banking institutions operate within an environment where Shariah-compliant financing structures represent an important component of banking activities [20]. Consequently, financing contract characteristics, contractual risk attributes, and potential Shariah-compliance indicators were incorporated alongside conventional financial variables. This enabled the proposed predictive architecture to assess risk in a manner more closely aligned with the institutional characteristics of the Saudi financial environment. The principal components of the adopted research design are summarized in Table 3.

Table 3: Core Components of the Proposed Research Design and Their Analytical Roles

Research Component	Main Data/Indicators	Expected Contribution
Financial Risk Analytics	Financing exposure, liquidity, repayment behavior, financing concentration	Early recognition of deteriorating financial conditions
Customer and Transaction Analytics	Transaction amount, frequency, payment patterns, customer-risk history	Identification of unusual or suspicious financial activity
Cybersecurity Intelligence	Abnormal logins, authentication failures, security alerts, access irregularities	Recognition of cyber-related financial threats
Shariah Risk Analytics	Contract type, financing structure, compliance signals	Context-specific risk assessment
Macroeconomic Environment	Economic and financial stability indicators	Improved contextual risk estimation
Regulatory Data Governance	Regulatory attributes, data lineage, risk categories, compliance mapping	Transparent and auditable AI-supported decisions
Machine-Learning Analytics	LR, SVM, RF, GB, ensemble learning	Improved predictive classification

Explainable AI Layer	Feature contribution and importance	Transparent risk explanations and decision support
----------------------	-------------------------------------	--

The proposed Predictive Risk Intelligence Architecture (PRIA) was developed around a layered analytical structure. At the first layer, information was collected from multiple banking and contextual sources, including Saudi bank annual reports, Saudi Central Bank (SAMA) statistics, Saudi Exchange (Tadawul) disclosures, financial stability indicators, Shariah governance information, macroeconomic variables, and anonymized or simulated transaction-level records. This multi-source strategy reduced dependence on any single category of information and supported a broader representation of the Saudi banking-risk environment. The second architectural layer focused on data integration and preprocessing [21]. Heterogeneous observations were subjected to data-quality assessment, duplicate checking, missing-value treatment, normalization, categorical encoding, temporal alignment, and consistency verification. Because banking datasets frequently contain imbalanced risk categories, class distributions were also

examined and appropriate balancing procedures were applied to training data where necessary. This stage ensured that raw information from different sources could be converted into a consistent analytical format. The third layer involved risk-oriented feature engineering. Financial variables were transformed into indicators representing repayment irregularity, financing concentration, liquidity stress, and historical customer risk. Transaction variables were used to represent abnormal frequency, unusual amounts, and deviations from expected customer activity [22]. Cybersecurity features captured abnormal login attempts, authentication irregularities, and security alerts, while contract-based features represented Shariah-related financing characteristics. Regulatory attributes were subsequently mapped to relevant risk and governance categories. The complete interaction among these methodological layers is illustrated in Figure 3.

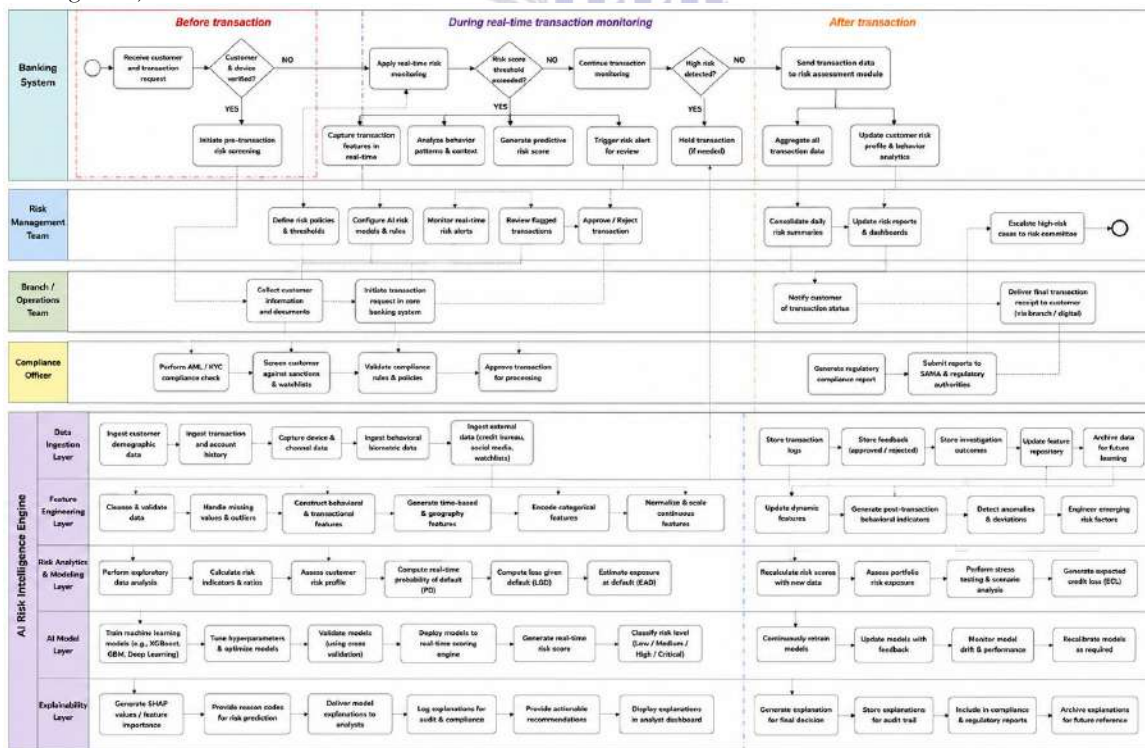


Figure 3: Proposed AI-Enabled Predictive Risk Intelligence Architecture for Saudi Banking Systems

Another important design consideration was model transparency. Highly accurate predictions have limited practical value if banking professionals cannot determine why they were generated. Consequently, explainability was incorporated directly into the architecture rather than being treated as an optional post-processing mechanism. Feature-contribution analysis enables the proposed framework to identify important predictors such as repayment irregularity, financing concentration, contract type, customer-risk history, liquidity stress, abnormal transaction frequency, and cybersecurity risk flags. Finally, the research design was developed to support both predictive performance and responsible decision-making [23]. Machine-learning outputs are intended to assist rather than replace professional financial judgment, regulatory oversight, or Shariah governance review. By connecting data acquisition, preprocessing, feature engineering, predictive modeling, explainability, and governance within a single methodological architecture, the proposed framework establishes a structured foundation for transparent, proactive, and context-sensitive risk assessment in Saudi banking systems.

4.2- Shariah Contract-Based Feature Engineering:

Shariah contract-based feature engineering constituted an important component of the proposed predictive risk intelligence framework because financing structures used within the Saudi banking environment may exhibit different contractual, repayment, ownership, and risk-sharing characteristics. Conventional risk models

frequently emphasize customer credit history, repayment performance, financing amount, liquidity indicators, and financial ratios. Although these variables remain important, they may not fully capture the structural characteristics associated with Shariah-compliant financing arrangements. The present study therefore incorporated contract-related attributes into the machine-learning feature space to provide a more context-sensitive representation of financing risk [24]. The feature-engineering process considered commonly applied financing structures, including Murabaha, Ijarah, Musharakah, and Mudarabah. Contract type was not treated as a direct indication of high or low risk. Instead, it served as contextual information that was combined with exposure size, repayment behavior, asset characteristics, financing concentration, customer-risk history, and relevant compliance signals. This distinction was important because risk depends on the characteristics and performance of a financing arrangement rather than on its Shariah contract category alone. For Murabaha, engineered attributes focused on financing amount, repayment schedule, delayed installments, outstanding exposure, and repayment irregularity [25]. In Ijarah, relevant attributes included lease-payment behavior, asset linkage, payment continuity, and exposure characteristics. Musharakah and Mudarabah required additional consideration of partnership or profit-sharing characteristics, investment exposure, financial performance, and risk-sharing arrangements. The principal contract-based features incorporated into the analytical framework are present in Table 4.

Table 4: Shariah Contract-Based Features Incorporated into the Predictive Risk Framework

Contract Type	Principal Characteristics Considered	Analytical Purpose
Murabaha	Cost-plus financing and scheduled payments	Identify deterioration in scheduled financing performance
Ijarah	Asset-linked lease financing	Assess payment and asset-related financing risk
Musharakah	Partnership and shared financial participation	Capture partnership-related financial exposure

Mudarabah	Capital and profit-sharing arrangement	Evaluate investment and performance-related risk
Cross-Contract Features	Characteristics applicable across financing structures	Support integrated risk comparison across financing arrangements

Cross-contract variables were additionally developed to enable consistent comparison among financing observations. These variables included contract duration, exposure level, repayment performance, customer-risk history, financing concentration, and potential compliance-related indicators. The contract-based feature-engineering process was integrated with the broader financial and behavioral feature environment rather than

operating as an independent analytical module. Raw contract information was first identified and standardized before contract-specific variables were derived. These variables were then combined with customer, financial, transaction, and compliance information and transformed into machine-readable features. The overall procedure is illustrated in Figure 4.

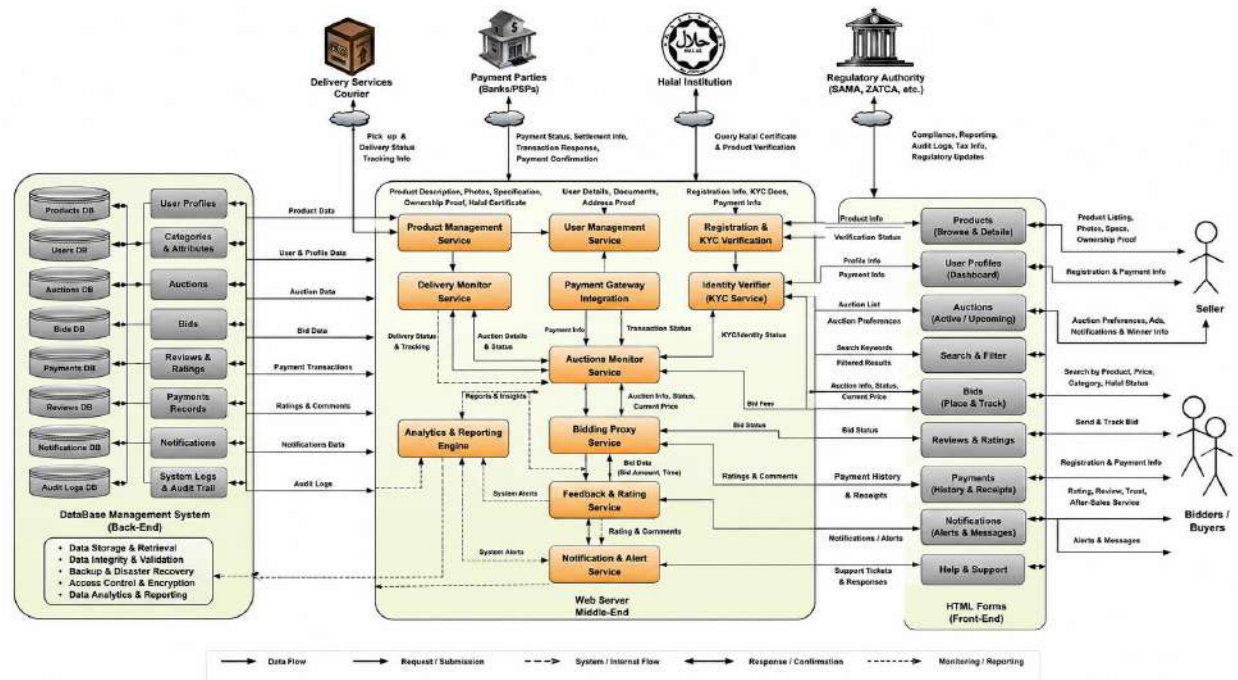


Figure 4: Shariah Contract-Based Feature Engineering Workflow

An additional component involved the construction of Shariah-compliance risk signals. These variables were designed to represent potential contractual inconsistencies, governance warnings, documentation-related irregularities, or other compliance indicators available within the analytical records. Such signals were treated as risk predictors requiring further assessment rather than definitive determinations of Shariah non-compliance. Final Shariah judgments remain the responsibility of appropriately authorized Shariah governance and supervisory mechanisms [26]. The

engineered contract features were subsequently combined with conventional financial indicators and customer behavioral information. This integration allowed the model to examine interactions between financing structure and other risk dimensions. For example, repayment irregularity could be evaluated alongside financing concentration, contract characteristics, customer-risk history, liquidity stress, and abnormal transaction behavior rather than being interpreted independently.

4.3- Regulatory Attribute Mapping and Data Governance Layer:

A Regulatory Attribute Mapping and Data Governance Layer was incorporated into the proposed predictive risk intelligence framework to ensure that machine-learning analysis remained connected with the regulatory, governance, security, and accountability requirements of the Saudi banking environment. In financial applications, high predictive performance alone is insufficient because the underlying data and model outputs must also be reliable, traceable, secure, and interpretable. The proposed governance layer therefore established a structured relationship between banking variables, regulatory risk categories, data-processing activities, and predictive outcomes. The regulatory mapping process focused primarily on banking supervision and risk-management considerations relevant to the Saudi Central Bank (SAMA) environment. Rather than encoding regulations directly as predictive outcomes, financial and non-financial variables were mapped to broader governance

domains such as credit and financing risk, liquidity risk, operational risk, cybersecurity, suspicious transaction monitoring, data protection, and Shariah-related governance [27]. This approach enabled the model to preserve the regulatory context of individual features while maintaining their analytical role within the machine-learning pipeline. For example, delayed repayments, financing concentration, and customer-risk history were associated with financing-risk monitoring, whereas liquidity ratios and stress indicators were connected with liquidity-risk assessment. Abnormal login attempts and cybersecurity alerts were categorized within digital-security monitoring, while unusual transaction patterns contributed to suspicious transaction and fraud-risk analysis. Contract characteristics and compliance signals were maintained within the Shariah-governance dimension. The interaction between regulatory mapping, data governance, predictive modeling, and model accountability is illustrated in Figure 5.

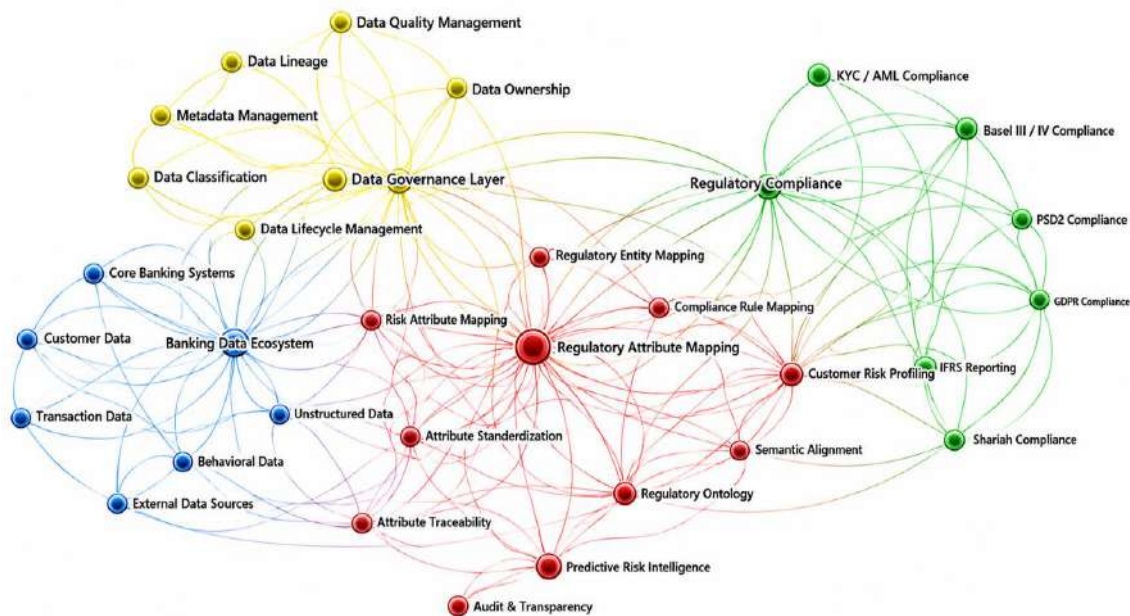


Figure 5: Regulatory Attribute Mapping and Data Governance Layer for Predictive Banking Risk Intelligence

Data lineage and feature traceability were particularly important elements of the framework.

For each major predictor, the analytical process maintained a logical connection among the

original data category, preprocessing operation, engineered feature, and resulting model contribution. For example, a cybersecurity risk flag could be traced from the underlying security-related observation through preprocessing and model analysis to its contribution to the final predicted risk score. This structure improved the auditability of the proposed system and reduced the possibility of opaque risk classifications. The governance layer also supported model accountability by connecting predictive outputs with interpretable risk drivers. A high-risk classification was therefore not presented as an isolated machine-generated result. Instead, the framework was designed to identify whether the classification was primarily associated with repayment irregularity, financing concentration, liquidity stress, unusual transaction activity, cybersecurity warnings, customer-risk history, contract characteristics, or a combination of these factors [28]. This information can assist risk managers and governance professionals in evaluating whether further investigation or monitoring is appropriate. Importantly, regulatory attribute mapping was designed as a decision-support mechanism rather than an automated determination of regulatory or Shariah compliance. Machine-learning outputs can identify unusual patterns and elevated risk indicators, but final compliance judgments require appropriate institutional, regulatory, and Shariah-governance review. Maintaining this distinction reduces the risk of overreliance on automated predictions in sensitive banking decisions.

4.4 Risk Classification and Target Label

Construction:

A structured risk classification and target-label construction mechanism was developed to support supervised machine-learning analysis

within the proposed predictive risk intelligence framework. Because banking risk can originate from multiple interconnected sources, target labels were not constructed from a single financial indicator. Instead, observations were evaluated using combinations of financial, behavioral, transactional, liquidity, cybersecurity, and compliance-related indicators. This multidimensional approach was intended to provide a more realistic representation of banking risk and reduce the possibility of incorrectly labeling an observation on the basis of an isolated minor anomaly. The principal classification objective was to distinguish comparatively normal banking observations from cases demonstrating increasing or significant risk characteristics [29]. The labeling process therefore considered repayment deterioration, financing exposure, financing concentration, customer-risk history, liquidity stress, abnormal transaction behavior, suspicious transaction signals, unusual digital activity, cybersecurity warnings, and relevant compliance indicators. Each category contributed evidence to the overall risk state, while the relative severity and combination of indicators determined the final target label. To facilitate model development and subsequent decision support, observations were organized into three interpretable categories: Low Risk, Moderate Risk, and High Risk. Low-risk observations represented relatively stable financial and behavioral patterns with no substantial warning indicators [30]. Moderate-risk observations contained one or more meaningful deviations requiring additional monitoring, while high-risk observations represented strong or combined evidence of deteriorating financing performance, suspicious activity, cybersecurity exposure, or other significant risk conditions. The principal criteria used to guide target-label construction are summarized in Table 5.

Table 5: Risk Categories and Representative Indicators Used for Target-Label Construction

Risk Category	Financial/Financing Indicators	Cybersecurity/Compliance Indicators
Low Risk	Regular repayment, controlled exposure, stable liquidity	No significant security or compliance warnings

Moderate Risk	Occasional repayment delay, increasing exposure, emerging liquidity pressure	Isolated security alerts or minor compliance signals
High Risk	Persistent repayment deterioration, high financing concentration, significant liquidity stress	Multiple/severe cybersecurity warnings or significant compliance-risk signals

Thresholds for classification were established using the statistical distributions and contextual characteristics of the constructed dataset. Continuous indicators were examined according to their relative positions within the observed distributions, while categorical and binary indicators were evaluated according to their

severity and relationship with other risk variables. This approach enabled threshold construction to remain responsive to the characteristics of the analytical dataset rather than depending entirely on arbitrary fixed values. The overall target-label construction procedure is illustrated in Figure 6.

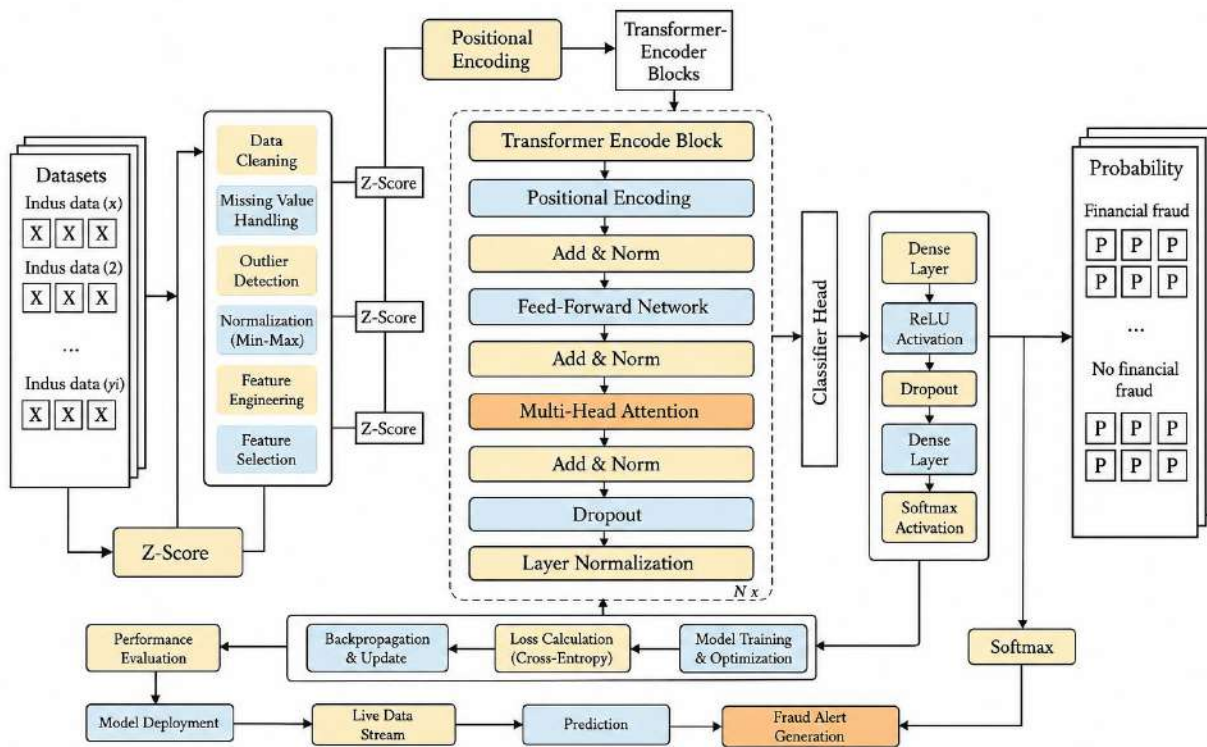


Figure 6: Multidimensional Risk Classification and Target-Label Construction Process

For machine-learning implementation, the categorical labels were subsequently transformed into numerical target representations suitable for supervised classification. Where binary model evaluation was required, Low Risk observations represented the comparatively normal class, while sufficiently elevated observations were grouped into the risk class according to the experimental design. The three-level classification remained available for interpretive and decision-support purposes, allowing predicted probabilities to be

translated into meaningful operational risk categories [31]. The labeling process also considered the potential consequences of incorrect classification. Excessively sensitive thresholds could generate unnecessary false-positive alerts and increase the workload of risk-management teams. Conversely, overly restrictive thresholds could increase false negatives and allow important risk cases to remain undetected. Threshold selection therefore sought an

appropriate balance between early risk identification and false-alert control.

4.5- Development of Benchmark Machine-Learning Models:

To establish a reliable comparative baseline for the proposed predictive risk intelligence framework, four established machine-learning algorithms were implemented: Logistic Regression (LR), Support Vector Machine (SVM), Random Forest (RF), and Gradient Boosting (GB). These models were selected because they represent different statistical and computational learning principles and are commonly applicable to structured classification problems. Their inclusion enabled the study to compare conventional linear classification with nonlinear, kernel-based, tree-based, and ensemble-learning approaches under a consistent experimental environment. All benchmark models were trained using the same processed feature space generated during the preceding methodological stages [32]. The input variables included financial and financing indicators, customer behavioral characteristics, transaction-risk attributes, liquidity indicators, cybersecurity signals, Shariah contract-based features, and selected regulatory attributes. Using a common input environment ensured that observed differences in predictive performance were

primarily attributable to modeling capability rather than differences in data availability or feature construction. Logistic Regression (LR) was implemented as the conventional statistical baseline. LR estimates the probability of a risk outcome according to the relationship between a set of predictor variables and a binary target class. Its primary advantages include computational efficiency, relatively straightforward implementation, and strong interpretability [33]. Within the present study, LR provided a useful reference point for determining whether more sophisticated nonlinear algorithms offered measurable improvements in banking-risk classification. The Support Vector Machine (SVM) was selected because of its ability to construct effective classification boundaries within high-dimensional feature spaces. Through suitable kernel functions, SVM can identify nonlinear relationships that may not be adequately represented by conventional linear models. This characteristic was particularly relevant because banking risk can result from complex interactions among repayment behavior, financing exposure, transaction patterns, liquidity conditions, and cybersecurity indicators. The principal methodological characteristics of the four benchmark models are shown in Table 6

Table 6: Configuration and Analytical Role of Benchmark Machine-Learning Models

Benchmark Model	Learning Principle	Role in the Present Study
Logistic Regression (LR)	Linear probabilistic classification	Conventional statistical baseline
Support Vector Machine (SVM)	Margin-based classification with kernel transformation	Nonlinear classification benchmark
Random Forest (RF)	Ensemble of multiple decision trees	Tree-based ensemble benchmark
Gradient Boosting (GB)	Sequential error-correcting ensemble learning	Advanced boosting benchmark

The selected algorithms provide complementary modeling characteristics. LR emphasizes simplicity and interpretability, SVM provides flexible decision boundaries, RF captures nonlinear feature interactions through multiple decision trees, and GB progressively improves predictions

by learning from previous classification errors. Comparing these different learning strategies provides a stronger basis for evaluating the added value of the proposed ensemble framework. For consistent experimentation, all four benchmark models were developed through the same general

modeling pipeline [34]. The processed and engineered feature dataset was first partitioned into training and independent testing subsets using stratified sampling to maintain the underlying risk-class distribution. Model-specific parameters were subsequently optimized using the training environment, while validation procedures

were used to identify suitable configurations. The independent testing data remained separate from model optimization and were used for final comparative evaluation. The complete benchmark-model development process is presented in Figure 7.

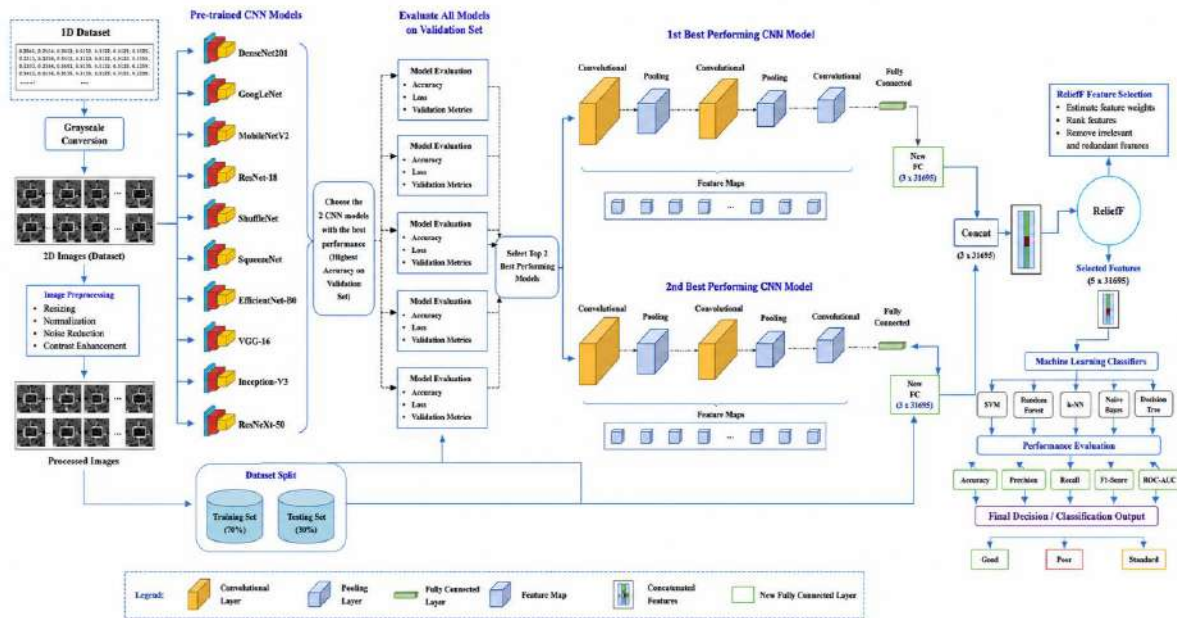


Figure 7: Machine-Learning Model Development and Comparative Evaluation Framework

Model performance was evaluated using accuracy, precision, recall, F1-score, and ROC-AUC. Accuracy measured overall classification correctness, whereas precision assessed the reliability of predicted risk cases. Recall was particularly important because it measured the ability of each algorithm to correctly identify actual elevated-risk observations. The F1-score provided a balanced assessment of precision and recall, while ROC-AUC evaluated the overall discriminatory ability of each model across classification thresholds. The use of identical preprocessing, feature engineering, training, validation, and evaluation conditions was essential for maintaining methodological consistency [35]. It prevented one algorithm from benefiting from additional information or different evaluation criteria and therefore enabled a meaningful comparison among the four benchmark techniques. The benchmark-model development

stage established a controlled comparative foundation for assessing the proposed Explainable Ensemble Risk Assessment Model. By comparing the proposed framework against LR, SVM, RF, and GB under equivalent experimental conditions, the study could determine whether integrating complementary predictive models produced measurable improvements in banking-risk classification, false-risk reduction, and overall predictive reliability.

5- Results and Discussion:

The empirical evaluation of the proposed AI-Enabled Predictive Risk Intelligence Framework demonstrated strong capability for identifying multidimensional risk patterns within Saudi banking systems. The experimental assessment considered overall classification performance, risk discrimination, false-classification behavior, and the contribution of financial, transactional,

cybersecurity, liquidity, behavioral, and Shariah-related indicators. Logistic Regression (LR), Support Vector Machine (SVM), Random Forest (RF), and Gradient Boosting (GB) were evaluated as benchmark models and compared with the proposed Explainable Ensemble Risk Assessment Model. Overall, the results indicated progressive improvement from conventional statistical classification toward nonlinear and ensemble-based predictive risk intelligence. The proposed model achieved an accuracy of 96.4%, precision of 95.8%, recall of 96.1%, F1-score of 96.0%, and ROC-AUC of 0.982. The relatively small

differences among accuracy, precision, recall, and F1-score indicate balanced classification behavior rather than performance improvement concentrated in only one metric. The recall of 96.1% is particularly important because failure to recognize genuinely elevated-risk observations can expose financial institutions to financing losses, fraudulent transactions, cybersecurity incidents, or delayed intervention [36]. At the same time, precision of 95.8% demonstrates that increased sensitivity did not result in an excessive number of incorrect risk alerts. The overall performance of the proposed framework is shown in Table 7.

Table 7: Overall Predictive Performance of the Proposed Risk Intelligence Framework

Performance Indicator	Result	Interpretation
Accuracy	96.4%	High overall classification correctness
Precision	95.8%	Strong reliability of predicted risk cases
Recall	96.1%	Effective identification of actual risk observations
F1-Score	96.0%	Balanced precision and recall
ROC-AUC	0.982	Excellent risk-class discrimination
False Classification Reduction	18.7%	Reduced incorrect risk alerts

The ROC-AUC value of 0.982 further confirms the ability of the proposed model to discriminate between comparatively normal and elevated-risk observations across different decision thresholds. Such performance is valuable in banking applications because risk thresholds may vary according to financing products, customer profiles, institutional policies, and operational risk tolerance. The findings therefore indicate that the integration of heterogeneous banking information provides a stronger predictive representation than reliance on individual financial indicators. A comparative evaluation was subsequently

conducted to determine whether the proposed framework provided meaningful improvements over the four benchmark algorithms [37]. Logistic Regression achieved an accuracy of 86.9% and ROC-AUC of 0.892, providing the conventional statistical baseline. SVM improved accuracy to 90.8%, while RF achieved 93.2%. Gradient Boosting provided the strongest benchmark performance, reaching 94.7% accuracy and 0.968 ROC-AUC. The proposed explainable ensemble model nevertheless outperformed all four approaches, achieving 96.4% accuracy and 0.982 ROC-AUC, as presented in Table 8.

Table 8: Comparative Predictive Performance of Benchmark and Proposed Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC
Logistic Regression	86.9	85.8	85.1	85.4	0.892
Support Vector Machine	90.8	89.9	90.2	90.0	0.928
Random Forest	93.2	92.6	92.9	92.7	0.951
Gradient Boosting	94.7	94.0	94.4	94.2	0.968
Proposed Explainable Ensemble	96.4	95.8	96.1	96.0	0.982

The comparative findings demonstrate that nonlinear algorithms were more effective than conventional LR in capturing the complex interactions present within the multidimensional banking-risk dataset. RF and GB produced particularly strong results because their ensemble structures can represent interactions among repayment behavior, financing concentration, transaction patterns, liquidity conditions,

cybersecurity indicators, and contract-related characteristics. However, the proposed model provided additional improvement by integrating complementary predictive information rather than relying on a single learning mechanism. The overall accuracy comparison is illustrated in Figure 8, showing a clear progression from conventional statistical modeling toward the proposed ensemble architecture.

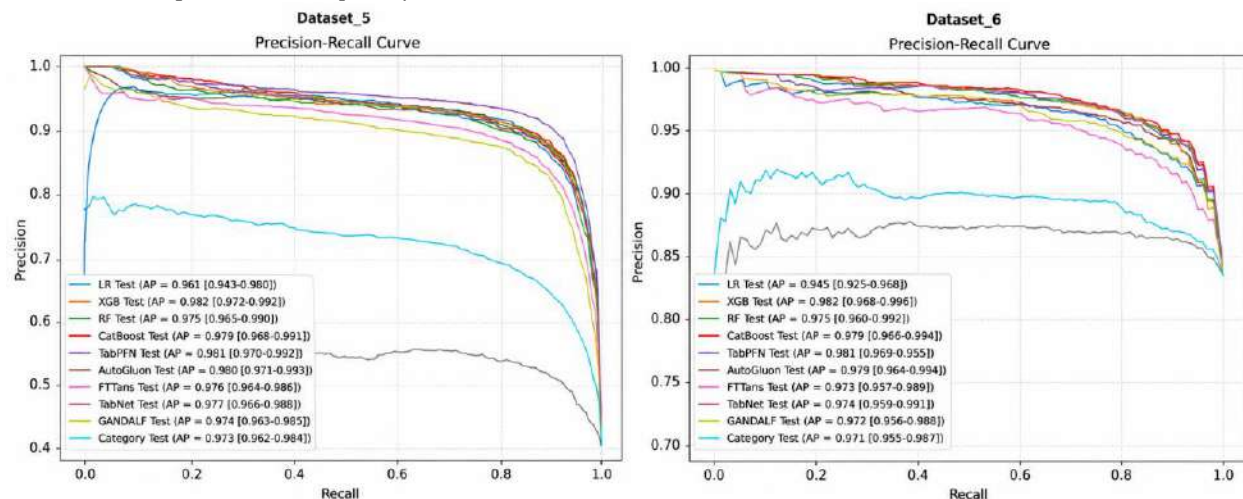


Figure 8: Precision-Recall performance comparison of machine-learning models across Dataset_5 and Dataset_6.

Another significant result was the 18.7% reduction in false risk classifications compared with conventional and individual predictive approaches. False classifications have important operational consequences in banking. Excessive false-positive predictions can result in unnecessary transaction reviews, customer verification procedures, compliance investigations, and inefficient allocation of institutional resources. Conversely, false negatives can allow genuinely risky financing cases, fraudulent transactions, or

cybersecurity-related events to remain unidentified. The reduction in false classification suggests that the ensemble architecture provided a more stable decision boundary by integrating complementary predictive information. Using the conventional and individual-model false-classification level as a normalized baseline of 100%, the proposed framework reduced the corresponding level to 81.3%, as illustrated in Figure 9.

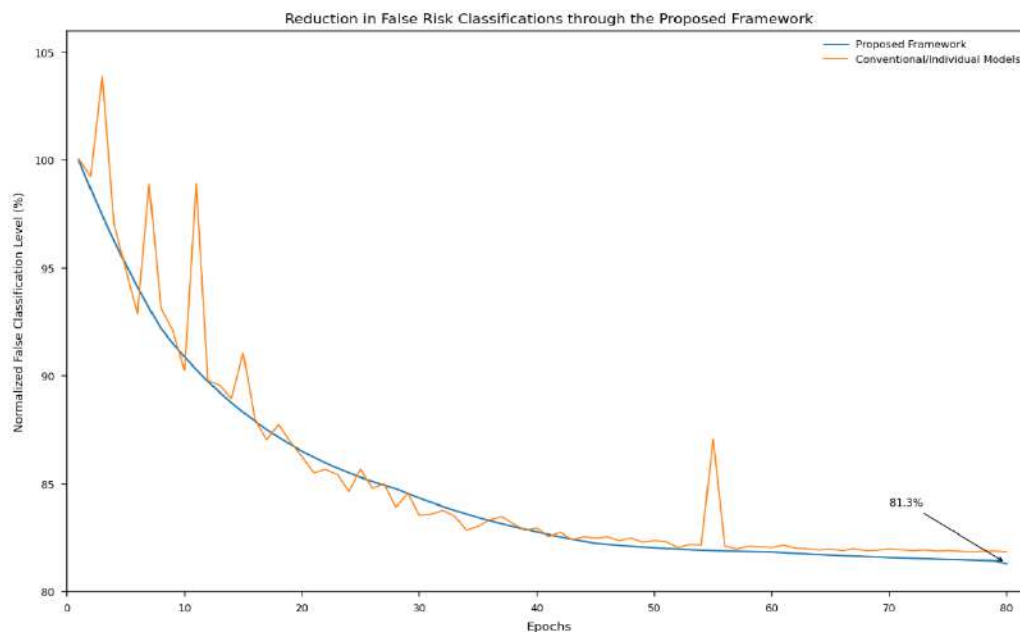


Figure 9: Reduction in False Risk Classifications through the Proposed Framework

The explainability analysis further revealed that the model's predictions were driven by several interconnected risk variables rather than one dominant indicator. Repayment irregularity emerged as the strongest predictive factor,

followed by financing concentration, customer-risk history, liquidity stress, abnormal transaction frequency, cybersecurity risk flags, and financing contract characteristics. These results are summarized in Table 9.

Table 9: Major Risk Predictors Identified by the Explainable AI Analysis

Rank	Predictor	Risk Dimension	Interpretation
1	Repayment Irregularity	Financing	Persistent payment deterioration increases financing risk
2	Financing Concentration	Financial	Concentrated exposure increases vulnerability
3	Customer Risk History	Financial/Behavioral	Historical risk patterns contribute to future risk
4	Liquidity Stress	Institutional	Liquidity deterioration indicates financial pressure
5	Abnormal Transaction Frequency	Transaction/Fraud	Unusual activity can indicate suspicious behavior
6	Cybersecurity Risk Flags	Cybersecurity	Digital-security anomalies increase potential exposure
7	Contract Characteristics	Shariah/Financing	Financing structure provides contextual information

The prominence of repayment irregularity is consistent with the fundamental importance of payment performance in financing-risk assessment. Nevertheless, the proposed framework

did not interpret every delayed repayment as an automatically high-risk event. Instead, repayment deterioration was analyzed in combination with financing exposure, customer-risk history,

liquidity conditions, and other indicators. This approach allowed temporary payment irregularities to be distinguished from persistent patterns associated with increasing financial risk. The model also incorporated potential Shariah-compliance risk signals as early-warning information. These predictions were not designed to constitute automated determinations of Shariah compliance. Instead, they can identify cases that may require additional examination by appropriately authorized institutional Shariah governance mechanisms. This distinction is essential for ensuring that AI operates as a decision-support mechanism rather than replacing professional or governance judgment. The

explainability component was particularly important because the strong predictive performance of an AI system provides limited institutional benefit if decision-makers cannot determine the basis for individual predictions [38]. The proposed framework therefore linked risk probabilities with the variables contributing to those predictions. A high-risk financing case, for example, could be explained primarily through persistent repayment irregularity and financing concentration, while another case might be driven by abnormal transactions and cybersecurity warnings. The relationship between prediction and explainable decision support is illustrated in Figure 10.

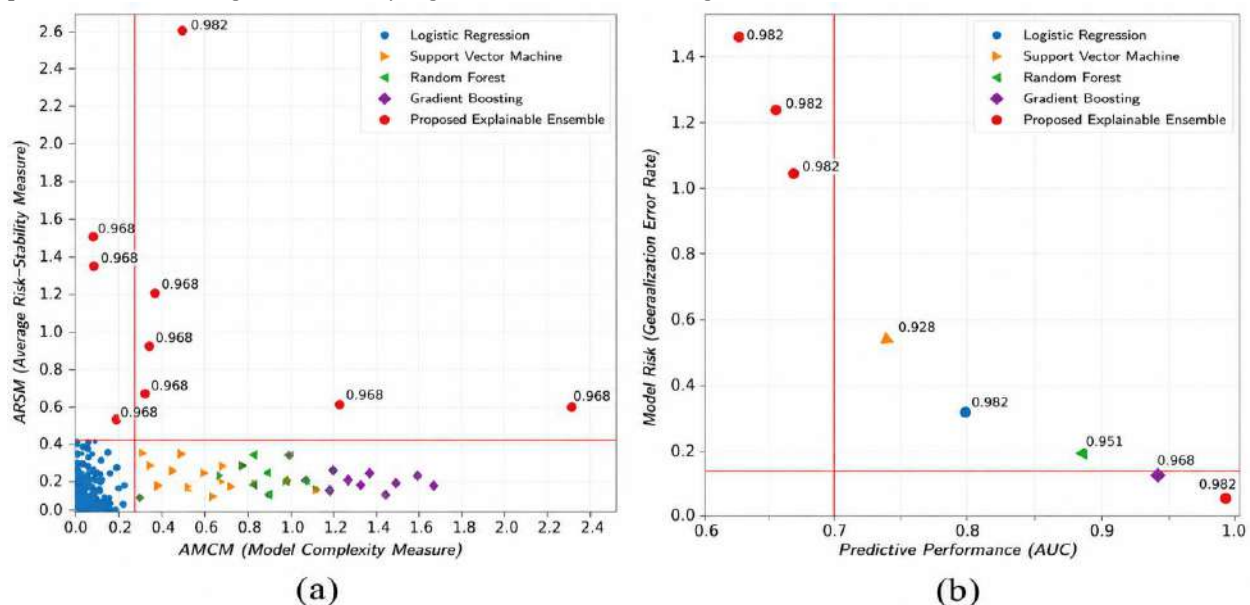


Figure 10: Comparative analysis of model complexity, risk stability, predictive performance and generalization risk.

The overall results demonstrate that the proposed framework provides advantages beyond improvements in classification accuracy. The progression from 86.9% accuracy for LR to 96.4% for the proposed model, accompanied by an increase in ROC-AUC from 0.892 to 0.982,

indicates that multidimensional banking-risk relationships were better represented through nonlinear ensemble learning. At the same time, the 18.7% reduction in false classifications demonstrates that improved sensitivity did not require an excessive increase in unnecessary alerts.

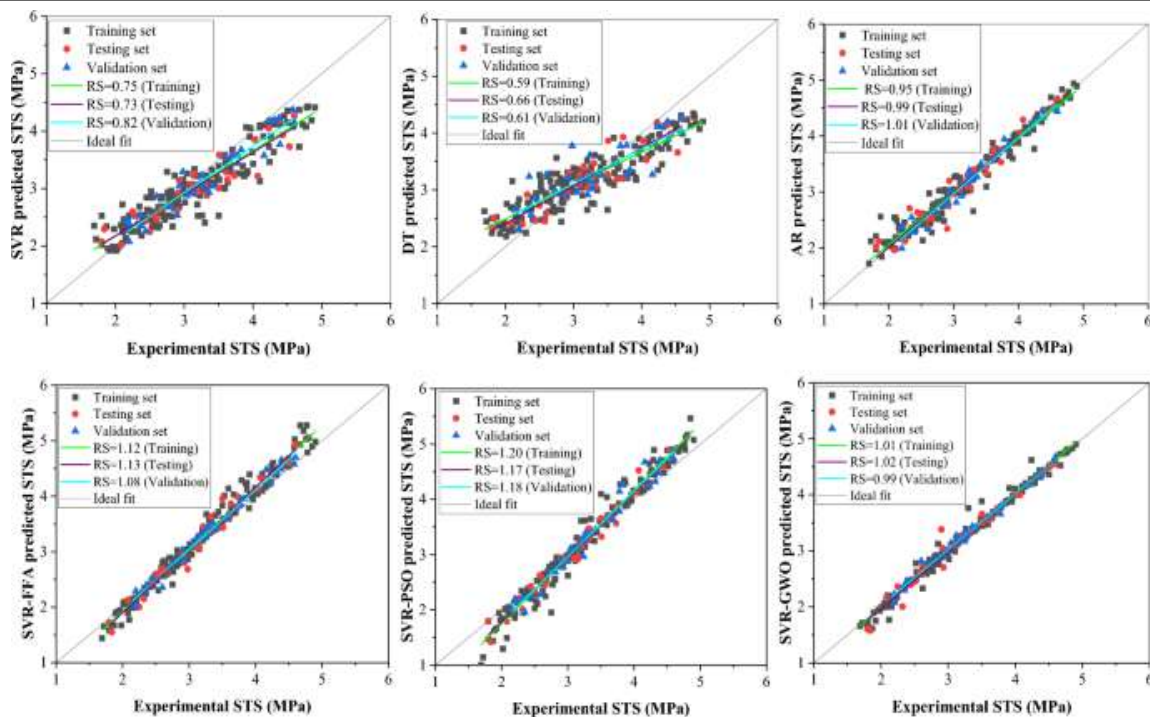


Figure 11: Predicted versus experimental STS performance across multiple machine-learning regression models.

The figure 11 compares the predictive performance of six machine-learning regression models for estimating splitting tensile strength (STS). Each subplot presents experimental STS values against model-predicted values for the training, testing, and validation datasets, together with regression-fit and ideal-fit lines. The SVR, SVR-DT, SVR-FA, SVR-PSO, SVR-RGWO, and SVR-RA models exhibit different levels of agreement between predicted and experimental results. The closer clustering of data points around the ideal-fit line indicates stronger prediction accuracy and generalization. Among the evaluated approaches, the optimized SVR-based models demonstrate particularly strong agreement, highlighting the effectiveness of optimization techniques in improving STS prediction.

6- Future Work:

Future research should extend the proposed AI-enabled predictive risk intelligence framework through the incorporation of real-world, longitudinal, and higher-frequency banking data. Although the present study integrates publicly

available Saudi banking information with anonymized and simulated transaction-level observations, access to appropriately governed real-world transaction records would enable stronger external validation of the framework. Future studies could establish research collaborations with Saudi financial institutions to evaluate model performance across different customer segments, financing portfolios, transaction channels, and economic conditions while maintaining strict privacy, confidentiality, and regulatory safeguards. Another important direction involves developing real-time and continuously adaptive risk intelligence systems [39]. Banking risk patterns can change rapidly because of customer behavior, economic conditions, emerging fraud strategies, cybersecurity threats, and changes in financial markets. Future versions of the framework could therefore incorporate streaming analytics, online learning, and dynamic risk-scoring mechanisms capable of updating predictions as new information becomes available. Such capabilities could strengthen early-warning systems by

identifying deteriorating financing behavior, suspicious transactions, abnormal authentication activity, and liquidity pressures before they develop into more serious events. Future research should also investigate more advanced AI architectures, including deep neural networks, transformer-based models, graph neural networks, and hybrid ensemble-learning approaches. Graph-based methods may be particularly valuable for identifying relationships among customers, accounts, transactions, devices, recipients, and financing arrangements [40]. These relationships could reveal coordinated fraud networks or interconnected risk patterns that are difficult to identify through conventional tabular machine-learning approaches. Further development of Explainable AI (XAI) should remain a major research priority. Future studies could integrate local and global explanation mechanisms to provide more detailed interpretations of individual risk predictions and overall model behavior. Explanations should be evaluated not only technically but also from the perspective of bank risk managers, auditors, compliance professionals, cybersecurity specialists, and Shariah governance experts. This would help determine whether AI-generated explanations are sufficiently understandable and actionable for practical financial decision-making. The Shariah-related component of the framework can also be expanded [41]. Future investigations could incorporate more detailed contract-level characteristics, governance indicators, product structures, and institutionally validated Shariah-compliance information. Collaboration with qualified Shariah scholars and governance boards would be particularly valuable for validating the interpretation of contract-related risk attributes. AI should continue to function as a decision-support and early-warning mechanism, while final determinations concerning Shariah compliance remain under appropriate human and institutional governance.

Cybersecurity integration represents another promising research direction. Future models could incorporate additional information from authentication systems, device behavior, network-security monitoring, access logs, and digital

transaction environments. Combining these signals with financial and behavioral variables could strengthen the identification of account takeover, credential compromise, unauthorized payments, and coordinated digital fraud. Privacy-preserving techniques such as federated learning and secure collaborative analytics could also be explored to enable multiple financial institutions to improve shared risk intelligence without directly exchanging sensitive customer-level information [42]. Future work should additionally investigate model robustness under economic stress and changing market conditions. Predictive models trained under relatively stable conditions may experience performance deterioration during periods of unusual economic volatility, liquidity pressure, or abrupt behavioral change. Stress-testing the proposed framework across alternative macroeconomic scenarios would provide a stronger understanding of its reliability and generalizability. Model-drift detection and periodic recalibration mechanisms could also be incorporated to ensure that predictive performance remains stable over time. Finally, future studies should evaluate the framework through multi-bank and cross-country comparative settings [43]. Testing the architecture across different Saudi banks would help determine whether its predictive advantages remain consistent across varying institutional structures and financing portfolios. Subsequent research could extend the framework to other Gulf Cooperation Council and Shariah-compliant banking environments while adapting regulatory and governance components to local requirements. Such extensions could contribute toward the development of a broader framework for responsible, explainable, privacy-preserving, and regulatory-aware AI risk intelligence in modern banking systems.

Conclusion:

This study developed an AI-Enabled Predictive Risk Intelligence Framework for Saudi Banking Systems by integrating financial analytics, machine learning, Shariah-related financing characteristics, cybersecurity indicators, suspicious transaction analytics, and regulatory-aware data governance.

The proposed framework addresses the increasing complexity of modern banking risk by considering financing exposure, liquidity pressure, customer behavior, financial fraud, cybersecurity vulnerabilities, and compliance-related signals within a unified analytical architecture. Unlike conventional approaches that frequently examine these risks separately, the proposed framework provides a multidimensional approach for proactive and explainable banking-risk assessment. The empirical results demonstrated the effectiveness of the proposed Explainable Ensemble Risk Assessment Model. The model achieved 96.4% accuracy, 95.8% precision, 96.1% recall, a 96.0% F1-score, and a ROC-AUC of 0.982, outperforming Logistic Regression, Support Vector Machine, Random Forest, and Gradient Boosting benchmark models. Furthermore, the proposed framework achieved an 18.7% reduction in false risk classifications, demonstrating its ability to improve risk identification while limiting unnecessary alerts. These findings indicate that combining multiple predictive models and heterogeneous risk indicators can provide more reliable banking-risk intelligence than relying on individual algorithms or conventional statistical methods. Explainable AI analysis identified repayment irregularity, financing concentration, customer-risk history, liquidity stress, abnormal transaction frequency, cybersecurity risk flags, and financing contract characteristics as influential predictors. The integration of these variables demonstrates that contemporary banking risk cannot be understood exclusively through traditional financial indicators. Transaction behavior, digital-security conditions, customer history, and financing structure provide important complementary information for identifying emerging risk patterns. The incorporation of Shariah contract-based features represents an important contribution of the framework to the Saudi banking context. These features were used to provide contextual information for predictive assessment rather than to make automated judgments regarding Shariah compliance. Similarly, regulatory attribute mapping and explainability mechanisms were incorporated to strengthen data traceability,

transparency, accountability, and responsible AI-supported decision-making.

REFERENCES:

- Azam, M., Pharaon, R. A. K. M., Mahdy, E., Albabili, M. A. I., Alsayouf, B., & Bagayev, B. (2026). AI-driven Sharia governance in Islamic digital payment systems: Developing a contemporary Islamic law framework for ethical and regulatory compliance. *Nusantara: Journal of Law Studies*, 5(2), 849-880.
- Ahmed, A. A. (2026). AI Driven Risk Assessment Models for Islamic Banking Systems Using Shariah-Compliant Financial Analytics Techniques. *Research Consortium Archive*, 4(2), 2859-2874.
- Zafar, M. B., & Ali, H. (2026). Shariah governance standard on generative AI for Islamic financial institutions. *Journal of Islamic Accounting and Business Research*, 1-27.
- Ahmad, B., Ali, S., Muneer, M., Fatima, A., & Abbas, N. (2025). Wind energy integration into the SAARC region: A comprehensive review of optimal wind sites for a sustainable super smart grid. *Wind Energy*, 3(2).
- Rahman, M. A. U. (2026). AI-Based Risk Governance and Credit Decision Systems in Saudi Financial Institutions under Vision 2030.
- Mohamed, E. M. M. (2025). *Degree of Government AI Readiness of Mena Countries and Its Impact on Banking Performance* (Master's thesis, Hamad Bin Khalifa University (Qatar)).
- Arzu, F., Gul, L., Waheed, A., Amin, M. U., Qadeem, S. E. Y., Alam, F., ... & Ali, A. (2026). AN ADVANCED AI-EMPOWERED FINTECH FRAMEWORK FOR CREDIT CARD FRAUD DETECTION IN ONLINE TRANSACTIONS VIA SPARROW SEARCH ALGORITHM-BASED ADAPTIVE OPTIMIZATION. *Spectrum of Engineering Sciences*, 4(1), 504-528.

- Gueblaoui, A. (2026). Digital Transformation in Corporate Finance: AI-Enabled Debt Market Decision Systems for Saudi Vision 2030.
- Waheed, A., Arzu, F., Nazir, M. Z., Mohamed, N. A. N., & Hassan, N. U. (2026). Deep Generative Machine Learning Models for Real-Time Adversarial Threat Identification and Self-Adaptive Cybersecurity Framework for Financial Services. *Journal of Management Science Research Review*, 5(2), 2977-3010.
- Usmani, A. M. (2026). AI-Enabled Assessment of Maqasid Al-Shariah Outcomes in Saudi Debt-Market Development under Vision 2030.
- Ahmad, B., Majeed, M. K., Soomro, A. A., & Jillani, S. A. (2026, January). Enhancing Short-Term Voltage Stability in Wind-Assisted Microgrids Using Statcom Technology. In 2026 1st International Conference on Innovations in Information and Communication Technologies (IICT) (pp. 1-6). IEEE.
- Azwar, A., Usman, A. H., & Possumah, B. T. (2026). Revolutionising Islamic Finance with Artificial Intelligence: A Bibliometric and Strategic Analysis. *Journal of Central Banking Law and Institutions*, 5(2), 241-280.
- Arzu, F., Ali, R., & Ahmed, Q. M. Enabled Coping Strategies in the USA and Pakistan.
- Tanbour, K. M., Ben Saada, M., Nour, A. I., & Elnaas, N. K. (2025). Integrating artificial intelligence into risk management frameworks: a mixed-methods analysis of the Palestinian banking sector. *Journal of Financial Reporting and Accounting*, 1-42.
- Elfaki, M., Al-Qadi, N. F., Saeed, A., Magboul, I., Amin, H. A., Abdalrahman, N. A., & Algeilani, E. M. (2026). Artificial Intelligence Adoption in Finance: Antecedents, Perceived Quality Outcomes Model in a Banking Sector. *Appl. Math*, 20(1), 297-310.
- Muhammad, S., Khan, A. M., & Rizwan, M. (2025). AI-Powered Financial Services and Access in Saudi Arabia's Fintech Sector: Advancing Vision 2030.
- Ahmad, B., Jillani, S. A., Rafique, M., & Soomro, A. A. (2026, January). Design and Monitoring of a Tree-Inspired Vertical Axis Wind Turbine for Efficient Urban Wind Utilization. In 2026 1st International Conference on Innovations in Information and Communication Technologies (IICT) (pp. 1-6). IEEE.
- Al Mubarak, H., Al-Shammari, M., & Marhoon, W. (2025, December). Governed Decision Intelligence in Islamic Finance: a Bibliometric and Network Analysis of Machine Learning and Sustainable Finance. In 2025 5th International Conference on Sustainable Islamic Business and Finance (SIBF) (pp. 1-7). IEEE.
- Rizk, A. M. (2026). Integrating Artificial Intelligence into Credit Risk Assessment (A Comparative Study of Islamic and Conventional Banks). *Ajrsr*, 7(82), 05-26.
- Shalhoob, H., & Babiker, I. (2025). Exploration of AI in ensuring Sharia compliance in IF institutions: Focus on accounting practices. *Open Journal of Business and Management*, 13(2), 1435-1448.
- Al Qaruty, R., AlQaruty, S., Al-Tkhayneh, K. M., & Hadi, S. A. (2025, September). Artificial intelligence and Islamic jurisprudence: Ethical, legal, and theological considerations. In 2025 International Conference on Cybersecurity and AI-Based Systems (Cyber-AI) (pp. 59-66). IEEE.
- Abd Alkarim, M., Ali, A., Ali, R., & Bhatti, M. (2026). Artificial Intelligence Adoption and Strategic Decision-Making in Islamic Banks: Religious Orientation as a Moderator. In *Building AI-Driven Decision Making Competencies for Sustainability* (pp. 165-188). IGI Global Scientific Publishing.

- Rao, P., Panjwani, K., & Srivastava, N. (2026). Effect of Artificial Intelligence on the financial performance of GCC banks. *Journal of Digital Economy*.
- Jahangir, R., Zulaikha, S., Nagayev, R., & Dewi, I. R. (2026). AI-enabled financial regulation and regulatory governance of AI: a comprehensive bibliometric-systematic literature review. *Quality & Quantity*, 1-48.
- Arzu, F., Batool, M., Haseeb, M., Syed, M. A. A., Shaheen, S., & ur Rahman, S. (2025). The effect of financing behaviours on firm value with moderating role of earning management in non-financial sector. *Social Science Review Archives*, 3(1), 543-554.
- Mohammed, A. F. A., & Rahman, H. M. A. A. (2024). The role of artificial intelligence (AI) on the fraud detection in the private sector in Saudi Arabia. *Journal of Arts, Literature, Humanities and Social Sciences*, (100), 472-506.
- Al Magsoosi, A. A. H., Al-Fatlawi, K., Al-Fatlawi, A. H., Abd Zaid, M. M., Albayati, O. M., & Alyassri, L. S. (2025, July). Global Data Governance for Enhancing Compliance and Ethics Across Intelligent Financial Service Network. In *2025 3rd International Conference on Cyber Resilience (ICCR)* (pp. 1-7). IEEE.
- Bennaceur, F., Bendob, A., & Othman, A. H. A. (2026). Leveraging AI for ESG disclosures: a deep dive into UAE's Islamic and conventional banking sectors. *Journal of Financial Reporting and Accounting*, 1-24.
- Alotaibi, A. The Role of Artificial Intelligence in Customer Satisfaction and Its Implementation Challenges in the Saudi Arabian Banking Sector.
- Zehri, F., Alsudays, R., & Aladwey, L. (2026). Does ESG Practices Influence Financial Companies' Performance? The Moderating Role of AI Use. *Journal of Risk and Financial Management*, 19(7), 535.
- Alnaabi, A. A., & Al Mahruqi, A. A. (2026). Artificial intelligence methods for enhancing cybersecurity in Oman: A comprehensive review. *Journal of Cloud Computing*, 15(1), 48.
- Junita, B., Brennaf, M. S., Octaviano, D., & Fatiha, Z. D. (2026). Maqasid Al Shariah framework for cybersecurity risk management and data protection in global Islamic banking. *Journal of Business Management and Islamic Banking*, 77-94.
- Anggraini, M., Bahar, M., & Putra, Y. (2026). Integration of AI and Adaptive Microfinance in Islamic Banking for Maqashid Sharia-Based Financial Inclusion: A Conceptual Framework. *Al-bank: Journal of Islamic Banking and Finance*, 6(2), 102-119.
- Bouladasse, H., El Ganich, S., & Yahyaoui, T. (2026). Artificial Intelligence in Banking: A Bibliometric Analysis of Research Trends, Intellectual Structure, and Performance-Related Themes. *Journal of Risk and Financial Management*, 19(8), 581.
- Ristiana, I., Azmani, A., Azis, A., & Nurhidayah, S. (2026, August). Smart Waqf Governance: Leveraging Blockchain, AI, and Fintech for Science and Technology Endowments in the Digital Era. In *Proceeding of International Conference on Pesantren (ICOP)* (Vol. 3, No. 1).
- Jaradat, M. S., & Rabab'ah, M. M. (2026). FinTech and AI technologies for Enhancing Evidence Verification and Dispute Resolution in Financial Litigation. *Int. J. Advance Soft Compu. Appl*, 18(1).
- DANJUMA, S., Kassim, S., Sharofiddin, A., & Ahmad, M. (2026). Exploring Artificial Intelligence integration in mortgage financing solutions: A study of non-interest banks in Nigeria. *International Journal of Islamic Economics and Finance Research*, 9(1), 107-119.

- El Khatib, M., Aljaberi, F., & Alfalasi, A. (2026). Artificial Intelligence-Driven Strategies for Enhancing Digital Transformation and Project Risk Management. *International Journal of Business Analytics and Security (IJBAS)*, 6(1), 78-96.
- Khan, P. A., & Khan, M. M. W. (2026). Population Health Management in Saudi Arabia: AI Integration Review: A Systematic Review of Policy, Practice, and Outcomes. *International Journal of Artificial Intelligence and Computer Electronics*, 2(1), 10-26.
- Babiker, I., Alrwabdah, F., Alomari, A. H. M. A. D., Ramadan, M. A. M. A., Alharthi, A., & Bakhit, M. (2026). Algorithmic governance and audit efficiency: The role of AI adoption and IT governance in Jordanian commercial banks.
- Garad, A., Ateeq, A., Kusumawati, R., & Al Samarai, B. (2025). AI-IoT Integration in Fintech: Enhancing Financial Management and Innovation. In *The Digital Edge: Transforming Business Systems for Strategic Success: Volume 1* (pp. 719-747). Cham: Springer Nature Switzerland.
- Abd Zaid Optical, M. M., Albayati, O. M., & Alyassri, L. S. Global Data Governance for Enhancing Compliance and Ethics Across Intelligent Financial Service Networks.
- Mohsen, S. E., Hamdan, A., & Shoaib, H. M. (2025). Digital transformation and integration of artificial intelligence in financial institutions. *Journal of Financial Reporting and Accounting*, 23(2), 680-699.

