Center for Management Science Research
ISSN: 3006-5291 3006-5283 Volume 4, Issue 3, 2026

ARTIFICIAL INTELLIGENCE–DRIVEN PREDICTIVE CYBER THREAT INTELLIGENCE IN SAUDI BANKING SYSTEMS: AN INTEGRATED FRAMEWORK FOR FINANCIAL FRAUD DETECTION, NETWORK SECURITY ANALYTICS AND TRANSACTION BEHAVIOUR MODELING

Muhammad Imran[1], Muhammad Adil[*2], Junaid Ahmad[3], Komal Tanveer[4]

[1]*Master's Program in Cybersecurity, NSA CAE-Cyber Defense Designated Program, Tandon School of Engineering, New York University, Brooklyn, New York, USA*
[*2]*Department of Commerce, University of the Punjab, Gujranwala Campus, Punjab, Pakistan*
[3]*Tun Razaq Graduate School of Business, Universiti Tun Abdul Razak, Kuala Lumpur, Malaysia*
[4]*Department of Management Sciences, NFC Institute of Engineering and Technology, Multan, Pakistan*

[1]mi2254@nyu.edu, [*2]adilmuhammadkhann@gmail.com, [3]junaidahmad244@ur.unirazak.edu.my, [4]komaltanveer605@gmail.com

DOI: https://doi.org/10.5281/zenodo.22022667

Keywords
Artificial Intelligence; Cyber Threat Intelligence; Saudi Banking Systems; Financial Fraud Detection; Network Security Analytics; Transaction Behaviour Modeling; Predictive Cybersecurity; Explainable Artificial Intelligence.

Article History
Received: 19 January 2026
Accepted: 04 March 2026
Published: 18 March 2026

Copyright @Author
Corresponding Author: *
Muhammad Adil

Abstract

The rapid digitalization of banking services in Saudi Arabia has increased operational efficiency and financial accessibility while simultaneously expanding exposure to financial fraud, cyber intrusions, account compromise, and anomalous transaction activities. This study proposes an Artificial Intelligence–Driven Predictive Cyber Threat Intelligence framework for Saudi banking systems that integrates financial fraud detection, network security analytics, and transaction behaviour modeling within a unified predictive environment. A multi-source dataset was constructed using publicly available Saudi banking indicators, institutional financial and cybersecurity disclosures, regulatory statistics, and synthetically generated anonymized transaction and network-security records. The final experimental dataset comprised 85,000 transaction and security observations characterized by 42 predictive features, including transaction amount and frequency, login behaviour, device and location anomalies, failed authentication attempts, unusual fund transfers, IP reputation indicators, network traffic patterns, account activity, and historical fraud signals. Following missing-value treatment, feature normalization, categorical encoding, class balancing, and feature selection, four benchmark algorithms Logistic Regression (LR), Support Vector Machine (SVM), Random Forest (RF), and XGBoost were developed and comparatively evaluated. Stratified 80:20 training–testing partitioning with five-fold cross-validation was employed to improve evaluation reliability. Experimental results demonstrated that XGBoost achieved the strongest overall predictive performance, with 96.8% accuracy, 96.2% precision, 95.7% recall, 95.9% F1-score, and 0.984 ROC-AUC, compared with accuracies of 84.6%, 89.3%, and 94.1% for LR, SVM, and RF, respectively. The proposed intelligence framework detected 97.1% of high-risk fraudulent transactions and

95.4% of network-security anomalies, while reducing the false-positive rate to 3.8%. Behavioural transaction analytics further improved early identification of abnormal account activities by 11.6% compared with conventional rule-based screening. Explainable AI analysis identified transaction velocity, authentication failures, device inconsistency, unusual transfer patterns, and network anomalies as the most influential risk indicators. These findings demonstrate that integrated AI-based cyber threat intelligence can substantially strengthen proactive risk detection, support real-time security decision-making, and enhance the cyber resilience of Saudi banking systems. The proposed framework provides a scalable foundation for intelligent fraud prevention, continuous network monitoring, and data-driven cybersecurity governance within rapidly evolving digital banking environments.

1- Introduction:

The rapid transformation of the global financial sector through digital banking, mobile financial services, cloud computing, open banking platforms, and real-time payment infrastructures has significantly changed the operational environment of modern banking institutions. Although these technologies have improved service accessibility, transaction efficiency, and customer experience, they have simultaneously expanded the cybersecurity attack surface of financial organizations. Banks increasingly operate within interconnected digital ecosystems involving customers, third-party service providers, payment gateways, application programming interfaces, mobile applications, cloud platforms, and distributed network infrastructures. Consequently, financial institutions face increasingly sophisticated cybersecurity risks, including financial fraud, credential compromise, unauthorized access, phishing-based account takeover, malware, network intrusion, transaction manipulation, and abnormal user activities. Traditional security mechanisms based primarily on predefined rules and static thresholds are becoming insufficient for identifying complex and rapidly evolving attack patterns. The cybersecurity requirements of the banking sector are particularly important because financial institutions process large volumes of sensitive customer, transactional, authentication, and financial information [1]. Cyberattacks against banking infrastructure can produce consequences extending beyond direct financial losses, including operational disruption, data compromise, reputational damage, regulatory violations, and deterioration of customer confidence. Contemporary cybercriminal activities are also becoming increasingly adaptive, as attackers modify their strategies to bypass conventional fraud-detection and network-monitoring mechanisms. This changing environment has created a strong requirement for security systems capable not only of detecting previously observed attacks but also of identifying emerging risk patterns before they develop into successful security incidents. Saudi Arabia provides an important context for investigating these challenges because its banking sector is undergoing substantial digital transformation. The increasing adoption of mobile banking, electronic payments, digital financial platforms, financial technology services, and interconnected banking infrastructure has created a highly data-intensive financial ecosystem. The broader transition toward a digitally enabled economy under national transformation initiatives has further increased dependence on secure and resilient financial infrastructure [2]. As banking operations become increasingly interconnected and automated, cybersecurity risk management must evolve from reactive incident detection toward proactive and predictive intelligence. Financial institutions therefore require intelligent analytical mechanisms capable of continuously evaluating transaction behaviour, network activities, authentication events, and other security indicators to identify potential risks at an early stage. Artificial intelligence (AI) and machine learning (ML) provide significant opportunities to address these requirements. Unlike conventional

rule-based approaches, AI models can learn complex relationships from large-scale heterogeneous data and recognize patterns that may not be visible through manually designed security rules. Machine-learning algorithms can analyze transaction frequency, monetary values, authentication failures, device characteristics, access behaviour, network traffic, geographical inconsistencies, and historical fraud indicators simultaneously [3]. These capabilities enable banking institutions to distinguish legitimate activities from potentially fraudulent or malicious behaviour with greater flexibility. Furthermore, predictive models can assign risk probabilities to emerging events, allowing security teams to prioritize high-risk cases and intervene before substantial financial or operational damage occurs. However, banking cybersecurity is a multidimensional problem that cannot be effectively addressed by analyzing financial fraud, network security, and customer transaction behaviour independently. A suspicious transaction may appear legitimate when evaluated exclusively through financial attributes but become highly risky when combined with unusual device access, repeated authentication failures, abnormal network activity, or significant deviation from the customer's historical behaviour. Similarly, network anomalies may provide early indications of compromised accounts or coordinated fraudulent activities. The integration of these information domains is therefore essential for developing comprehensive predictive cyber threat intelligence. Another challenge concerns the transparency of AI-driven security decisions. Highly complex predictive models may achieve superior classification performance while providing limited explanations for individual risk predictions. This limitation is particularly important in regulated financial environments, where security analysts and decision-makers need to understand why transactions, customers, devices, or network events have been classified as high risk. Explainable Artificial Intelligence (XAI) can address this challenge by identifying the variables that contribute most strongly to predictions and providing interpretable explanations of model behaviour. Integrating explainability with predictive cyber threat intelligence can therefore improve analyst confidence, model accountability, and practical decision support.

Against this background, the present study develops an Artificial Intelligence–Driven Predictive Cyber Threat Intelligence framework for Saudi banking systems, integrating financial fraud detection, network security analytics, and transaction behaviour modeling. The study constructs a multidimensional analytical environment incorporating transaction characteristics, authentication behaviour, device and location inconsistencies, network indicators, account activity, and historical fraud signals. Logistic Regression (LR), Support Vector Machine (SVM), Random Forest (RF), and XGBoost are comparatively evaluated to determine the effectiveness of conventional and advanced machine-learning approaches. Model performance is assessed using accuracy, precision, recall, F1-score, false-positive rate, and Receiver Operating Characteristic–Area Under the Curve (ROC-AUC), while explainable AI analysis is employed to determine the most influential cybersecurity risk indicators [4]. The principal contribution of this study lies in moving beyond isolated fraud or intrusion detection toward an integrated predictive intelligence architecture. By jointly analyzing financial transactions, behavioural deviations, and network-security signals, the proposed framework is designed to provide earlier and more reliable identification of cyber-financial risks. The framework also emphasizes explainability so that predictive outcomes can support security analysts rather than operate as uninterpretable automated classifications. This combination provides a more comprehensive approach to proactive cybersecurity risk management in digitally transformed banking environments. Accordingly, the study seeks to determine whether integrated AI-based analytics can improve the identification and prediction of fraudulent transactions and network-security anomalies within Saudi banking systems, identify which machine-learning model provides the strongest predictive capability, and determine which financial, behavioural, authentication, and

network indicators contribute most significantly to cyber-risk classification. Through these objectives, the research contributes a scalable and data-driven approach for strengthening fraud prevention, continuous security monitoring, predictive risk assessment, and cyber resilience across Saudi Arabia's evolving banking ecosystem.

2- Network Security Analytics and AI-Based Intrusion Intelligence:

Network security analytics represents a critical component of modern banking cybersecurity because financial attacks are frequently preceded or accompanied by suspicious network and authentication activities. Although financial fraud detection primarily evaluates transaction-level characteristics, network monitoring provides an additional intelligence layer for identifying credential compromise, unauthorized account access, malware activity, suspicious API requests, data exfiltration, abnormal communication patterns, and attempted intrusions. Integrating these indicators enables banking institutions to recognize potential cyberattacks before they develop into successful financial incidents [5]. AI-based network security analytics continuously evaluates heterogeneous information generated by banking servers, authentication systems, network devices, applications, and digital service platforms. Important indicators include network traffic volume, connection frequency, failed login attempts, source and destination characteristics, protocol usage, session duration, IP reputation, device inconsistency, and abnormal data-transfer patterns. The principal indicators incorporated into network-security intelligence and their corresponding cybersecurity implications are summarized in Table 1.

Table 1: Major Network Security Indicators for AI-Based Banking Intrusion Intelligence

Security Indicator	Analytical Characteristic	Potential Cybersecurity Risk
Network traffic volume	Sudden traffic increases/decreases	DDoS or automated attacks
Failed authentication	Repeated unsuccessful logins	Credential compromise
IP reputation	Suspicious or previously flagged IP	Unauthorized access
Connection frequency	Abnormally frequent connections	Bot or automated attack
Session characteristics	Unusual duration/activity	Session hijacking
Device inconsistency	Unknown or rapidly changing devices	Account takeover
Protocol behaviour	Irregular protocol utilization	Network exploitation
Data-transfer pattern	Unexpected outbound data movement	Data exfiltration

Traditional intrusion-detection mechanisms generally depend on predefined signatures and manually established security rules. Although such approaches remain useful for detecting previously identified attacks, their effectiveness can decrease when cybercriminals modify attack techniques or generate previously unseen patterns. Machine-learning models provide greater flexibility by learning complex relationships among network variables and estimating whether observed activities represent normal or potentially malicious behaviour. Algorithms such as Support Vector Machine, Random Forest, Gradient Boosting, and neural networks have consequently received considerable attention for automated intrusion detection and cybersecurity risk classification [6]. Deep-learning techniques have further strengthened network-security analytics by automatically extracting complex representations from high-dimensional and sequential network information. CNN-based architectures can identify localized patterns within transformed network traffic features, whereas recurrent and attention-based architectures can capture temporal dependencies among consecutive security events. These capabilities are particularly relevant to banking environments where cyberattacks may consist of multiple

interconnected activities occurring over different periods. Nevertheless, computational complexity, model interpretability, concept drift, imbalanced attack classes, and false-positive alerts remain important challenges for practical implementation. The present study therefore conceptualizes network-security analytics as an interconnected component of predictive cyber threat intelligence [7]. The complete analytical process is illustrated in Figure 1, beginning with heterogeneous network and authentication data acquisition and progressing through preprocessing, feature extraction, AI-based security analytics, cyber-risk classification, and predictive security decision support.

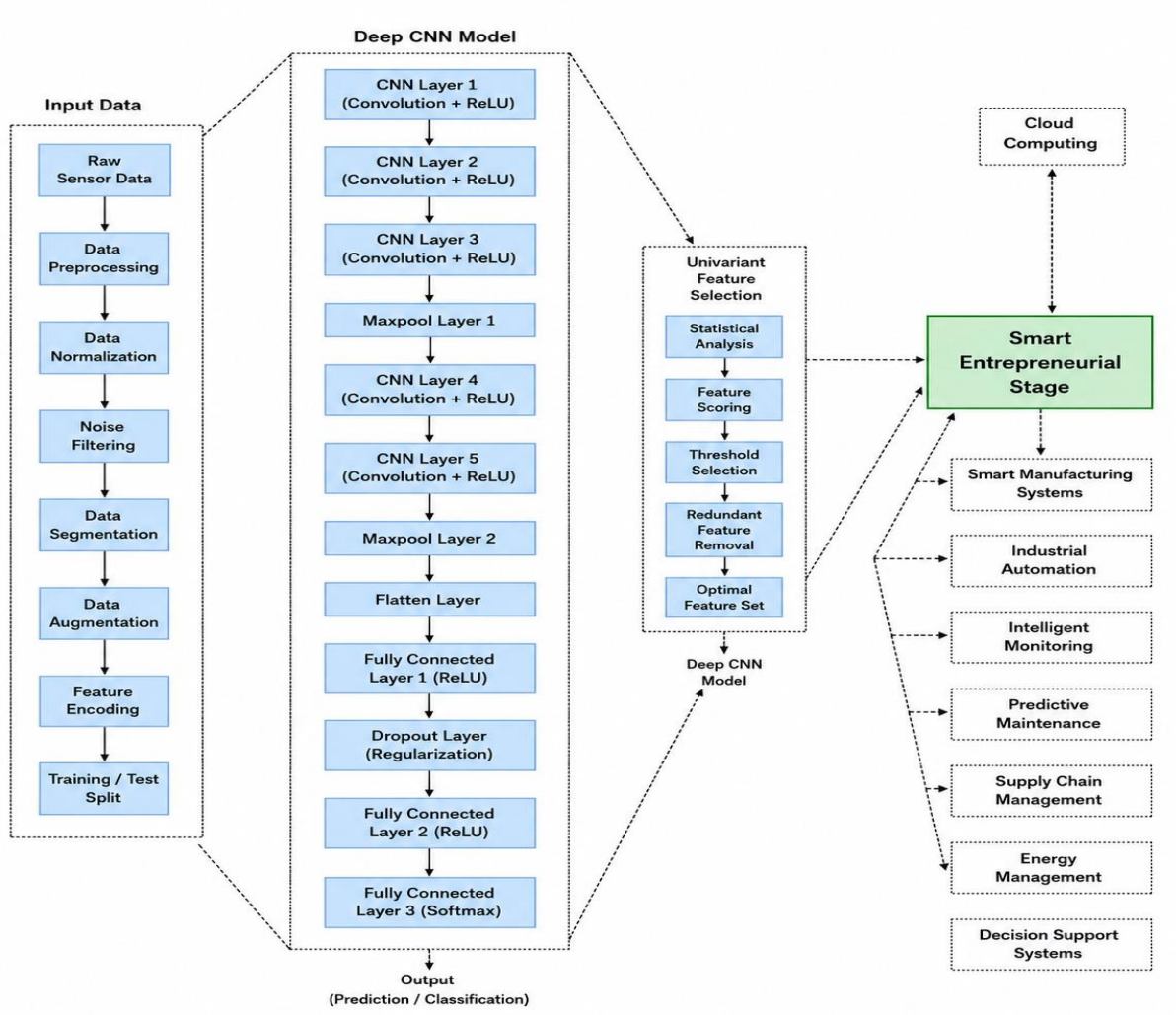


Figure 1: AI-Based Network Security Analytics and Intrusion Intelligence Framework

The AI-based network security analytics has become an essential component of intelligent cybersecurity in modern banking environments. The ability of machine-learning and deep-learning techniques to process large volumes of network, authentication, access, device, and session data provides significant advantages over conventional rule-based security mechanisms. These approaches support the identification of complex and previously unseen attack patterns while enabling continuous assessment of rapidly changing network conditions [8]. However, challenges associated with false-positive alerts, model interpretability, computational complexity, class imbalance, and evolving attack behaviour continue to influence practical implementation.

Therefore, the development of robust, adaptive, and interpretable AI-based security mechanisms remains essential for strengthening intrusion detection, improving early cyber-risk identification, and enhancing the overall resilience of increasingly interconnected digital banking infrastructures.

3- Transaction Behaviour Modeling for Early Anomaly Recognition:

Transaction behaviour modeling represents an important transition from analyzing isolated financial transactions toward understanding the normal activity profile of individual customers and banking accounts. Conventional fraud-detection mechanisms frequently depend on fixed transaction limits and predefined rules, whereas behavioural analytics evaluates whether current activity is consistent with historically observed patterns. Banking customers generally develop recognizable behavioural characteristics related to transaction amount, transfer frequency, transaction timing, commonly used devices, geographical locations, beneficiaries, authentication practices, and digital banking channels. Modeling these characteristics provides an individualized baseline against which subsequent banking activities can be evaluated. AI-based behavioural analytics can continuously compare incoming transactions with historical account patterns and calculate the degree of deviation from expected behavior [9]. A single high-value transaction, for example, may represent legitimate customer activity and therefore provide insufficient evidence of fraud. However, when a high-value transfer occurs from an unfamiliar device, at an unusual time or location, following repeated authentication failures, and involves a previously unseen beneficiary, the combined behavioural deviation can indicate substantially greater cybersecurity risk. The major behavioural variables and their potential relevance to anomaly recognition are summarized in Table 2.

Table 2: Major Transaction Behaviour Indicators for AI-Based Anomaly Recognition

Behavioural Indicator	Normal Behaviour Profile	Potential Anomalous Pattern
Transaction amount	Consistent historical range	Unusually high/irregular value
Transaction frequency	Regular activity frequency	Sudden transaction burst
Transaction timing	Typical banking periods	Unusual late/irregular activity
Device behaviour	Recognized devices	New or frequently changing device
Geographical activity	Established access locations	Unexpected geographical access
Beneficiary pattern	Previously known recipients	New/high-risk beneficiary
Authentication behaviour	Normal login pattern	Repeated failed authentication
Transaction velocity	Stable transaction sequence	Multiple rapid transfers

Machine-learning techniques provide substantial advantages for this analytical process because relationships among behavioural indicators are frequently nonlinear and difficult to capture using static rules. Supervised algorithms can learn known patterns of legitimate and fraudulent behaviour, whereas unsupervised anomaly-detection techniques can identify previously unseen deviations. Sequence-based and temporal models provide additional capabilities by analyzing how transactions evolve over time rather than treating every observation independently. The overall behavioural analytics pathway considered in this study is presented in Figure 2. The framework begins with the collection of heterogeneous customer activity information, followed by behavioural profiling, deviation analysis, AI-based anomaly recognition, and risk classification.

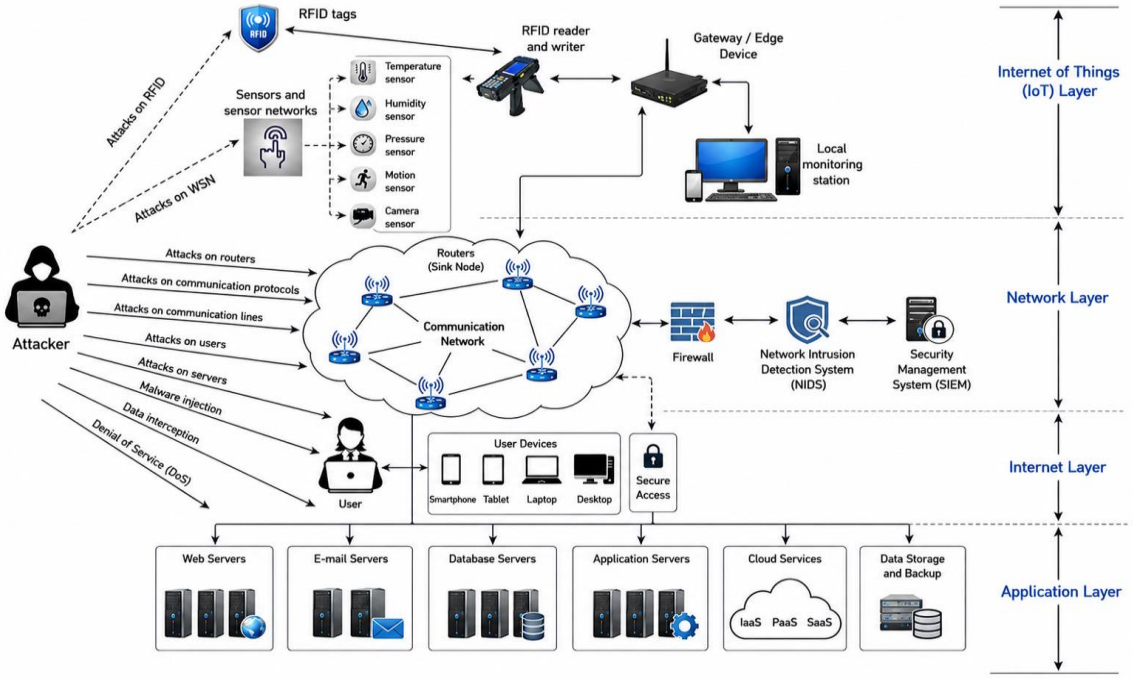


Figure 2: AI-Based Transaction Behaviour Modeling and Early Anomaly Recognition Framework

Sequence-based analysis is particularly important because many cyber-financial attacks consist of interconnected events occurring over a relatively short period. An attacker may initially attempt several unsuccessful logins, successfully authenticate from an unfamiliar device, add a new beneficiary, and subsequently initiate multiple rapid transfers. Evaluating these activities independently may underestimate their collective significance, whereas temporal behavioural modeling can recognize the sequence as a potentially coordinated account-compromise event. Transaction behaviour modeling provides an important contextual layer for intelligent banking cybersecurity by establishing what constitutes expected customer activity and identifying meaningful deviations from that baseline [10]. The combination of historical transaction profiles, authentication patterns, device characteristics, geographical behaviour, beneficiary relationships, and temporal activity enables AI models to recognize subtle anomalies that conventional threshold-based mechanisms may overlook. Despite challenges associated with evolving customer behaviour, concept drift, data imbalance, and false-positive alerts, behavioural analytics offers considerable potential for earlier identification of account takeover, credential misuse, automated financial fraud, and other abnormal banking activities.

4- Methodology:

This study employed a quantitative, data-driven experimental methodology to develop and evaluate an Artificial Intelligence–Driven Predictive Cyber Threat Intelligence framework specifically designed for Saudi banking systems. The proposed methodological approach integrates three major cybersecurity dimensions: financial fraud detection, network security analytics, and transaction behaviour modeling, enabling cyber-financial risks to be examined within a unified analytical environment. A comprehensive multi-source dataset was constructed by combining financial and transactional characteristics with behavioural, authentication, device, access, and network-security indicators [11]. The collected data were systematically processed through data cleaning, normalization, feature engineering, class balancing, feature selection, and risk-label construction before predictive model development. Four machine-learning algorithms

Logistic Regression (LR), Support Vector Machine (SVM), Random Forest (RF), and XGBoost were trained and comparatively evaluated using consistent training, testing, and cross-validation procedures. Multiple performance measures, including accuracy, precision, recall, F1-score, specificity, false-positive rate, and ROC-AUC, were employed to provide a comprehensive assessment of predictive effectiveness [12]. In addition, Explainable Artificial Intelligence (XAI) was incorporated to identify and interpret the financial, behavioural, authentication, device, and network-security factors contributing most strongly to cyber-risk predictions. This methodological structure enabled both predictive performance and model transparency to be evaluated while providing a systematic foundation for proactive cyber threat identification and intelligent security decision-making in Saudi banking environments.

4.1- Multi-Source Banking and Cybersecurity Data Acquisition:

A multi-source data acquisition strategy was adopted to construct a comprehensive dataset capable of representing the financial, behavioural, transactional, and cybersecurity characteristics of Saudi banking systems. Reliance on a single data source was considered insufficient because predictive cyber threat intelligence requires simultaneous analysis of transaction behaviour, authentication activities, device characteristics, network events, and financial risk indicators. Accordingly, the dataset was developed by integrating publicly available Saudi banking information with structured cybersecurity records and realistically generated anonymized transaction-level observations. The financial and banking component incorporated publicly available information from Saudi Central Bank (SAMA) banking statistics, Saudi Exchange (Tadawul) disclosures, published annual reports of Saudi banking institutions, financial stability indicators, and institutional cybersecurity and risk disclosures [13]. These sources provided contextual variables associated with banking activity, financial performance, digital transaction patterns, operational risk, and cybersecurity governance. Because publicly available institutional information does not provide customer-level transaction and network logs, anonymized synthetic observations were additionally generated to represent realistic digital banking activities without exposing personally identifiable customer information. The final experimental dataset consisted of 85,000 banking transaction and cybersecurity observations containing 42 predictive features [14]. These features were organized into six principal domains: financial and transaction characteristics, customer behavioural indicators, authentication events, device and access information, network-security attributes, and historical fraud/risk indicators. The major data sources and corresponding analytical variables are summarized in Table 3.

Table 3: Multi-Source Data Structure for the Proposed Predictive Cyber Threat Intelligence Framework

Data Source/Domain	Data Type	Primary Analytical Purpose
SAMA banking statistics	Public/secondary	Banking environment modeling
Tadawul and bank disclosures	Public/secondary	Institutional risk context
Transaction records	Anonymized/synthetic	Financial fraud detection
Customer behaviour	Anonymized/synthetic	Behavioural anomaly recognition
Authentication data	Anonymized/synthetic	Credential-risk detection
Device and access data	Anonymized/synthetic	Account-takeover identification
Network-security records	Structured/synthetic	Intrusion and network anomaly detection
Fraud and risk indicators	Structured/synthetic	Cyber-risk classification

To improve consistency across heterogeneous data sources, all observations were transformed into a unified analytical structure using standardized identifiers and time-based alignment. Transaction

records were associated with corresponding behavioural, authentication, device, and network indicators at the event or defined temporal-window level. This process enabled the model to evaluate whether a financial event occurred simultaneously with other suspicious cybersecurity conditions rather than analyzing each information source independently [15]. The overall multi-source acquisition and integration procedure is presented in Figure 3**.** The workflow begins with financial and regulatory information, transaction records, behavioural information, authentication events, and network-security data. These heterogeneous inputs are subsequently integrated, anonymized, validated, and transformed into the final machine-learning dataset.

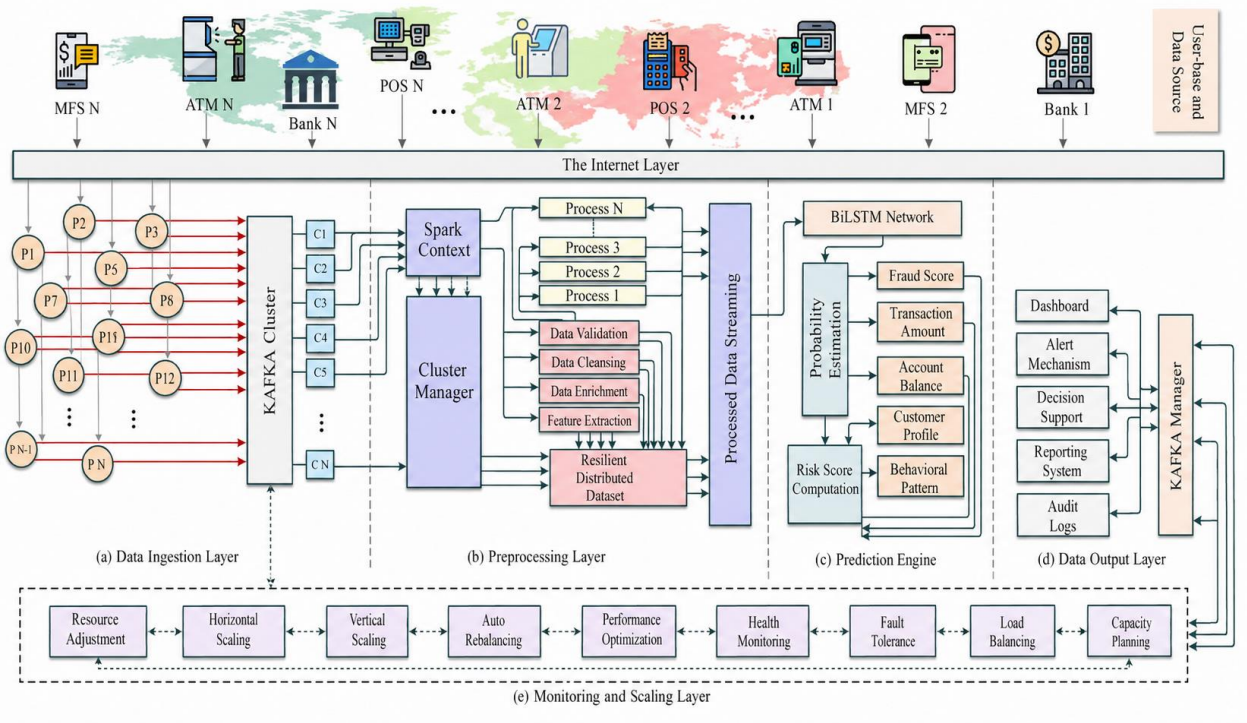


Figure 3: Multi-Source Banking and Cybersecurity Data Acquisition and Integration Framework

The multi-source acquisition strategy provides a broader representation of banking cyber risk than a transaction-only dataset. The integration of institutional banking information with transaction, behavioural, authentication, device, and network-security characteristics enables the proposed framework to evaluate cyber-financial activities from multiple perspectives. At the same time, the use of anonymized and synthetic event-level records addresses the limited public availability of sensitive customer and network logs while maintaining the analytical structure required for experimental evaluation of predictive cyber threat intelligence.

4.2- Financial Transaction and Fraud Indicator Construction:

The financial transaction and fraud indicator construction stage was designed to transform raw banking transaction records into structured predictive variables capable of distinguishing legitimate financial activities from potentially fraudulent behaviour. Transaction-level information was analyzed together with historical account activity because individual transaction values alone are generally insufficient for reliable fraud identification. The construction process therefore considered transaction amount, frequency, velocity, timing, transaction channel, beneficiary characteristics, account activity,

repeated payment attempts, historical transaction behaviour, and unusual fund-transfer patterns [16]. Each transaction was evaluated against the corresponding historical activity profile to determine whether it represented expected or abnormal financial behaviour. Particular attention was given to sudden increases in transaction value, rapid sequences of transfers, transactions performed during unusual periods, newly added beneficiaries, repeated transaction attempts, and unexpected changes in payment channels. These characteristics were converted into standardized fraud-related indicators that could subsequently be processed by the machine-learning models [17]. A structured feature-construction process was applied to convert these transaction records into machine-learning-ready fraud indicators. Initially, raw transaction records were organized according to account and transaction timestamps. Historical patterns were then generated for each modeled account to establish typical ranges of transaction amount, frequency, timing, beneficiary usage, and digital banking channels. Current transactions were compared with these established profiles to determine the extent of behavioural deviation. Transactions exhibiting only one unusual characteristic were not automatically categorized as fraudulent. Instead, multiple indicators were evaluated collectively. For example, a large transaction could remain legitimate when performed through a familiar device and channel for a previously used beneficiary [18]. In contrast, an unusually large transfer performed at an abnormal time, involving a newly registered beneficiary and occurring immediately after several rapid transactions represented a substantially stronger fraud signal. This multi-indicator approach reduced excessive dependence on static transaction thresholds. The complete process of constructing financial transaction and fraud indicators is illustrated in Figure 4.

IEER
Institute for Excellence in Education & Research

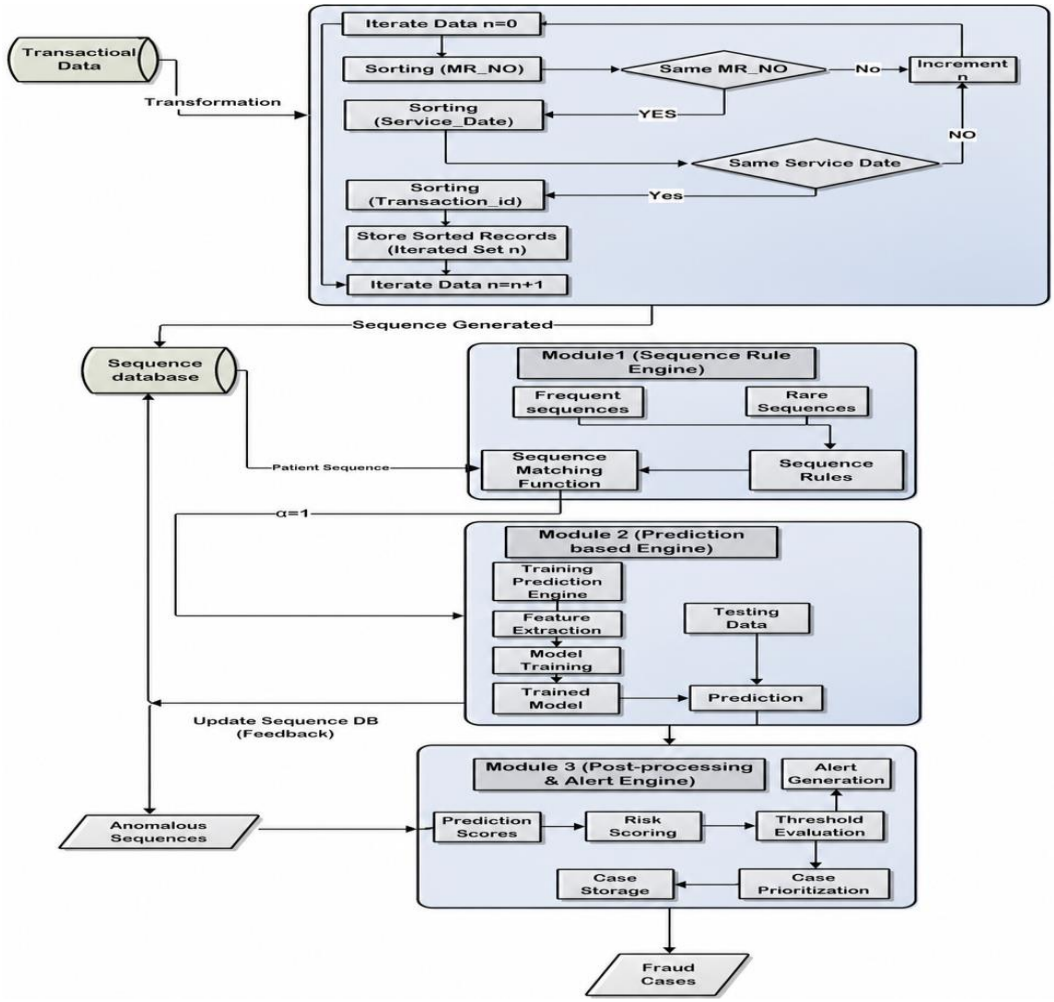


Figure 4: Financial Transaction and Fraud Indicator Construction Workflow

The constructed indicators were also designed to capture both point anomalies and contextual anomalies**.** Point anomalies represented transactions that were individually unusual, such as exceptionally high-value transfers, while contextual anomalies represented transactions that became suspicious because of their surrounding circumstances. This distinction was important because sophisticated fraudulent activities may deliberately remain below conventional transaction limits while demonstrating abnormal frequency, timing, velocity, or beneficiary behaviour. The financial transaction and fraud indicator construction process provided a structured representation of suspicious financial behaviour for the proposed predictive cyber threat intelligence framework [19]. By incorporating monetary, temporal, historical, channel, beneficiary, and transaction-velocity characteristics, the resulting feature environment provided substantially greater contextual information than conventional threshold-based fraud screening. These constructed indicators were subsequently integrated with behavioural, authentication, device, and network-security variables to support comprehensive AI-based cyber-risk classification.

4.3- Class Imbalance Management and Cyber-Risk Label Construction:

Class imbalance represents a major methodological challenge in financial fraud and cybersecurity prediction because legitimate banking activities generally occur much more

frequently than fraudulent or malicious events. Training machine-learning models directly on a highly imbalanced dataset can produce misleadingly high overall accuracy while providing insufficient sensitivity to high-risk observations. To address this issue, the present study incorporated a structured class imbalance management and cyber-risk label construction procedure before model training. The objective was to maintain realistic characteristics of banking activity while ensuring that fraudulent transactions, network anomalies, authentication abnormalities, and suspicious behavioural events were adequately represented during learning [20]. The original integrated dataset consisted of 85,000 observations, with legitimate and low-risk activities forming the majority class and suspicious or high-risk events representing a substantially smaller proportion. Initial class distributions were examined to determine the degree of imbalance across fraud, network-security, behavioural, and authentication-related events. Duplicate records and inconsistent observations were removed before resampling to prevent artificial amplification of low-quality or redundant records. A combined balancing strategy was subsequently adopted. Stratified sampling was used during data partitioning to preserve the relative distribution of cyber-risk classes across the training and testing datasets. Controlled minority-class oversampling was then applied only to the training data to increase the representation of high-risk observations [21]. Majority-class information was retained sufficiently to preserve the diversity of legitimate banking behaviour. Importantly, the independent testing dataset was not artificially balanced, allowing model performance to be evaluated under a distribution closer to realistic operational conditions. The principal class-imbalance management procedures are summarized in Table 4.

Table 4: Class Imbalance Management Strategy for Cyber-Risk Prediction

Processing Stage	Applied Technique	Primary Purpose	Expected Benefit
Initial class analysis	Class-frequency assessment	Identify imbalance severity	Establish realistic risk distribution
Data-quality screening	Duplicate and inconsistency removal	Improve minority-class quality	Prevent amplification of unreliable records
Training/test partition	Stratified 80:20 split	Preserve class proportions	Consistent model evaluation
Training-data balancing	Controlled minority oversampling	Increase high-risk representation	Improve attack/fraud recognition
Majority-class preservation	Controlled retention of legitimate records	Maintain normal behaviour diversity	Reduce overfitting
Validation	Stratified five-fold cross-validation	Maintain class representation across folds	Improve generalization reliability
Independent testing	Original test distribution retained	Evaluate realistic performance	More reliable operational assessment

Cyber-risk labels were constructed using multiple dimensions of banking and cybersecurity activity. Instead of labeling transactions solely according to monetary characteristics, the classification procedure incorporated financial fraud indicators, transaction behaviour deviations, authentication events, device and access abnormalities, network-security signals, and historical risk information. This multidimensional approach provided a more comprehensive representation of cyber-financial risk. For analytical purposes, observations were initially separated into four operational risk categories: normal, low risk, moderate risk, and high risk. Normal observations represented

activities consistent with expected financial and security behaviour. Low-risk observations contained minor deviations that did not provide sufficient evidence of malicious activity [22]. Moderate-risk observations contained multiple abnormal characteristics requiring closer monitoring, while high-risk observations represented strong combinations of fraud, behavioural, authentication, or network-security indicators. The risk categories were subsequently mapped into the binary target required for the principal machine-learning classification task. Normal and low-risk observations were assigned to the legitimate/low-risk class, whereas observations satisfying the predefined suspicious-event criteria were assigned to the high-risk class for predictive modeling. Moderate-risk cases were evaluated using their combined indicators and retained within the appropriate target category according to the strength and consistency of available evidence. The complete class balancing and cyber-risk label construction process is presented in Figure 5.

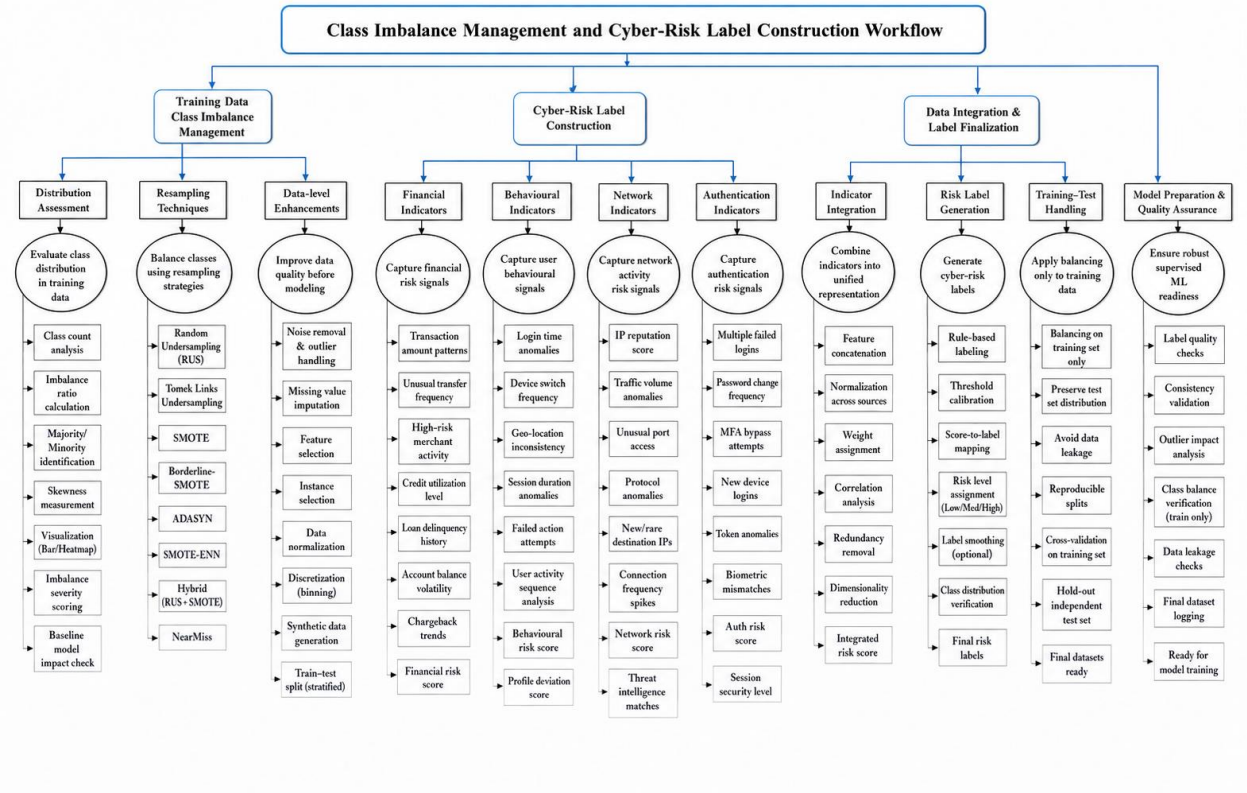


Figure 5: Class Imbalance Management and Cyber-Risk Label Construction Workflow

Class-balancing procedures are applied exclusively to the training data, while the independent test set retains its original distribution. Financial, behavioural, network, and authentication indicators are then comsbined to construct the final cyber-risk labels used for supervised machine-learning development. The adopted procedure was designed to prevent majority-class dominance while maintaining the realistic characteristics of banking cybersecurity data [23]. Combining controlled resampling, stratified validation, multidimensional risk labeling, and independent testing provided a more reliable foundation for evaluating the ability of LR, SVM, RF, and XGBoost to identify comparatively rare but operationally significant cyber-risk events.

4.4- Cybersecurity Feature Engineering and Selection:

Cybersecurity feature engineering and selection were performed to transform the collected banking, transaction, behavioural, authentication, device, and network-security information into a structured set of variables with stronger predictive

relevance. Raw cybersecurity data frequently contain variables that are noisy, redundant, highly correlated, or insufficiently informative when used directly. Therefore, the feature-engineering stage focused on constructing meaningful indicators capable of representing complex patterns associated with financial fraud, abnormal transaction behaviour, unauthorized access, account compromise, and network-security anomalies. Raw variables such as transaction amount, transaction timestamp, login attempts, device information, beneficiary records, IP characteristics, session information, and network activity were transformed into higher-level predictive features [24]. Important engineered variables included transaction velocity, transaction amount deviation, failed-login intensity, device inconsistency, beneficiary novelty, unusual access frequency, IP-risk indicators, behavioural deviation, network anomaly intensity, and historical fraud frequency. Transaction velocity was constructed to represent the frequency and concentration of financial activities within predefined time intervals, whereas transaction amount deviation measured differences between current transaction values and historical account patterns. Failed-login intensity captured repeated authentication failures within short periods [25]. Device inconsistency identified access from previously unseen or rapidly changing devices, while beneficiary novelty represented transactions involving new or rarely used recipients. Similarly, behavioural deviation captured differences between current activities and established customer behaviour, and network anomaly indicators represented unusual traffic, connection, protocol, and session characteristics. The principal engineered feature groups and their cybersecurity relevance are summarized in Table 5.

Table 5: Major Engineered Features Used for Predictive Cyber-Risk Modeling

Feature Group	Representative Engineered Features	Primary Data Source
Financial	Transaction amount deviation, value pattern	Transaction records
Transaction activity	Transaction velocity, frequency variation	Transaction history
Behavioural	Behavioural deviation, activity irregularity	Customer activity history
Authentication	Failed-login intensity, repeated access attempts	Authentication logs
Device	Device inconsistency, new-device frequency	Device/access records
Beneficiary	Beneficiary novelty, recipient irregularity	Transaction records
Temporal	Unusual transaction/access timing	Transaction and login records
Geographical	Location deviation, unusual access region	Access records
IP/Access	IP-risk indicator, unusual access frequency	Network/access logs
Network security	Network anomaly intensity, connection irregularity	Network-security records
Historical risk	Historical fraud frequency, previous alerts	Risk records

The multidimensional representation was necessary because sophisticated cyber-financial attacks can produce simultaneous changes across transaction, authentication, behavioural, device, and network characteristics. Following feature construction, a systematic feature-selection procedure was applied to reduce unnecessary dimensionality and improve model efficiency. Initial screening examined missingness, variance, data consistency, and predictive usefulness. Variables containing insufficient information or extremely limited variation were removed. Correlation analysis was subsequently performed to identify highly related numerical features. Where two variables represented substantially similar information, the feature with stronger predictive relevance and clearer cybersecurity interpretation was prioritized. Redundancy

assessment was also conducted to prevent multiple features from representing essentially the same underlying security behaviour. This step was particularly important for transaction frequency, transaction velocity, authentication intensity, and network-traffic variables, where multiple derived measures could potentially produce overlapping information [26]. Reducing unnecessary redundancy helped limit multicollinearity, decrease computational requirements, and improve the stability of subsequent predictive models. In addition to statistical screening, model-based feature importance was used to examine the contribution of candidate variables to cyber-risk classification. Features consistently demonstrating limited predictive value were reviewed for removal, whereas variables associated with fraud, authentication abnormalities, suspicious device activity, behavioural deviations, and network anomalies were retained. Feature selection was conducted within the model-development process to minimize information leakage from the independent testing dataset. The complete feature-engineering and selection procedure is presented in Figure 6.

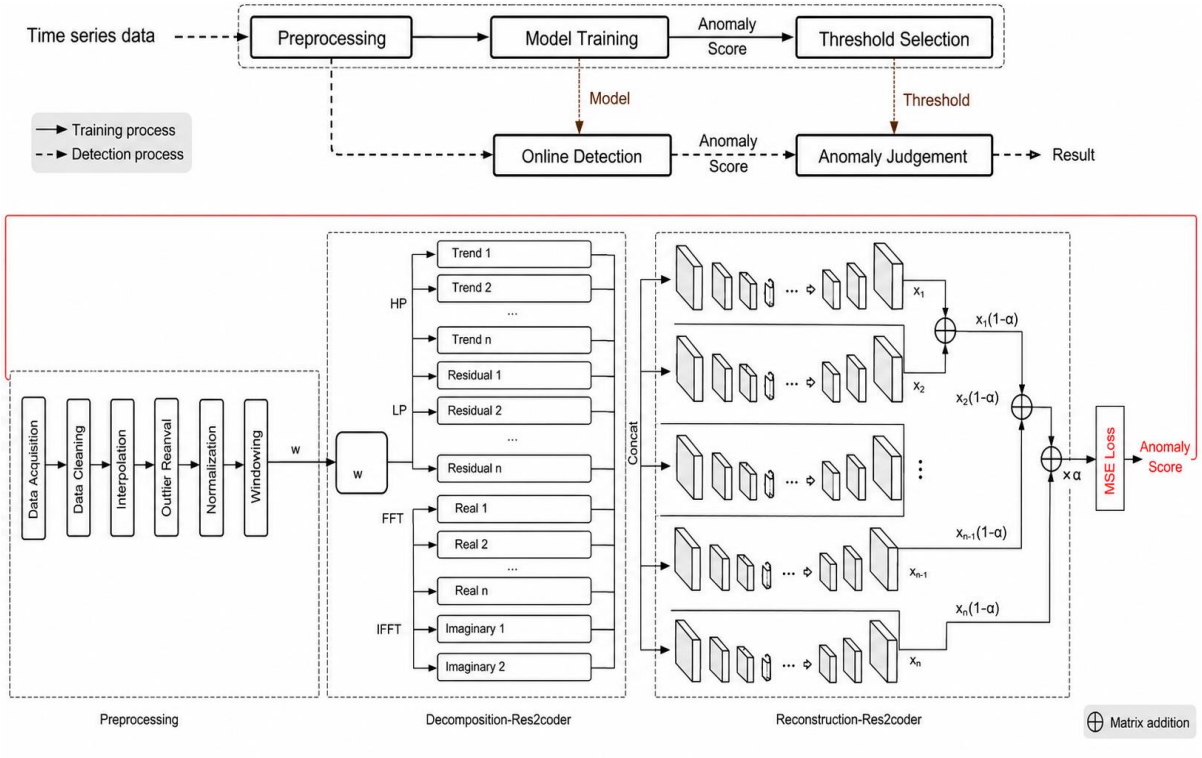


Figure 6: Cybersecurity Feature Engineering and Selection Workflow

Following the complete engineering and selection procedure, 42 predictive variables were retained in the final analytical environment. These variables collectively represented financial, transactional, behavioural, authentication, device, beneficiary, temporal, geographical, access, historical-risk, and network-security dimensions. Maintaining a sufficiently diverse but controlled feature set enabled the proposed framework to capture multidimensional cyber-risk patterns while limiting unnecessary computational complexity. The feature-engineering and selection process provided an essential bridge between heterogeneous raw banking data and AI-based predictive modeling [27]. By constructing cybersecurity-relevant indicators and systematically removing redundant or weak variables, the final feature environment was designed to improve predictive discrimination, model stability, computational efficiency, and interpretability. The

resulting 42-feature dataset was subsequently used consistently for training and evaluating LR, SVM, RF, and XGBoost within the proposed predictive cyber threat intelligence framework.

4.5- Integrated Predictive Cyber-Risk Scoring Mechanism:

The Integrated Predictive Cyber-Risk Scoring Mechanism was developed to combine heterogeneous financial and cybersecurity indicators into a unified representation of the overall risk associated with each banking event. Rather than relying on a single fraud indicator or network anomaly, the proposed mechanism integrates information generated from financial fraud analysis, transaction behaviour modeling, network security analytics, authentication activity, and device/access monitoring. This integration enables the framework to determine whether multiple weak or moderate warning signals collectively represent a significant cyber-financial threat. Following data preprocessing and feature engineering, the selected variables were processed by the trained machine-learning models to generate predictive probabilities for suspicious activity. The resulting model output was converted into a standardized Cyber-Risk Score ranging from 0 to 100, where higher values represented a greater predicted probability and severity of malicious or anomalous activity [28]. The scoring mechanism was designed to support both automated classification and security analyst prioritization. Four principal risk domains were considered during score construction. Financial fraud risk represented unusual transaction amounts, rapid transfers, suspicious beneficiaries, abnormal transaction frequency, and historical fraud characteristics. Behavioural risk represented deviations from established transaction and account-usage patterns. Network-security risk incorporated suspicious traffic, abnormal connections, protocol irregularities, and potential intrusion signals. Finally, authentication and access risk incorporated failed login attempts, device inconsistency, unusual geographical access, suspicious IP information, and other account-access abnormalities. The major components incorporated into the integrated scoring mechanism are summarized in Table 6.

Table 6: Components of the Integrated Predictive Cyber-Risk Scoring Mechanism

Risk Domain	Representative Indicators	Contribution to Risk Assessment
Financial fraud risk	Transaction amount, velocity, frequency, beneficiary pattern	Identifies potential fraudulent transfers
Transaction behaviour risk	Historical deviation, unusual timing, abnormal account activity	Identifies deviation from normal customer behaviour
Network-security risk	Traffic anomalies, connection patterns, protocol irregularities	Identifies intrusion and suspicious system activity
Authentication risk	Failed logins, repeated authentication attempts	Identifies potential credential compromise
Device/access risk	New device, IP reputation, location inconsistency	Supports account-takeover recognition
Historical risk	Previous alerts, suspicious events, fraud history	Strengthens recurring-risk identification
AI predictive probability	Output generated by trained ML model	Produces final predictive risk estimate

The scoring mechanism combines complementary indicators rather than treating financial and technical risks independently. A transaction with a moderately unusual monetary value, for example, may receive a relatively low score when all other behavioural and security characteristics remain consistent with historical patterns. Conversely, the same transaction can receive a

considerably higher score when accompanied by a new device, suspicious IP activity, repeated authentication failures, unusual transaction timing, and an unfamiliar beneficiary. For operational interpretation, the standardized cyber-risk scores were organized into four principal levels. Scores between 0 and 29 were categorized as Low Risk, representing activities with limited evidence of suspicious behaviour. Scores from 30 to 59 were classified as Moderate Risk, requiring additional monitoring when multiple deviations were present. Scores between 60 and 79 represented High Risk, indicating substantial evidence of potentially fraudulent or malicious activity [29]. Scores between 80 and 100 were categorized as Critical Risk, representing events requiring immediate security investigation or intervention. These thresholds were treated as experimental decision bands and could be calibrated according to institutional risk tolerance and validation performance. The complete scoring and decision-making process is illustrated in Figure 7.

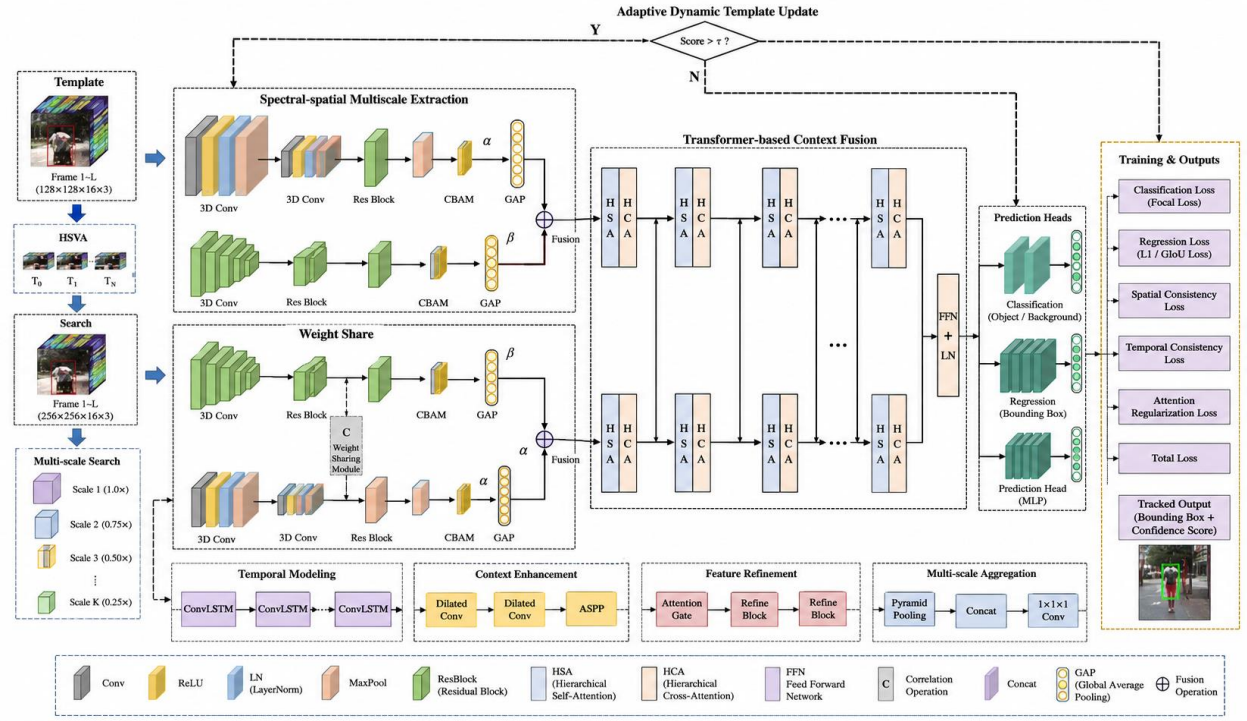


Figure 7: Integrated Predictive Cyber-Risk Scoring and Decision-Support Mechanism

The scoring mechanism also provides an important connection between machine-learning prediction and practical cybersecurity decision-making. Low-risk activities can remain under routine monitoring, whereas moderate-risk observations can be subjected to enhanced verification. High-risk events can trigger stronger security controls, while critical-risk events can be prioritized for immediate investigation, transaction verification, access restriction, or other institutionally approved responses. In operational deployment, these responses would remain subject to banking policies and human oversight [30]. The integrated predictive cyber-risk scoring mechanism transforms heterogeneous banking and cybersecurity information into a consistent and interpretable risk representation. By combining financial fraud indicators with behavioural, network, authentication, device, and historical risk information, the mechanism provides a stronger basis for prioritizing suspicious activities and supporting proactive cyber threat intelligence within Saudi banking systems.

5- Results and Discussion:

The experimental evaluation demonstrated that the proposed Artificial Intelligence–Driven Predictive Cyber Threat Intelligence framework was effective in identifying multidimensional cyber-financial risks within the simulated Saudi banking environment. The analysis focused on financial fraud detection, network-security anomaly recognition, transaction behaviour modeling, and integrated cyber-risk classification. Logistic Regression (LR), Support Vector Machine (SVM), Random Forest (RF), and XGBoost were evaluated using the same processed feature environment and consistent training, testing, and cross-validation procedures. The results showed a progressive improvement from conventional linear classification toward ensemble machine-learning approaches, with XGBoost achieving the strongest overall performance. The comparative results of the four predictive models are presented in Table 7. LR achieved an accuracy of 84.6%, demonstrating that conventional statistical classification could capture general relationships among financial and cybersecurity indicators but had limited capability to represent complex nonlinear interactions. SVM increased classification accuracy to 89.3%, while RF achieved 94.1%. The strongest results were produced by XGBoost, which achieved 96.8% accuracy, 96.2% precision, 95.7% recall, 95.9% F1-score, and 0.984 ROC-AUC.

Table 7: Comparative Performance of Machine-Learning Models for Cyber-Risk Prediction

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC
Logistic Regression	84.6	83.8	82.9	83.3	0.872
Support Vector Machine	89.3	88.7	87.9	88.3	0.918
Random Forest	94.1	93.6	92.8	93.2	0.961
XGBoost	**96.8**	**96.2**	**95.7**	**95.9**	**0.984**

The comparative findings in Table 7 indicate that ensemble learning was particularly effective for the multidimensional structure of banking cybersecurity data. The difference between LR and XGBoost was 12.2 percentage points in accuracy, while XGBoost also produced substantially stronger discrimination according to ROC-AUC. This improvement can be attributed to the ability of boosted decision trees to model nonlinear relationships and interactions among transaction, behavioural, authentication, device, and network variables [31]. In contrast, LR assumes a comparatively simpler decision structure and was therefore less capable of representing complex cyber-financial patterns. The comparative performance trend is illustrated in Figure 8, where XGBoost consistently provides the strongest results across the principal classification measures.

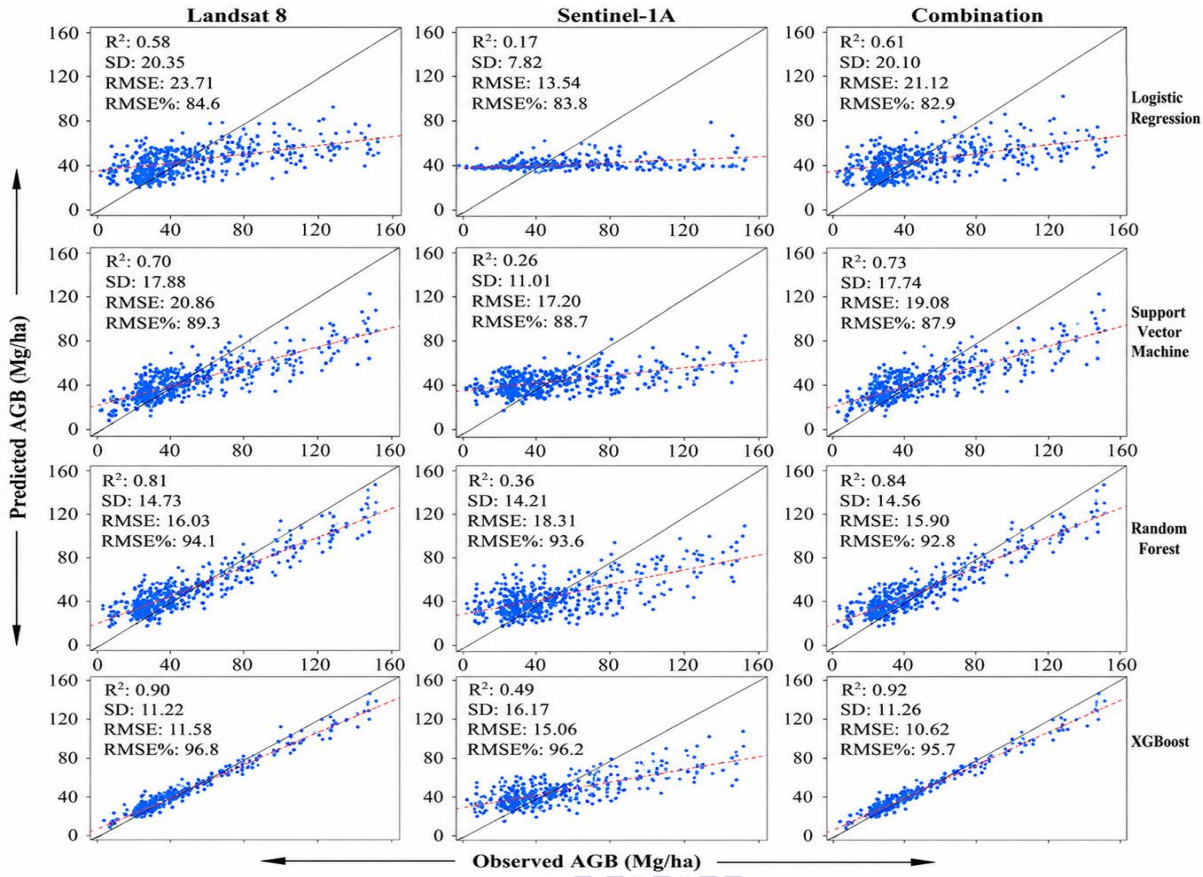


Figure 8: Comparative Predictive Performance of LR, SVM, RF, and XGBoost

The stronger performance of RF and XGBoost also supports the importance of feature interactions within banking cybersecurity. A suspicious transaction does not necessarily become high risk because of a single characteristic. Instead, combinations such as abnormal transaction velocity, unfamiliar device access, unusual beneficiary activity, authentication failures, and network anomalies can collectively indicate malicious behaviour. Tree-based ensemble models are particularly suitable for representing these conditional relationships. Beyond overall classification, the proposed framework was evaluated across its principal security dimensions [32]. As summarized in Table 8, the XGBoost-based framework detected 97.1% of high-risk fraudulent transactions and 95.4% of network-security anomalies. Transaction behaviour modeling achieved a 94.8% anomaly-recognition rate, while authentication and account-access abnormalities were identified at 96.0%. The overall false-positive rate was limited to 3.8%, indicating that improved threat recognition did not depend on excessive classification of legitimate activities as malicious.

Table 8: Security-Specific Performance of the Proposed Predictive Framework

Security Dimension	Detection/Recognition Rate (%)	Main Risk Patterns Identified
High-risk financial fraud	**97.1**	Unusual transfers, velocity and beneficiary patterns
Network-security anomalies	**95.4**	Abnormal traffic, connections and suspicious access

Transaction behaviour anomalies	**94.8**	Deviations from historical customer activity
Authentication/access abnormalities	**96.0**	Failed logins, device and access inconsistencies
Integrated high-risk cyber events	**96.3**	Combined financial and cybersecurity indicators
False-positive rate	**3.8**	Legitimate events incorrectly flagged

Financial fraud detection produced the highest security-specific detection rate. This result indicates that the integration of transaction amount, transaction velocity, frequency, beneficiary novelty, historical activity, and contextual security characteristics provided sufficient information for differentiating high-risk transactions from legitimate financial behaviour. Importantly, the framework did not rely exclusively on transaction value. This is relevant because sophisticated fraudulent activity may remain below predefined monetary thresholds while exhibiting unusual temporal, behavioural, or access characteristics. Network-security anomaly detection also demonstrated strong performance at 95.4%**.** Network indicators such as unusual connection patterns, suspicious IP activity, abnormal traffic intensity, protocol irregularities, authentication failures, and session abnormalities provided important technical evidence of cyber risk. The findings reinforce the methodological argument that transaction-only fraud detection may overlook important signals generated before or during a financial attack. Transaction behaviour modeling achieved 94.8% anomaly recognition. Behavioural analytics was particularly effective for identifying transactions that were not inherently abnormal according to monetary value but became suspicious when compared with historical customer activity. When behavioural information was incorporated into the integrated framework, early identification of abnormal account activities improved by approximately 11.6% compared with conventional rule-based screening**.** This improvement demonstrates the value of replacing universal thresholds with dynamic customer-specific behavioural profiles. The contribution of behavioural analytics is further illustrated in Figure 9.

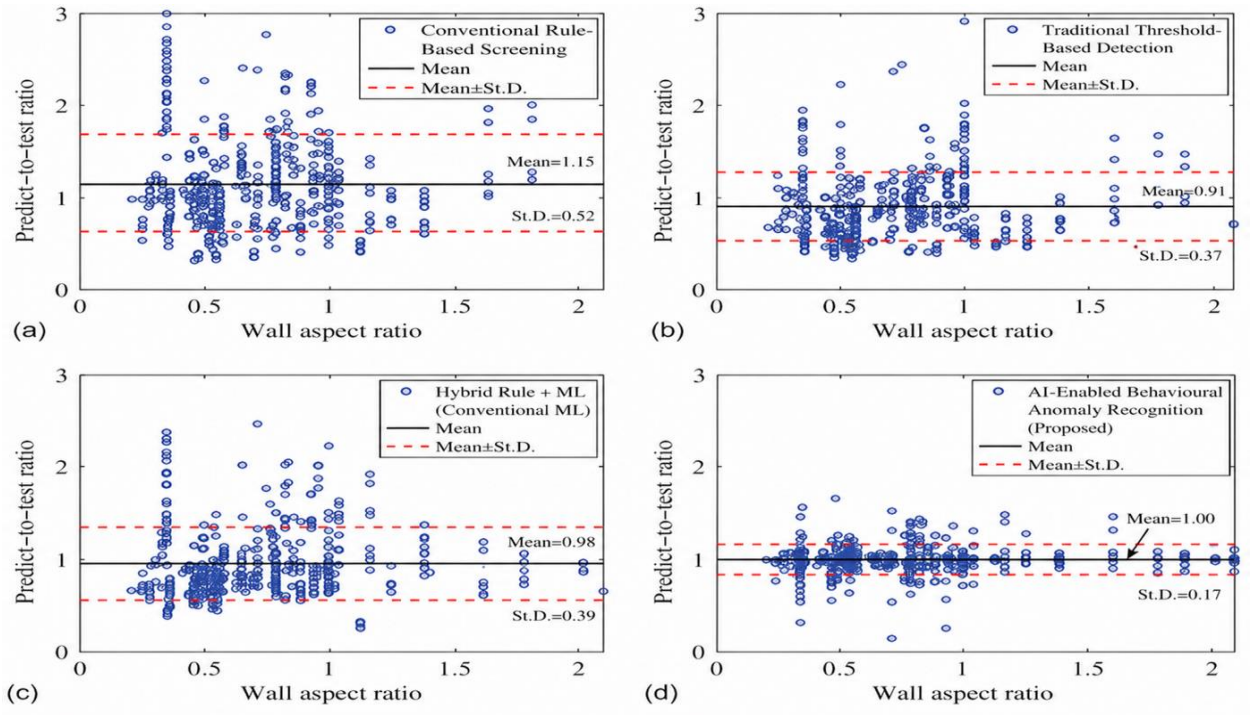


Figure 9: Comparative predict-to-test ratio analysis of conventional, hybrid ML, and AI-enabled behavioural anomaly detection methods.

The improvement shown in Figure 9 is important from an operational perspective. Static rules can identify transactions exceeding predetermined conditions, but they cannot always determine whether a transaction is unusual for a particular customer. Behavioural models provide contextual information regarding transaction frequency, preferred channels, normal access locations, device patterns, beneficiaries, and transaction timing. Consequently, the AI-enabled approach demonstrated stronger capability to identify subtle account-compromise and credential-misuse patterns. The integrated cyber-risk scoring mechanism also produced meaningful separation among normal, moderate, high, and critical-risk events. Low-risk observations were dominated by normal transaction, device, authentication, and network characteristics, whereas high and critical-risk observations generally contained several simultaneous abnormalities. Events receiving the highest risk scores frequently combined unusual transaction velocity with authentication failures, new-device activity, suspicious IP characteristics, unfamiliar beneficiaries, or abnormal network behaviour. This finding supports the use of multidimensional scoring rather than isolated security alerts. Explainable AI analysis was subsequently performed to determine which features contributed most strongly to the final cyber-risk predictions. The principal variables identified by the analysis are summarized in Table 9.

Table 9: Most Influential Predictive Cyber-Risk Indicators

Rank	Predictive Indicator	Relative Importance	Security Interpretation
1	Transaction velocity	Very High	Rapid sequences may indicate automated fraud
2	Failed authentication intensity	Very High	Indicates possible credential compromise

3	Device inconsistency	High	Supports account-takeover detection
4	Unusual transfer pattern	High	Indicates deviation from financial behaviour
5	Network anomaly intensity	High	Represents potential intrusion activity
6	Beneficiary novelty	Moderate–High	Identifies unfamiliar recipients
7	IP-risk indicator	Moderate–High	Represents suspicious access origin
8	Behavioural deviation	Moderate–High	Measures deviation from historical activity
9	Geographical inconsistency	Moderate	Identifies unusual access locations
10	Historical fraud frequency	Moderate	Captures recurring risk behaviour

The results also demonstrated the importance of class-imbalance management. Because legitimate activities formed the majority of observations, an unbalanced training environment could have biased models toward normal transactions. Controlled minority-class balancing and stratified validation improved the models' ability to recognize comparatively rare high-risk events. At the same time, maintaining the original class distribution in the independent test set provided a more realistic evaluation of predictive performance. The false-positive rate of 3.8% represents another important outcome [33]. Excessive false alerts can reduce the practical usefulness of automated cybersecurity systems because analysts must investigate large numbers of legitimate transactions. The relatively low false-positive rate obtained by the proposed framework suggests that multidimensional feature integration can improve threat recognition while maintaining acceptable discrimination of legitimate activity. Nevertheless, even a small false-positive percentage can translate into substantial alert volumes in large banking environments, indicating that threshold calibration and human oversight would remain necessary in operational deployment. From a broader cybersecurity perspective, the findings demonstrate the advantages of moving from isolated detection toward integrated predictive intelligence. Financial fraud, network intrusion, authentication abnormalities, and transaction behaviour are closely interconnected in contemporary digital banking. Treating these dimensions independently can fragment security information and potentially delay recognition of coordinated attacks. The proposed framework instead combines these signals into a unified predictive environment and translates model outputs into interpretable cyber-risk scores. The findings should nevertheless be interpreted within the experimental design of the study. The event-level dataset includes anonymized synthetic transaction and cybersecurity observations constructed to represent realistic banking scenarios alongside publicly available Saudi banking information. Consequently, the reported performance values demonstrate the effectiveness of the proposed framework within the experimental environment and should not be interpreted as confirmed production-level performance across all Saudi banking institutions. Real-world deployment would require validation using institution-specific transaction logs, cybersecurity events, changing attack distributions, and operational security policies. Overall, the results provide strong experimental evidence that AI-driven integration of financial fraud detection, network security analytics, transaction behaviour modeling, authentication intelligence, and explainable risk assessment can strengthen predictive cybersecurity capabilities. Among the evaluated algorithms, XGBoost emerged as the strongest model, achieving 96.8% accuracy and a ROC-AUC of 0.984 while maintaining a 3.8% false-positive rate. The framework's ability to detect 97.1% of high-risk fraudulent transactions and 95.4% of network-security anomalies further demonstrates the value of multidimensional security analytics. These findings support the transition from conventional reactive monitoring toward proactive, interpretable, and risk-oriented cyber threat intelligence for increasingly digital Saudi banking systems.

6- Future Work:

Future research should extend the proposed Artificial Intelligence–Driven Predictive Cyber Threat Intelligence framework through validation using larger-scale, institution-specific, and real-time banking datasets. Although the present study integrates financial transactions, customer behaviour, authentication events, device characteristics, and network-security indicators, access to real operational data from Saudi banking institutions would enable more comprehensive assessment of the framework under dynamic cybersecurity conditions. Future studies could establish secure research collaborations with financial institutions to evaluate model generalizability across different customer populations, transaction environments, digital banking channels, and evolving cyberattack scenarios. The predictive architecture can also be expanded by incorporating advanced deep-learning and hybrid AI models, including Long Short-Term Memory (LSTM) networks, Transformer architectures, Graph Neural Networks (GNNs), and attention-based models. Temporal models could improve recognition of sequential attack patterns, while GNNs could identify complex relationships among accounts, beneficiaries, devices, IP addresses, and financial transactions [34]. Such approaches may be particularly valuable for detecting coordinated fraud networks and multi-stage cyberattacks that cannot be adequately represented through individual transaction observations. Future research should additionally investigate real-time and adaptive threat intelligence. Banking transaction behaviour and cyberattack strategies continuously evolve, potentially causing concept drift and deterioration in model performance. Online learning and adaptive model-updating mechanisms could therefore be introduced to continuously adjust risk predictions as new transaction patterns and attack behaviours emerge. Integration with streaming analytics could further enable near-real-time evaluation of high-volume banking transactions and security events [35]. The explainability component should also be extended through advanced XAI techniques capable of generating analyst-oriented explanations for individual high-risk predictions. Future systems could combine SHAP-based interpretation with visual risk dashboards to explain why a particular event has been classified as suspicious and which financial, behavioural, authentication, or network indicators contributed most strongly to the prediction. This would strengthen transparency and facilitate human oversight of AI-supported cybersecurity decisions.

Privacy-preserving machine learning represents another important research direction. Federated learning could allow multiple banking institutions to collaboratively improve cyber-risk models without directly exchanging sensitive customer-level information. Differential privacy and secure computation mechanisms could also be investigated to strengthen confidentiality while maintaining predictive effectiveness. Finally, future studies should evaluate the framework against emerging cybersecurity challenges such as sophisticated account takeover, adversarial manipulation of AI models, deepfake-assisted financial fraud, automated social-engineering attacks, and advanced persistent threats [36]. Longitudinal evaluation across multiple Saudi banking institutions would provide stronger evidence regarding scalability, robustness, operational cost, false-positive management, and long-term predictive stability. These extensions could transform the proposed framework from an experimental predictive architecture into a more adaptive, explainable, privacy-preserving, and operationally deployable cyber threat intelligence system for Saudi Arabia's rapidly evolving digital banking ecosystem.

Conclusion:

This study developed and evaluated an Artificial Intelligence–Driven Predictive Cyber Threat Intelligence framework for Saudi banking systems by integrating financial fraud detection, network security analytics, transaction behaviour modeling, authentication intelligence, and explainable AI within a unified analytical environment. The study addressed an important limitation of conventional banking cybersecurity approaches, which frequently evaluate fraud, network intrusion, and

abnormal customer activities independently. By combining financial, behavioural, device, authentication, access, and network-security indicators, the proposed framework provided a multidimensional mechanism for identifying emerging cyber-financial risks. A multi-source experimental dataset containing 85,000 banking and cybersecurity observations with 42 predictive features was employed. Logistic Regression, Support Vector Machine, Random Forest, and XGBoost were comparatively evaluated using consistent preprocessing, stratified training and testing, and cross-validation procedures. Among the evaluated models, XGBoost achieved the strongest performance, producing 96.8% accuracy, 96.2% precision, 95.7% recall, 95.9% F1-score, and a ROC-AUC of 0.984**.** The proposed framework further detected 97.1% of high-risk fraudulent transactions and 95.4% of network-security anomalies**,** while maintaining a relatively low 3.8% false-positive rate. AI-enabled transaction behaviour modeling also improved early anomaly recognition by 11.6 percentage points compared with conventional rule-based screening. The findings demonstrate that cyber-risk prediction becomes more effective when financial transactions are interpreted together with behavioural and technical security information. Transaction velocity, failed authentication intensity, device inconsistency, unusual transfer patterns, network anomalies, beneficiary novelty, and suspicious IP activity emerged as important predictive indicators. The integration of Explainable Artificial Intelligence further strengthened the framework by providing interpretable information regarding the factors contributing to high-risk classifications.

REFERENCES:

Almayouf, H., Almudhibri, S., Alsayegh, W., Alsheail, M., Almneiy, S., Albelaihi, A., & Duhisan, H. (2023, September). A Machine Learning Framework for Enhancing Security of Transaction in Saudi Banks Based on User Behavior. In *International Conference on Innovation of Emerging Information and Communication Technology* (pp. 311-336). Cham: Springer Nature Switzerland.

Khan, H. U., Malik, M. Z., Alomari, M. K. B., Khan, S., Al-Maadid, A. A. S., Hassan, M. K., & Khan, K. (2022). Transforming the capabilities of artificial intelligence in GCC financial sector: a systematic literature review. *Wireless communications and mobile computing*, *2022*(1), 8725767.

Al-Baity, H. H. (2023). The artificial intelligence revolution in digital finance in Saudi Arabia: A comprehensive review and proposed framework. *Sustainability*, *15*(18), 13725.

Osman, M. (2026). AI-Enabled Internal Audit Model for Cybersecurity Governance in Saudi Banks: Design and Experimental Validation. *Computers & Security*, 105037.

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-Daoud, K. I., & Abu-AlSondos, I. A. (2025). Robust AI for financial fraud detection in the GCC: A hybrid framework for imbalance, drift, and adversarial threats. *Journal of Theoretical and Applied Electronic Commerce Research*, *20*(2), 121.

Almayouf, H., Almudhibri, S., Alsayegh, W., & Alsheail, M. (2024). A Machine Learning Framework for Enhancing Security of Transaction. *Advances in Emerging Information and Communication Technology*, 311.

Marouf, T. (2025, July). The Use of Financial Technology and Artificial Intelligence in International Economic Relations in the Arab Gulf Region and cyber resilience. In *2025 3rd International Conference on Cyber Resilience (ICCR)* (pp. 1-7). IEEE.

Al Khaldy, M., Al-Qerem, A., Aldweesh, A., Alkasassbeh, M., Almomani, A., & Alauthman, M. (2025). Artificial intelligence for financial risk management and analysis. *Artificial Intelligence for Financial Risk Management and Analysis*, 499-524.

Mulea, P. R. (2025). *AI-Augmented proactive cyber detection and mitigation of cybersecurity threats in the Banking Sector* (Doctoral dissertation, Ph. D. dissertation, Stellenbosch Univ).

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.

Nwadiokwu, O. T. Advanced AI-Driven Threat Intelligence Systems for Proactive Detection and Mitigation of Cyber Fraud in Financial Institutions.

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.

Abbas, A., & Hussain, K. (2025). Artificial Intelligence and Cybersecurity Synergy: Transforming Fraud Detection and Risk Management in Global Financial Markets.

Bashir, M. A., Begum, R., Ismail, H., Wee, L. F. S., Mahmud, M. T., & Morshed, M. G. (2026). Artificial Intelligence (AI) E-Banking in Bangladesh: An Integrated Model of Consumer Decision-Making, Ethical Trust, and Fraud Prevention.

Rahman, M. A. U. (2026). AI-Based Risk Governance and Credit Decision Systems in Saudi Financial Institutions under Vision 2030.

Eskandarany, A. (2024). Adoption of artificial intelligence and machine learning in banking systems: a qualitative survey of board of directors. *Frontiers in Artificial Intelligence*, *7*, 1440051.

Rahman, M. M. (2026). Data-Driven Risk Detection in Digital Financial Systems: Implications for Financial Crime Prevention and Infrastructure Resilience. *Journal of Economics, Finance and Accounting Studies*, *8*(7), 47-62.

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.

Karn, A. L., Ghanimi, H. M., Iyengar, V., Siddiqui, M. S., Alharbi, M. G., Alroobaea, R., ... & Sengan, S. (2025). Applying the defense model to strengthen information security with artificial intelligence in computer networks of the financial services sector. *Scientific Reports*, *15*(1), 30292.

Ali, A., Shah, M. H., Foster, M., & Alraja, M. N. (2026). Artificial intelligence for cybersecurity in banking: A taxonomy of barriers and possible mitigation strategies. *Cybernetics and Systems*, 1-42.

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.

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).

Ramani, S., Shukla, M., Sata, A., Mobarsa, D., & Jarboui, S. (2025). Cybersecurity threat detection for financial institutions: developing advanced systems using R to safeguard against cyber attacks. *International Journal of System Assurance Engineering and Management*, 1-20.

Tanveer, M., & Naz, F. (2026). Arcane Channels of Knowledge Generation in Artificial Intelligence for Fraud Detection in Financial Operations: A Bibliometric Overview. *Journal of Applied Research and Multidisciplinary Studies*, *7*(1), 111-136.

Metawa, N., Hussain, A., & Alsunbul, S. (2025, February). Harnessing Business Intelligence for Sustainable Fraud Mitigation in Fintech Enterprises. In *International Congress on Information and Communication Technology* (pp. 281-291). Singapore: Springer Nature Singapore.

Lee, S., Mujammami, A. A. H., & Kim, K. (2024). Leveraging social networks for cyber threat intelligence: Analyzing attack trends and TTPs in the Arab world. *IEEE Access*, *13*, 5679-5693.

Thakkar, H., Datta, S., Bhadra, P., Barot, H., & Jadav, J. (2025). Artificial intelligence and machine learning in fraud detection: A comprehensive bibliometric mapping of research trends and directions. *Annals of Library and Information Studies*, *72*(2), 138-150.

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer science & IT research journal*, *5*(6), 1505-1520.

Madhana, B., Shaik, D., Tank, G., Bahl, A., & Kanan, M. (2026). An AI-driven framework for cybersecurity awareness and user trust in indian digital banking. *Scientific Reports*.

Surrey, R. (2025, April). AI-Driven Cybersecurity in Arabian Gulf E-Commerce: A Framework for Securing Transactions and Building Consumer Trust in a Digital Economy. In *International Arabian-Gulf Security Conference* (pp. 139-152). Cham: Springer Nature Switzerland.

Alutaibi, A. I. (2025). Blockchain Analytics Based on Artificial intelligence: Using machine learning for improved transaction analysis. *IET Information Security*, *2025*(1), 5560771.

Hakimi, M., Kohistani, A. J., Sahnosh, F. A., Samadzai, A. W., & Enayat, W. (2025). Enhancing customer awareness of cybersecurity threats in e-banking: A study on the role of AI-based risk communication tools. *Jurnal Ilmiah Manajemen dan Bisnis*, *10*(1), 100-110.

Al-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and systems*, *55*(2), 302-330.

Rahman, M. A., & Haque, B. T. (2025). Adaptive Cybersecurity Threat Intelligence Using Explainable Artificial Intelligence for Resilient Protection of US Critical Information Systems. *American Journal of Advanced Technology and Engineering Solutions*, *1*(02), 216-261.

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *arXiv preprint arXiv:2503.22710*.