



A Review of Machine Learning and Deep Learning Techniques for Financial Risk Assessment: Loan Default Prediction and Fraud Detection

Ayodeji Olusegun
Akinwumi

Department of Informatics
& Information Systems,
Faculty of Computing,
Adekunle Ajasin
University, Akungba-
Akoko, Ondo State,
Nigeria.

Samuel Adebayo
Oluwadare

Department of Computer
Science,
School of Computing,
Federal University of
Technology, Akure, Ondo
State, Nigeria.

Ilobekemen Perpetual
Oladoja

Department of Computer
Science,
School of Computing,
Federal University of
Technology, Akure, Ondo
State, Nigeria.

Hussein
Oluwaponmille
Adefuwa

Department of Computer
Science,
Faculty of Computing &
Information Technology,
Lagos State University,
Lagos State, Nigeria.

ABSTRACT

The growth of digital lending, fintech services, and online financial transactions has increased the need for financial institutions to improve credit risk assessment and fraud detection. Traditional approaches increasingly struggle with the volume, velocity, and complexity of modern financial data, contributing to growing interest in machine learning (ML) and deep learning (DL). However, existing reviews often examine loan default prediction and fraud detection separately, with limited systematic comparison of ML and DL techniques across both risk areas. This review addresses this gap by systematically synthesising 109 studies on statistical, ML, and DL techniques applied to loan default prediction and fraud detection. The review examines statistical models, tree-based and ensemble methods, support vector machines, neural networks, recurrent architectures, attention-based models, and hybrid approaches. Findings show that performance varies across techniques, datasets, and financial risk contexts, making it difficult to establish a universally superior approach. Tree-based ensemble methods, particularly Random Forest, XGBoost, Gradient Boosting, and LightGBM, show strong performance on structured financial data, while recurrent architectures such as LSTM, GRU, and BiLSTM, with CNN and attention-based models, show particular benefits where risk information contains complex or sequential patterns. Several studies also reported improved performance from hybrid ML-DL approaches. Persistent challenges are class imbalance, limited financial data, model interpretability, data privacy, computational requirements, and deployment costs. Approaches such as SMOTE, synthetic data generation, explainable artificial intelligence, and federated learning have been explored to address these issues. Studies using African financial datasets remain relatively few compared with those from other regions. The study concludes that the suitability of ML and DL techniques for financial risk assessment depends on the nature of the risk, the characteristics of the data, and the modelling approach used.

General Terms

Machine Learning, Deep Learning, Financial Risk Assessment, Credit Risk Management, Fraud Detection, Financial Data Mining, Financial Institution Algorithms.

Keywords

Loan Default Prediction, Credit Risk, Financial Fraud, Ensemble Learning, Recurrent Neural Networks, Hybrid Models, Class Imbalance, Synthetic Data, Explainable AI.

1. INTRODUCTION

The stability and growth of any economy depend heavily on financial institutions, as they provide essential services such as savings and investments options, credit facilities, insurance, and efficient systems for conducting payments [1], [2], [3]. Empirical studies also highlight the central role of financial institutions in today's society [4], [5], [6]. They connect savers with investors, helping resources flow efficiently and supporting overall economic stability. Their responsibilities also go beyond lending and deposits; businesses rely on them to process payments, households use them to manage personal finances, and governments channel funds for development projects. Through these functions, financial institutions play a crucial role in sustaining economic stability, promoting growth, and supporting the efficient functioning of markets, thereby benefiting individuals, businesses, and society as a whole. However, despite their central role in the economy, many financial institutions continue to face significant challenges that affect their stability and overall performance [7], [8], [9]. In some cases, these challenges have led to the collapse or near collapse of some financial institutions around the world [10].

[11], [12] posit that many of the challenges facing financial institutions largely stem from poor regulation, weak internal controls, excessive risk-taking, and exposure to fraudulent practices. These issues therefore leave financial institutions vulnerable to problems such as rising non-performing loans, increased fraud and liquidity shortages. Such pressures continue to undermine the stability and performance of financial institutions, especially in developing countries, where fragile financial systems and high economic risks make them even more vulnerable [10].

In the context of financial risk, financial institutions face a range of factors that can undermine their stability and overall performance. These include liquidity risk, which occurs when financial institutions struggle to meet short-term obligations or access funds without creating losses, a condition shown to significantly influence performance and risk behaviour in banks across different markets [13], [14], [15]; fraud risk such as cybercrime, insider misconduct, and falsification of records that threaten both institutional stability and public trust [16], [17], [18]; credit risk, which occurs when borrowers fail to fulfil their debt obligations, potentially causing financial losses [19], [20]; market risk, arising from fluctuations in interest rates, equity prices, and foreign exchange rates that can affect the financial position of such institution [21]; and operational risk, which stems from weaknesses in internal processes, human errors, or inefficiencies in systems and procedures [22]. These financial risks are summarized in Figure 1.

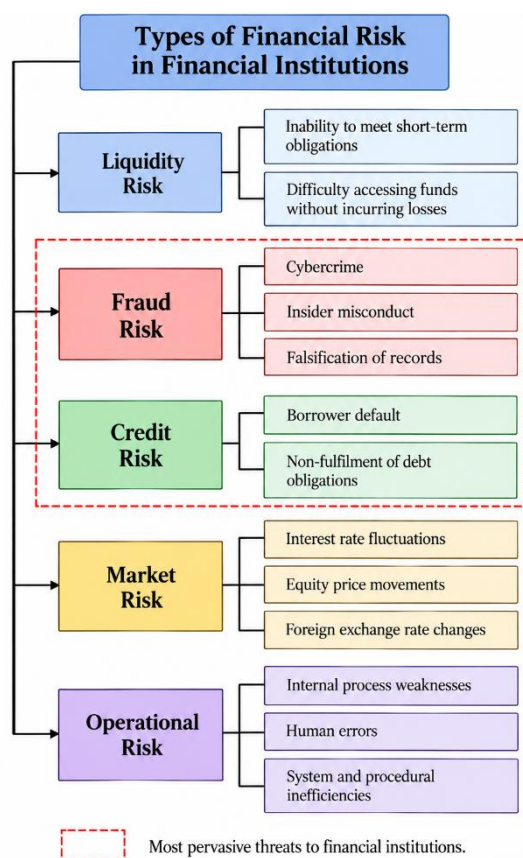


Figure 1: Types of Financial Risk in Financial Institutions

Out of the various risks confronting financial institutions, credit risk and fraud risk are often regarded as among the most pervasive threats to the stability of financial institutions [23]. Credit risk is particularly important because of its direct effect on loan losses and overall bank performance when borrowers fail to meet their repayment obligations [24], [25]. Fraud on the other hand has become a persistent and widespread problem worldwide [26], [27]. Empirical evidence from literature shows that fraudulent activities continue to undermine institutional stability, erode customer confidence, and cause significant financial losses [18], [28]. Given the severity and far-reaching implications of these risks, financial institutions must therefore prioritize the development and implementation of a robust and structured risk assessment framework capable of identifying emerging threats at an early stage and

safeguarding economic growth and public confidence. Effective financial risk assessment therefore a critical mechanism for identifying, measuring, and reducing vulnerabilities and strengthening financial stability at both national and global levels [29], particularly in today's financial landscape where economic uncertainty and rapid changes in financial markets have increased the exposure of various institutions to numerous risks [30].

Financial risk assessment has traditionally relied on statistical models, expert judgment, and other conventional techniques to evaluate and predict financial risks [31]. However, the increasing complexity, volume, and dynamic nature of financial data have exposed limitations in these approaches, particularly in their ability to capture complex patterns and changing relationships within financial systems [32]. The limitations of these traditional approaches have prompted growing interest in machine learning (ML) and deep learning (DL) as alternative tools for financial risk assessment [33], [34]. Unlike static, rule-based systems, ML and DL models can learn complex, non-linear patterns from large volumes of transactional and behavioural data [35], [36]. This makes them useful for identifying changing fraud patterns and borrower risk characteristics that may not be captured by traditional credit scoring methods [37], [38].

This capability has become increasingly relevant with the rapid growth of digital lending and fintech platforms, which generate large-scale, high-frequency data that traditional methods were not designed to process [39]. As a result, a substantial body of literature has emerged applying ML and DL techniques to loan default prediction and fraud detection, reporting improvements in predictive accuracy and adaptability over conventional approaches [40], [41], [42].

Even with this growing body of work, existing reviews in the area tend to focus narrowly on either loan default prediction or fraud detection in isolation, rather than examining both problems jointly within a single comparative framework [33]. Therefore, the aim of this study is to review machine learning and deep learning techniques applied to loan default prediction and fraud detection, identifying trends, performance metrics, limitations, and research gaps.

2. BACKGROUND AND CONCEPTUAL FOUNDATIONS

2.1 Financial Risk Assessment

Financial risk assessment refers to the processes financial institutions use to identify, measure, and manage the various forms of risk to which they are exposed. As discussed in Section 2, credit risk and fraud risk are key areas of financial risk assessment in financial institutions, though liquidity, market, and operational risk also affects the overall risk profile of an institution [13], [14], [15]. Credit risk refers to the possibility that a borrower will fail to meet contractual repayment obligations, and its accurate assessment underpins nearly every lending decision a financial institution makes. Fraud risk, by contrast, arises from deliberate deception like cybercrime, insider misconduct, identity theft, and falsification of records and threatens both the immediate financial position and the broader reputational standing of an institution. Operational risk, stemming from weaknesses in internal processes, human error, or system inefficiencies, is not a primary focus of this review but is worth noting briefly here, since credit and fraud losses frequently compound operational risk exposure, inadequate monitoring systems or process



failures make both default and fraud harder to detect and contain in the first place. This review concentrates specifically on credit risk and fraud risk, since these are the two risk types where machine learning and deep learning techniques have been most extensively applied and studied.

2.2 Loan Default Prediction

Loan default prediction is the task of estimating the likelihood that a borrower will fail to repay a loan according to its agreed terms, and it sits at the core of credit risk management. Historically, this task has relied on credit scoring models, structured, quantitative frameworks that translate borrower characteristics into a single risk score or default probability. Chen et al. [33] and Abdou and Pointon [34], in their respective reviews of credit risk assessment methods, trace this history through a progression of statistical techniques, beginning with simple univariate ratio analysis and moving toward multivariate statistical models capable of weighing several borrower characteristics simultaneously. The traditional statistical methods at the centre of this development, including logistic regression and linear or two group discriminant analysis, are still widely used because they provide clear and easy to check results. A lender or regulator can see exactly which borrower characteristics influenced a particular score. The work in [43], [44], for example, both applied discriminant analysis to credit scoring, with one focusing on consumer lending and the other on small and medium-sized enterprises (SMEs), illustrating how traditional statistical methods were used in financial institutions for loan default prediction before machine learning and deep learning methods became more widely used. A key limitation of these traditional statistical approaches is their reliance on linear or near-linear relationships between borrower characteristics and default risk. This creates a gap that machine learning and deep learning techniques can help address, as discussed later in this work.

2.3 Fraud Detection

Fraud detection, the second major focus of this review, is conceptually distinct from loan default prediction in that it seeks to identify deliberate deception rather than an inability to repay. The literature reviewed in this paper generally distinguishes between three overlapping categories of financial fraud. Transaction-based fraud involves the unauthorised or fraudulent use of payment instruments, such as stolen card details, manipulated transaction records, or fraudulent payment requests [45], [46]. This type of fraud is commonly addressed using machine learning and deep learning techniques, as demonstrated in studies on credit card transaction fraud [47], [48]. Identity fraud, in contrast, involves the use of stolen, synthetic, or falsified identity information to open accounts, apply for credit, or bypass verification controls [49], [50]. It is more closely associated with Know-Your-Customer (KYC) procedures, which financial institutions use to verify customer identities and reduce fraudulent activities [51]. Behavioural fraud is broader and involves unusual patterns of activity, such as changes in transaction timing, spending behaviour, or other deviations from a customer's established profile [52], [53]. As fraudsters continue to develop new techniques and adapt their behaviour to avoid detection, conventional rule-based systems may struggle to identify such changes [54]. Unlike transaction-based fraud, detecting behavioural fraud often requires examining a customer's activities over time. This has led to the use of sequential and attention-based deep learning models that

can learn patterns across multiple transactions rather than assessing each transaction independently [55].

As financial institutions increasingly adopt digital platforms and cloud-based systems, the boundaries between these three fraud categories have become less distinct [56], [57]. These systems have also created new opportunities for fraud, including credential compromise, cross-tenant data leakage, and large-scale synthetic identity creation. These forms of fraud can overlap and evolve as fraudsters adopt new techniques, creating new challenges for fraud detection. Such challenges can make these forms of fraud difficult to detect using conventional approaches, which highlights the pressing need for deep learning models that can identify complex and evolving patterns of fraudulent activity. These challenges and the role of deep learning in addressing them are discussed in a later section of this work.

2.4 Traditional Approaches to Risk Assessment

Beyond the conceptual risk categories discussed above, it is useful to examine in more depth the traditional tools financial institutions have relied on to assess and manage credit and fraud risk, since their limitations motivate the shift toward ML and DL based approaches discussed in later sections. Although there are a variety of existing traditional financial risk management approaches being used by financial institutions. Among the most commonly used approaches are credit bureau checks, Know-Your-Customer procedures, and rule-based monitoring systems. While these methods have proven valuable in financial sectors, they still present significant drawbacks, particularly when dealing with the increasing complexity and volume of modern-day financial transactions [58]. Table 1 synthesizes the key strengths, risk areas, and limitations of these approaches based on the literature reviewed. Credit bureaus are among the most commonly used mechanisms in loan evaluation. Financial institutions use them to obtain information about a borrower's credit history, existing loans, and to check past repayment behaviour. This information then provides a basis for assessing the borrower's financial reliability and helps the financial institutions decide whether a loan application should be approved or rejected [59]. Studies have shown that credit bureaus are effective in improving loan screening and reducing default rates [60], [61], [62]. In practice, however, there are certain significant challenges. The effectiveness of these systems depends heavily on the availability and completeness of financial data, which varies widely across diverse countries but more pronounced in developing countries. Using Nigeria as a case study, a large portion of adults remains unbanked or underbanked. According to the Global Findex, as reported by [63], about 39% of Nigerians do not have a bank account, and 65% of adults do not save with a financial institution, leaving no credit footprint for bureaus to report. As a result, lenders often lack the credit histories needed to make informed lending decisions. Even in situations when financial records exist, inconsistencies, gaps and errors in existing records often undermine the reliability of bureau scores [64]. A report by [65] also showed that when credit bureau data is incomplete, inconsistent, or inaccurate, it can lead to weak or flawed lending decisions. The study found that the debts reported in financial records do not always match actual repayment behaviour.

Table 1. Synthesis of Traditional Approaches to Loan and Fraud Risk Management and Their Limitations

Traditional approach	Risk area	Key strengths	Key limitations and challenges
Credit bureau checks	Loan/Credit risk	Provides borrowers' credit history, existing loans and repayment behaviour. Supports loan screening and approval decisions and can help reduce default rates.	Limited credit histories, inaccurate, incomplete records and outdated records usually affect assessment. Limited coverage of borrowers with little formal financial activity, making bureau information alone insufficient for comprehensive credit risk assessment.
KYC / Customer Due Diligence (CDD)	Credit/Fraud risk	Verifies customer identity and collects information such as identity documents, occupation, income, background and source of wealth. Helps reduce identity theft, fraud and money laundering risks.	Labour intensive, difficult to maintain continuously. Heavy reliance on manual checks increases the possibility of errors and oversight. Vulnerable to fake or synthetic identities, fabricated documents and outdated customer information.
Rule-based monitoring systems	Fraud risk	Uses predefined rules and thresholds to identify unusual transactions. Effective for detecting known and clearly defined fraud patterns, with flagged transactions reviewed by human experts.	Fixed rules may miss new, evolving and complex fraud patterns. Generate high false-positive rates, increasing analyst workload and operational costs.

This means that relying on credit bureau scores alone can miss important details about a borrower's true creditworthiness. Therefore, there is the need for alternate methodologies.

Know-Your-Customer (KYC) also called Customer-Due-Diligence (CDD) [66] require financial institutions to verify the identity of their customers before granting access to financial services and to help them understand their clients while reducing the risk of fraud or misuse [51], [67]. This means collecting basic personal information such as identity documents, background, occupation, income, and sources of wealth, for every new customer. It is also a structured process that every potential bank customer goes through before entering into an agreement with the bank, and this information is continuously monitored throughout the relationship [68]. KYC procedures help institutions reduce risks associated with identity theft, fraud, and money laundering [67], [69]. However, KYC is a challenging task because it is an ongoing process that requires financial institutions to continuously track changes in customers' financial behaviour [70]. The high volume of customers, evolving regulations, and the manual nature of work make the task even more complex [71]. As a result, this increasing the risk of errors, oversight, and exposure to fraud or other financial crimes. KYC faces other challenges. Criminals can exploit weaknesses in the system by creating fake or synthetic identities, or by submitting stolen or fabricated documents, which often pass verification checks and go undetected [72]. Since KYC relies heavily on documents and manual checks, even reliable customer information can quickly become outdated such as changes in address, job, or other personal details, which shows that the system may struggle to capture real-time changes and reduces its ability to detect risks [66], [71]. This therefore shows the need for supplementary approaches, such as automated monitoring tools which can continuously update customer information in real time and improve the accuracy and timeliness of risk assessments.

Many financial institutions use rule-based monitoring systems to detect fraudulent transactions. These systems apply predefined rules or thresholds to transaction data in order to flag unusual patterns or behaviour [73], [74]. The flagged transactions are then reviewed by human financial experts for

further action. For example, transactions above a certain amount or those carried out repeatedly within a short period may trigger alerts. This approach is useful for identifying known patterns of fraudulent activity; however, it tends to struggle when faced with new or evolving fraud techniques [73]. Because these systems rely on fixed rules, they cannot easily adapt to detect more subtle and complex fraud patterns. As financial transactions become faster and more interconnected, static rule-based approaches are more likely to miss important risk signals. Another major limitation is their low accuracy due to high false-positive rates. Studies show that as much as 95% of flagged alerts may turn out to be legitimate transactions [71], [75]. This means that most alerts do not represent real risks, yet they still require review. As a result, human analysts must spend considerable time examining large volumes of non-suspicious cases, increasing operational costs and workload. The limitations of conventional rule-based systems call for more intelligent and adaptive models for effective risk assessment.

3. REVIEW METHODOLOGY

This review followed a structured, PRISMA-informed approach to identify, screen, and select relevant literature. The process involved applying predefined search and selection criteria to ensure that the studies included in the review were relevant and met the requirements established for the review.

3.1 Databases Searched

Literature was identified through searches of major academic databases and scholarly search platforms, including Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. These searches were supplemented with targeted searches of other relevant academic sources, including preprint and working-paper repositories such as SSRN, to capture relevant and recent studies not yet available in indexed journals.

3.2 Search Keywords

Search strings combined a technique, concept, or background term with a domain term using Boolean operators. Two broad groups of search strings were used, reflecting the review's dual conceptual and technical scope.



Background and conceptual searches included, for example: (“financial institutions” AND “economic development” OR “economic stability”); (“credit bureau” OR “Know-Your-Customer” OR “KYC”) AND (“credit risk” OR “fraud prevention”); (“rule-based” OR “transaction monitoring”) AND (“anti-money laundering” OR “fraud detection”); and (“FinTech” AND “bibliometric”).

Technique-focused searches included, for example: (“random forest” OR “gradient boosting”) AND (“credit risk” OR “loan default”); (“logistic regression” OR “discriminant analysis”) AND “credit scoring”; (“LSTM” OR “GRU” OR “convolutional neural network”) AND (“fraud detection” OR “credit risk”); (“machine learning” AND “deep learning” AND “comparative analysis”); (“explainable AI” OR “interpretability”) AND (“financial risk” OR “credit scoring”); and (“class imbalance” OR “SMOTE”) AND “credit risk prediction”.

Searches were conducted iteratively across the major themes of the review, and the results were re-screened when new sub-themes emerged during the full-text review.

3.3 Inclusion Criteria

Studies were included if they:

- (i) addressed the role, stability, or risk exposure of financial institutions, established risk-type definitions (credit, fraud, liquidity, market, or operational risk), or described traditional risk assessment approaches (credit bureaus, Know-Your-Customer procedures, rule-based monitoring); or applied one or more machine learning or deep learning techniques to loan default prediction, credit risk assessment, or fraud detection in a financial services context;
- (ii) were published in a peer-reviewed journal, conference proceedings, or a reputable preprint repository;
- (iii) reported empirical results, conceptual analysis, a systematic review, or a bibliometric analysis relevant to the review's scope; and
- (iv) were published between 2011 and 2026, with the large majority concentrated in 2018–2026 to reflect more recent technical developments.

3.4 Exclusion Criteria

Studies were excluded if they:

- (i) addressed financial risk types outside credit and fraud risk (for example, pure market-risk or currency-risk forecasting) without a clear credit or fraud application;
- (ii) were purely theoretical or algorithmic contributions with no financial risk application, evaluation, or conceptual relevance;
- (iii) were extended abstracts of a study already captured through its full journal version; or
- (iv) could not be accessed in full text through available institutional or open-access channels.

3.5 Selection Outcome

A PRISMA-informed literature review approach was adopted to identify and screen studies relevant to financial risk assessment, with particular emphasis on credit risk assessment, loan default prediction, fraud detection, data imbalance, and synthetic data generation. The review covered both traditional financial risk assessment approaches and modern machine learning and deep learning techniques, thereby providing a basis for examining the evolution of financial risk modelling and the transition from conventional statistical and rule-based

methods to data-driven computational approaches.

The literature search identified 303 records, comprising 291 records obtained through database searching and 12 additional records identified through preprint and working-paper repositories. No duplicate records were identified. All 303 records therefore proceeded to the initial automated and manual screening stage. Following this screening, 169 records were excluded based on their lack of sufficient relevance to the research objectives and predefined review themes, leaving 134 references for detailed relevance assessment. Of these, 25 references were subsequently excluded, resulting in 109 references being retained as the core literature pool for the review. The screening process considered the publication's relevance to one or more of the following themes:

- (i) traditional credit risk assessment and credit scoring,
- (ii) loan or mortgage default prediction,
- (iii) financial and banking fraud detection,
- (iv) machine learning and deep learning techniques for financial risk prediction,
- (v) class-imbalance handling and data augmentation,
- (vi) synthetic data generation for financial-risk modelling, and
- (vii) explainable artificial intelligence and model interpretability in financial risk assessment.

Studies employing traditional statistical, econometric, rule-based, and expert-driven approaches were included where they provided relevant foundations for financial risk assessment. These approaches included methods such as logistic regression, discriminant analysis, statistical credit-scoring models, probability-based approaches, financial-ratio analysis, expert judgement, rule-based systems, and other conventional techniques used for credit risk, default prediction, or fraud detection. Their inclusion enabled comparison with more recent data-driven approaches and helped establish the methodological progression within the field.

Studies employing machine learning and deep learning techniques were also included, with particular attention to algorithms such as decision trees, random forest, support vector machines, artificial neural networks, ensemble learning, convolutional neural networks, recurrent neural networks, long short-term memory networks, gated recurrent units, graph neural networks, transformers, and hybrid architectures. Studies addressing SMOTE, resampling, GAN-based augmentation, synthetic data generation, and imbalance-learning techniques were considered because of their relevance to data scarcity and class-imbalance challenges associated with financial fraud and credit-risk prediction.

Following the relevance screening, 109 references were retained as the core literature pool for the review. The selected studies were subsequently organized thematically into traditional financial risk assessment approaches, credit-risk and loan-default prediction, financial fraud detection, broader financial-risk modelling, data imbalance and augmentation, synthetic data generation, explainable artificial intelligence, and privacy-preserving or federated learning approaches. The PRISMA-informed study selection flow is presented in Figure 2 and summarized in Table 2.

Table 2. PRISMA-informed study selection process

Stage	Description	Number (n)
Identification	Records identified through database searching (Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar)	[291]
Identification	Additional records identified through preprint/working-paper repositories (e.g., SSRN)	[12]
Identification	Total records identified	[303]
Screening	Duplicate records removed	[0]
Screening	Records after duplicates removed	[303]
Screening	Records subjected to initial automated and manual screening	[303]
Screening	Records excluded during initial automated and manual screening (see Section 3.4)	[169]
Eligibility	References identified as potentially relevant and retained for detailed relevance assessment	[134]
Eligibility	References excluded following detailed relevance assessment	[25]
Included	References retained as the core literature pool for the review (see section 3.3)	109

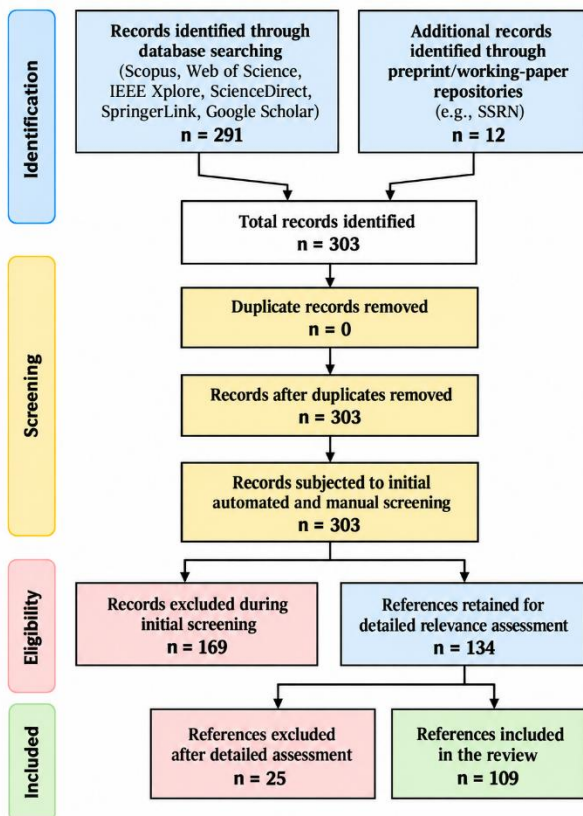


Figure 2: PRISMA-informed study selection flow diagram

4. MACHINE LEARNING APPROACHES FOR LOAN DEFAULT PREDICTION

4.1 Statistical and Regression-Based Models

Logistic regression and discriminant analysis remain the most widely used starting points for credit risk classification, largely because of their interpretability relative to more complex models. The work in [43] applied a two-group discriminant function to consumer loan data from a Vietnamese commercial bank using demographic, socio-economic, and loan-specific variables, achieving an average classification accuracy of 73%. Researchers in [76] directly compared discriminant analysis against logistic regression for predicting default risk among small and medium-sized enterprises in Tunisia., finding that both methods produced statistically significant classifications, although their performance varied across sectors. To address the class imbalance common in real-world credit datasets, a regularized LASSO-logistic regression ensemble was proposed in [44]. It performed better than decision trees, logistic regression, and random forests based on AUC and F-measure. Another ensemble approach, logistic-BWE, was proposed in [77] by combining sample-balancing methods with multiple logistic regression models. It improved the detection of minority default cases.

4.2 Tree-Based and Ensemble Methods

Several studies have examined tree-based and ensemble methods for credit risk prediction, largely because they have consistently shown strong performance on tabular financial data. Ghatasheh [78], for example, applied random forest to credit risk classification and found that it performed better than the individual classifiers considered. Using Ukrainian credit registry data, Krasovytskyi and Stavitskyk [37] predicted mortgage default over a one-year period and found that random forest and extreme gradient-boosting decision trees provided the best balance between accuracy and precision. A comparison of XGBoost, gradient boosting, random forest, KNN, and decision trees across two loan-approval datasets showed that XGBoost achieved the highest accuracy of 84% on one dataset, while random forest recorded 85% on the other [79]. Similarly, a stacking ensemble was found to outperform individual classifiers in loan application credit risk prediction [80]. In student loan default prediction, Wang et al. [81] combined different classifiers in a heterogeneous ensemble and used SHAP to explain the predictions of the model. SHAP shows the contribution of individual features to a prediction, helping to identify the factors that influence whether a borrower is classified as likely to default. This makes the decision of the model easier to understand, rather than providing only the final prediction. Such interpretability is important in credit risk assessment, where understanding the reasons behind a prediction can be as important as the prediction itself. For peer-to-peer lending, LightGBM achieved the highest AUC across three datasets, with scores of 70.77% for Lending Club, 93.25% for Australia, and 77.85% for Taiwan [82]. The study also reported that Bayesian optimization methods such as Hyperopt and Optuna produced similar accuracy to grid search while reducing runtime substantially. Other studies [83], [84] similarly reported better performance from ensemble classifiers than from individual algorithms in loan default prediction. The findings indicate that ensemble and tree-based methods can perform well in different credit risk applications, although their performance depends on the dataset, lending context, and

evaluation measure used.

4.3 Support Vector Machines

Zhou (2022) [85] proposed a hybrid model combining fuzzy integral theory with SVM for enterprise credit risk evaluation within supply chain finance, using fuzzy density weighting to combine multiple child-SVM outputs. The fused model outperformed both single-SVM and voting-based SVM ensembles in classification accuracy, and was noted to handle small sample sizes and non-normal data distributions better than purely statistical approaches.

4.4 Machine Learning for Fraud Detection

Beyond credit default prediction, several studies have focused on using ML techniques to detect fraudulent transactions. For example, the work in [47], [48] compared several machine learning algorithms such as, random forest, logistic regression, and Naïve Bayes, using credit card fraud datasets. Their results showed that tree-based and ensemble methods generally performed better in detecting fraudulent transactions. Another important issue in fraud detection is the imbalance between legitimate and fraudulent transactions. Fraud cases are usually much fewer than legitimate transactions, which can make it difficult for machine learning models to identify the minority fraud cases. Balancing techniques therefore help to reduce this problem by increasing the representation of the minority fraud class. Among the techniques reviewed, SMOTE was a common approach for addressing class imbalance. It generates synthetic examples of minority-class cases rather than simply duplicating existing fraud records. The reviewed studies also showed that the choice of balancing technique can affect fraud detection performance, even when the same classifier is used [26], [86], [87].

4.5 Broader Applications in Enterprise and Digital Financial Risk

ML techniques have also been applied to enterprise, digital financial, and supply chain risk assessment. A random forest-based enterprise risk assessment framework achieved an accuracy of 92%, compared with 85% obtained by the Support Vector Machine model across four experiments [88]. Another study compared several ML algorithms for digital financial risk assessment, with the aim of optimizing both accuracy and processing timeliness [39]. Ensemble methods have also been used to improve financial risk prediction. Random forest, AdaBoost, XGBoost, and LightGBM were combined with explainable AI techniques for credit risk assessment, with SHAP used to show the factors contributing to the predictions of the model [89]. This is important because while these models can provide strong predictive results, their decisions may be difficult to understand. ML has also been applied to supply chain finance, where it was used to predict and prevent financial risks in supply chain enterprises [90].

These studies show that ML techniques are being applied across different areas of financial risk assessment, rather than being limited to credit default and fraud detection. Tree-based and ensemble methods, such as random forest, XGBoost, and LightGBM, feature prominently in these applications because of their strong predictive performance. However, the complexity of these models can make their predictions difficult to interpret, which explains the growing use of explainable AI techniques such as SHAP to provide insight into how the models arrive at their predictions.

5. DEEP LEARNING TECHNIQUES

5.1 Artificial Neural Networks

Feedforward artificial neural networks (ANNs) represent the earliest deep learning applications in this literature, predating the more recent shift toward recurrent and convolutional architectures. Unlike traditional statistical models, ANNs can learn non-linear relationships between input variables and credit outcomes, making them suitable for financial data where the relationship between borrower characteristics and default risk may not be straightforward [91]. Pacelli and Azzollini [92], for example, applied an ANN model to credit risk management using data from Italian manufacturing companies and demonstrated its ability to model credit risk from financial information. Similar applications were reported in other credit-risk settings. An ANN-based model was developed for evaluating the credit risk of commercial bank customers [93], while another study used an ANN approach to predict credit risk and compared its performance with linear regression [94]. The results from these studies support the use of neural networks as an alternative to conventional statistical models, particularly where the relationships among credit variables are complex and non-linear.

The use of ANN models has also been examined across different credit-risk applications. A systematic review of 76 credit-risk studies identified ANN and multilayer perceptron (MLP) among the deep-learning approaches used in credit risk assessment [95]. However, the early use of ANN models also revealed some limitations. Predictions from ANN-based credit risk models can be difficult to interpret because the relationship between the model inputs and the resulting prediction is not always clear [96], [97]. This is particularly important in credit risk assessment, where financial institutions may need to justify why a borrower was classified as low or high risk. This limitation, together with the increasing availability of larger and more complex financial datasets, have encouraged researchers to explore other deep-learning architectures.

Recent reviews indicate a gradual shift from basic feedforward neural networks toward specialised architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, transformers, and graph-based models [32], [96]. These architectures can capture patterns across sequences, identify local patterns in structured data, and learn complex relationships within financial data. This progression shows efforts by various researchers to develop deep-learning models that can better handle the complexity of financial risk data.

5.2 Recurrent Architectures for Sequential Credit Risk

Because loan repayment behaviour develops over time, researchers have increasingly explored recurrent neural networks that can learn from sequences of borrower activities. For example, [98] proposed a cascaded Long Short-Term Memory–Gated Recurrent Unit (LSTM–GRU) model for loan default prediction. The model combines the ability of LSTM to retain information over longer periods with the simpler and more efficient structure of GRU. The study also tested different learning rates and optimisation methods to assess the model's performance. Further improvements have been made by incorporating attention and residual mechanisms into recurrent models. A Residual Enhanced Encoder Bidirectional Long Short-Term Memory (ResE–BiLSTM) model was proposed in [38] to capture important patterns that may occur at different

points in a repayment history of the borrower. The model used an attention mechanism to focus on important information and residual connections to help retain information across the network. It was evaluated using the Freddie Mac Single-Family Loan-Level Dataset and compared with LSTM, BiLSTM, GRU, CNN, and RNN models. Hybrid approaches have also been explored for loan default prediction. Xie and Huang [99] combined CatBoost with GRU, together with sample optimisation and bagging techniques, to improve prediction under imbalanced data conditions. This approach combines the strengths of a tree-based machine-learning model with a recurrent neural network, allowing both structured borrower information and sequential patterns to be considered in the prediction.

5.3 Convolutional and Attention-Based Networks for Fraud Detection

Convolutional Neural Networks (CNNs) and attention-based models have been widely used for transaction-level fraud detection because they can identify patterns in transaction data. CNN-based models have been applied to online transaction and e-commerce fraud detection [99], [100], while an attention-based neural network was developed to capture both the order of transactions and the relationships between them in credit card fraud detection [101]. Another study combined competitive swarm optimisation with a deep neural network to improve fraud detection performance [101]. More recent studies have explored transformer-based and other advanced deep-learning approaches. A blockchain-assisted Transformer-CNN framework combined several transformer models to capture temporal and contextual information from transaction data for real-time digital payment fraud detection [102]. Another deep-learning framework combined sea-horse optimisation with a stacked contractive autoencoder to address false alarms and class imbalance in banking fraud detection [103]. RNN-based models, including Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), have also been compared with tree-based models for imbalanced fraud detection. The findings suggest that the choice of model involves a balance between detection performance and computational efficiency [104].

5.4 Hybrid Deep Learning Models for Enterprise and Systemic Risk

A growing number of studies have combined different deep-learning architectures or integrated deep learning with traditional machine-learning methods to improve financial risk prediction. One study proposed a hybrid Convolutional Neural Network (CNN) model for bankruptcy prediction and used Synthetic Minority Over-sampling Technique (SMOTE) to deal with the imbalance in bankruptcy data [105]. Another study developed ExHybridNet, which combines CNN, an attention mechanism, and random forest for corporate financial risk prediction. The model was tested using data from companies in China and achieved better accuracy, precision, and F1-score than several traditional ML, standalone deep-learning, and other hybrid models [106]. SHAP was also used to identify the factors that contributed to the model's predictions. Hybrid recurrent models have also been applied to financial risk prediction. A CNN-LSTM-GRU model was developed as an early warning system, combining CNN for feature extraction with LSTM and GRU for learning patterns that develop over time [107].

A broader review of deep learning in financial risk prediction

also highlighted the rapid development of these approaches and their increasing use across different financial applications [40]. Literature review shows a progression from basic feedforward ANN models to recurrent networks and, more recently, hybrid and attention-based models. The main aim of these developments is to improve the ability of deep-learning models to capture complex patterns in financial data while also addressing issues such as class imbalance, prediction accuracy, and model interpretability. The comparison between traditional ML and deep-learning approaches is discussed in the next section, with particular attention to whether the additional complexity of deep-learning models leads to meaningful improvements in financial risk prediction.

6. DISCUSSION

6.1 Performance in Loan and Credit Risk Studies

The selected studies summarized in Table 3 show considerable variation in credit risk prediction performance across datasets and modelling approaches. Earlier studies were based largely on statistical methods and conventional machine-learning algorithms. Duong et al. [43] reported 73% accuracy using discriminant analysis for consumer loan data, while Alagic et al. [79] obtained 84% accuracy with XGBoost and 85% with Random Forest on two loan-approval datasets. Perera and Premaratne [80] adopted a stacking ensemble and reported 78% accuracy, 78% precision, 92% recall, 0.84 F1-score and 0.75 ROC-AUC. These show the shift from individual classifiers to ensemble methods, although the reported performance varies with the evaluation measure used.

Class imbalance is another recurring issue in credit-risk prediction. Abedin et al. [108] combined weighted SMOTE with ensemble learning and obtained 0.9822 for both G-Mean and AUC. Mapfumo and Shongwe [109] also that the performance of the model could improve if imbalance is addressed. On the German dataset, SMOTE-ENN with MLP achieved 95.4% accuracy and an F1-score of 0.928, whereas the same imbalance-handling strategy combined with Random Forest produced 82.1% accuracy and an F1-score of 0.789 on the Taiwanese dataset. The difference suggests that the effectiveness of a model is closely related to the dataset and the way the class distribution is handled.

These findings do not show a consistent advantage for deep learning over conventional machine learning. Thuy et al. [110] obtained 85.55% accuracy with a Deep Neural Network, but Random Forest gave more balanced results across the measures considered, while Gradient Boosting recorded stronger recall. Dendramis et al. [91] likewise compared an ANN-based approach with logit models. These findings indicate that increasing the complexity of a model does not automatically lead to better credit-risk prediction.

Another issue emerging from the literature is the temporal nature of financial behaviour. Many studies on credit risk are based on structured or static data. However, repayment behaviour develops over time, and some patterns may only become apparent when successive observations are examined together. This has led to the use of recurrent architectures such as LSTM, GRU and BiLSTM to capture temporal dependencies in repayment and other financial sequences [38], [98], [99]. These models are particularly relevant when earlier financial behaviour can provide information about later repayment outcomes.

Table 3. Selected Reported Performance Results for Loan and Credit Risk Prediction Studies

Author(s)	Loan / credit-risk application	Model / approach	Reported result / finding
Duong et al. [43]	Consumer loans, Vietnam	Two-group discriminant analysis	72.3% average accuracy in classifying consumer-loan customers.
Abedin et al. [108]	Small-business credit risk	Weighted SMOTE + ensemble learning	G-Mean = 0.9822; AUC = 0.9822. Combining resampling with ensemble learning improved performance on the imbalanced data.
Alagic et al. [79]	Loan approval / credit risk	XGBoost, Random Forest, Gradient Boosting, KNN and others	XGBoost = 84% accuracy; Random Forest = 85% accuracy. Results varied across datasets.
Perera & Premaratne [80]	Loan application credit risk	Stacking ensemble with Logistic Regression	Accuracy = 0.78; Precision = 0.78; Recall = 0.92; F1 = 0.84; ROC-AUC = 0.75. The ensemble performed better than the individual models on key measures.
Zhao et al. [128]	Credit risk with class imbalance	Resampling techniques with traditional classifiers and ensembles	On Lending Club, KNN G-Mean increased from 0.1168 to 0.5715 with SENN, showing the effect of resampling on minority-class detection.
Souadda et al. [82]	P2P lending: Lending Club, Australia and Taiwan	LightGBM, XGBoost, RF and LR with hyperparameter optimisation	LightGBM AUC: 70.77% (Lending Club), 93.25% (Australia), 77.85% (Taiwan). Performance varied across datasets.
Thuy et al. [110]	Student credit scoring, Vietnam	RF, Gradient Boosting, SVM and DNN	DNN = 85.55% accuracy. RF gave more balanced results, while Gradient Boosting showed stronger recall.
Mapfumo & Shongwe [109]	German and Taiwanese credit risk	MLP, CNN, LSTM, GRU and traditional ML with SMOTE, ENN and SMOTE-ENN	German: SMOTE-ENN + MLP = 95.4% accuracy, F1 = 0.928. Taiwan: SMOTE-ENN + RF = 82.1% accuracy, F1 = 0.789. The study used primarily static/tabular credit data. For the LSTM and GRU training, the static/tabular German credit data were treated as a single-time-step sequence because they lacked explicit temporal attributes
Ramachandra & Vaithiyanathan [111]	Loan default with distributed financial data	Federated WGAN + differential privacy + CTGAN	95% accuracy, compared with 82% for the non-federated model and 73% for FLIGAN.

The results in shown in Table 3 vary considerably across lending environments. Souadda et al. [82] reported LightGBM AUC values of 70.77% for Lending Club, 93.25% for Australia and 77.85% for Taiwan. Mapfumo and Shongwe [109] obtained different results on the German and Taiwanese credit datasets. For the LSTM and GRU experiments, the German dataset consisted of static credit records, with each record representing a borrower through a single set of credit attributes. Since the dataset had no explicit temporal observations, the authors presented these attributes to the recurrent models as a single-time-step input rather than as a sequence of monthly observations. The study therefore showed that LSTM and GRU can be applied to static credit-risk data, although temporal dependencies cannot be captured in this setting.

Recent studies have started to combine recurrent models with techniques for handling imbalance and generating additional data. Xie and Huang [99], for example, integrated SMOTE-ENN, CatBoost-GRU and Bagging, reporting 0.9991 AUC, 98.75% accuracy and 0.9937 F1-score in the main experiment. Ramachandra and Vaithiyanathan [111] approached data scarcity and privacy from a different direction by combining a

federated WGAN with differential privacy and CTGAN. Their framework achieved 95% accuracy, compared with 82% for the non-federated setup and 73% for FLIGAN.

This analysis show that credit risk performance is strongly influenced by the nature of the data, the presence of class imbalance, the pre-processing strategy and the model architecture. Conventional machine learning methods remain useful for structured credit data, while recurrent models offer a way to represent temporal dependencies that may be missed by static approaches. This progression provides the basis for investigating a hybrid framework that can model sequential financial behaviour while also addressing the data limitations and imbalance found in loan-default prediction.

6.2 Performance in Fraud Detection Studies

Research on fraud detection shows that fraudulent transactions usually make up only a small fraction of financial datasets, making the problem difficult. This imbalance can affect model performance and makes the choice of classifier and method used to address it important.

Table 4. Selected Reported Performance Results for Loan and Credit Risk Prediction Studies

Author(s)	Fraud application	Model / approach	Reported result / finding	Key issue addressed
Varmedja et al. [48]	Credit-card fraud	Logistic Regression, Random Forest, Naïve Bayes, MLP + SMOTE	The four models were evaluated after SMOTE-based balancing and achieved strong classification performance.	Class imbalance in conventional ML
Jurgovsky et al. [117]	Credit-card fraud	LSTM sequence classifier compared with Random Forest	LSTM improved fraud detection for offline transactions by modelling transaction sequences. The study also found that sequential and static models detected partly different fraud cases.	Sequential transaction behaviour and historical cardholder information
Benchaji et al. [118]	Credit-card fraud	LSTM + attention + UMAP + SMOTE	The LSTM-attention model achieved approximately 96.7% accuracy, 98.85% precision and 91.91% recall on the European credit-card dataset.	Long-term transaction dependencies and class imbalance
Xie et al. [100]	E-commerce fraud	CNN compared with LR, SVM and RF	CNN achieved 83.60% fraud prediction accuracy, compared with 80.81% for LR, 70.10% for SVM and 70.35% for RF.	Class imbalance and cold-start problem
Ming et al. [112]	Auto-insurance and credit-card fraud	CNN + ML classifiers + soft voting	Credit-card data: 99.99% accuracy, 100% precision, 99.97% recall, 100% F1 and 100% AUC.	Combining deep features with conventional classifiers
Chen et al. [113]	Credit-card fraud	FDNN + intelligent sampling + self-supervised learning	F1 = 0.83 at a 1.4% fraud-rate threshold.	Severe imbalance, noisy labels and changing fraud rates
Ge et al. [115]	Imbalanced credit-card fraud	Gated-attention GAN + classifier	F1 improved from 0.770 to 0.875 after synthetic-record augmentation.	Minority-class scarcity and imbalance
Becerra-Suarez et al. [116]	Bank fraud	XGBoost + Gaussian-noise-generated synthetic data	99.95% accuracy and 99.95% AUC.	Data scarcity and class imbalance
Fnu et al. [102]	Digital payment fraud	Transformer + CNN + feature selection + blockchain	Accuracy of 99.713%, 99.689% and 99.768% across three datasets; AUC values exceeded 99.28%.	Real-time detection and computational requirements

Varmedja et al. [48] evaluated Logistic Regression, Random Forest, Naïve Bayes and Multilayer Perceptron, using SMOTE to address the severe class imbalance in the credit-card dataset. Random Forest achieved the highest accuracy of 99.96%, followed by Multilayer Perceptron (99.93%), Naïve Bayes (99.23%) and Logistic Regression (97.46%).

The work of Xie et al. [100] compared CNN with Logistic Regression, SVM and Random Forest and reported 83.60% fraud prediction accuracy with CNN, compared with 80.81%, 70.10% and 70.35%, respectively. Ming et al. [112] combined CNN feature extraction with machine learning classifiers and soft voting, with the combined approach outperforming the individual classifiers considered in the study. This work further suggests that combining deep learning features with conventional classifiers can improve fraud detection compared with individual models.

To address the ongoing issue of class imbalance in existing studies, researchers have adopted different approaches to reduce its effect on model performance. Chen et al. [113] used intelligent sampling together with self-supervised learning to reduce the imbalance and the effect of noisy labels. The model achieved an F1-score of 0.83 at a fraud-rate threshold of 1.4%. Albalawi and Dardouri [114] used SMOTE to balance the credit-card data and applied focal loss in the deep-learning model to improve the detection of difficult fraud cases. Random Forest recorded 99.95% accuracy, 0.8256 F1-score and 0.9759 ROC-AUC, while the deep-learning model achieved the highest precision. Another response to the limited number of fraud cases has been the use of synthetic data. The generation of synthetic fraud records by Ge et al. [115] through a gated-attention GAN increased the F1-score from 0.770 to 0.875, suggesting improved detection of the fraud class. Becerra-Suarez et al. [116] also generated additional data using

Gaussian noise and combined them with XGBoost, obtaining 99.95% accuracy and 99.95% AUC. These results demonstrate the potential of data augmentation, although the effectiveness of such approaches still needs to be examined using class-specific measures.

The sequential nature of transaction data has led researchers to explore recurrent neural networks for fraud detection. Jurgovsky et al. [117] formulated credit-card fraud detection as a sequence-classification problem and used LSTM to model transaction sequences. Their findings showed that the sequential model and the static approach identified partly different fraudulent cases, indicating that transaction history can provide information that may not be captured when transactions are analysed independently. Benchaji et al. [118] further developed the recurrent approach by combining LSTM with attention, UMAP and SMOTE. On the European credit-card dataset, the model achieved approximately 96.7% accuracy, 98.85% precision and 91.91% recall. These results suggest that incorporating transaction history can improve the representation of fraudulent behaviour, particularly where suspicious activity becomes apparent through a sequence of transactions rather than an isolated event.

More recent work has introduced additional concerns beyond prediction. Fnu et al. [102] combined Transformer and CNN components with feature selection and blockchain for digital-payment fraud detection, reporting accuracy values of 99.713%, 99.689% and 99.768% across three datasets. In a broader comparison involving nine fraud datasets, Yapp and Yeh [119] found that performance varied across the models and datasets. Random Forest and XGBoost performed strongly overall, while a convolutional spiking neural network achieved higher recall at a fixed false-positive rate.

Therefore, the evidence in Table 4 points to a show a gradual change in fraud detection research. Conventional machine-learning models remain useful for transaction level classification, while recurrent models address sequential behaviour and transaction history. More recent studies have added imbalance handling and synthetic data techniques as researchers seek to improve detection of the relatively small fraud class. The variation in reported results also shows why fraud detection cannot be adequately assessed using accuracy alone. Precision, recall, F1-score, AUC and false-positive behaviour provide important additional information about model performance.

6.3 Key Challenges

Studies on loan default prediction and fraud detection have reported several challenges that affect the reliability and practical use of ML and DL models in financial risk assessment. The major challenges identified from the review are discussed below and summarized in Table 5.

6.3.1 Interpretability and Explainable AI (XAI)

One major challenge in both machine-learning and deep-learning applications for financial risk assessment is understanding how a model arrives at its prediction. This is particularly important for deep-learning models because their complex structures can make it difficult to identify how individual variables influence the final decision. The authors in [120] reviewed different explainable artificial intelligence (XAI) methods used in finance and noted that the lack of transparency in deep-learning models can limit their use in situations where decisions need to be clearly explained. Similarly, a review of 138 studies published between 2005 and

2022 found that the use of XAI in finance has increased, although its application differs across financial tasks [121].

Several studies have therefore incorporated XAI into financial risk models. It has been combined with deep learning for credit card default prediction [122], integrated with federated learning for financial fraud detection, and used alongside ensemble learning for mobile-money fraud detection [123]. In another study, SHAP was used to identify the factors contributing to enterprise financial distress predictions [124]. Ni et al. [125] used time-series visualisation to help users understand the temporal patterns influencing AI-based risk decisions. The issue has also extended to generative artificial intelligence, where the use of models such as large language models and generative adversarial networks introduces additional concerns about transparency and governance [126].

In financial risk assessment, prediction accuracy alone does not fully address the needs of practice. There is also a need to understand the reasons behind a model's prediction, particularly when the decision may affect borrowers, financial institutions, or regulatory processes. Explainability is therefore an important consideration when using complex machine-learning and deep-learning models for financial risk assessment.

6.3.2 Class Imbalance and Data Scarcity

Another recurring challenge observed in the review is the severe class imbalance that characterises most credit and fraud datasets, which occurs when loan default or fraudulent cases make up only a small proportion of the dataset. In loan default prediction, this means that borrowers who fail to repay their loans are much fewer than those who repay as expected. Similarly, in fraud detection, fraudulent transactions usually represent only a small fraction of all transactions. This imbalance can make it difficult for a model to correctly identify these minority cases, as a model may achieve high overall accuracy while still missing many loan defaults or fraudulent transactions. A systematic review of ensemble learning for imbalanced credit scoring found that resampling and ensemble methods generally improve the detection of minority cases, although no single combination performed well across all datasets [127]. A weighted SMOTE-ensemble approach was proposed by combining weighted oversampling with bagging to improve the representation of minority cases [108]. Another comparative study of resampling techniques for credit risk prediction also showed that the effectiveness of a balancing method depends on the model and the characteristics of the dataset [128].

Another challenge that needs to be considered alongside class imbalance is data scarcity. Data scarcity is a broader problem in which the amount of available data may be insufficient for training complex models effectively. This is particularly important for deep learning, since these models generally require large amounts of data to learn useful patterns and produce reliable predictions. Financial data can also be difficult to obtain because loan and transaction records contain sensitive information and are usually held by individual financial institutions. Consequently, researchers have increasingly explored synthetic data generation as a way of increasing the amount of training data without relying entirely on additional real customer records [129]. Generative Adversarial Networks (GANs) have received considerable attention for this purpose. A review of GAN-based data augmentation for credit card fraud detection identified GANs as an increasingly used approach for generating additional minority-class records and addressing the limited availability of fraudulent transactions

[129], [130], [131]. These show that synthetic data generation is not only being considered as a way of balancing datasets but also as a means of producing additional examples of rare financial events.

Several reviewed studies have reported improvements in the performance of the developed models after synthetic data were introduced into financial risk models. A GAN-based approach for financial-statement fraud detection generated synthetic fraud-prone samples and reported performance comparable with supervised models and better than the unsupervised approaches examined [132]. A gated-attention GAN (GA-GAN) was used to generate synthetic fraudulent transactions. When the synthetic records were added to the training data, the F1-score on one of the evaluated datasets increased from 0.770 to 0.875 [115]. Another study used an embedding-aware conditional GAN to generate minority-class fraudulent transactions and reported that the approach was able to produce stable results even when labelled data were limited [133].

The use of synthetic data has also been extended to loan default prediction. A federated Wasserstein GAN (WGAN) framework was proposed to generate synthetic credit-risk data while keeping the original loan data distributed across institutions. The framework combined federated learning, differential privacy, WGAN and CTGAN, and achieved 95% accuracy, compared with 82% for the non-federated approach and 73% for the FLIGAN approach [111]. GANs are not the only approach being explored. Other studies have used methods such as Variational Autoencoders (VAEs), Gaussian-noise augmentation and hybrid generative approaches to create additional financial records. For example, a 2025 study compared Gaussian-noise augmentation with SMOTE and ADASYN for bank fraud detection and found that XGBoost trained with the Gaussian-noise-generated data achieved an accuracy of 99.95% and an AUC of 99.95% [116]. Similarly, a recent comparison of synthetic oversampling methods reported that GAN- and VAE-generated data produced higher precision and F1-scores than SMOTE and ADASYN in the evaluated credit-card fraud experiments [134]. The implication of these findings is that the choice of synthetic-data generation method can influence the subsequent performance of the risk model. The growing use of synthetic data therefore provides a possible response to both data scarcity and class imbalance in financial risk assessment.

However, synthetic data should not be considered a replacement for real financial data. While it can help address data scarcity, class imbalance, and privacy concerns, its quality depends on how well the generative model captures the patterns and relationships in the original data. Poorly generated synthetic data may introduce bias or unrealistic patterns, which can affect the reliability of the resulting model [135]. Other work on synthetic financial data has also highlighted the need to evaluate both data utility and privacy before synthetic records are used for financial modelling [136]. Regulatory work in financial services has similarly identified both the opportunities and risks of synthetic data, including privacy, data quality, governance and the possibility of misleading model results [137].

Therefore, researchers should be cautious when relying on synthetic data. Where possible and ethically permitted, real financial data should first be obtained and properly protected, after which synthetic data generation techniques can be applied to supplement the dataset and support the research process. Models developed using synthetic data should be validated and,

where necessary, fine-tuned using real-world data before deployment. This ensures that the research findings and predictive models remain relevant to actual financial conditions.

6.3.3 Data Privacy, Federated Learning, and Cross-Institution Collaboration

Machine-learning and deep-learning models often require large amounts of data, but financial institutions cannot freely share customer records because these data contain sensitive personal and financial information and are subject to privacy and regulatory requirements. This creates a situation where institutions may have useful data for improving risk models but cannot simply combine their datasets in a central location. Federated learning has therefore been explored as a way of allowing institutions to benefit from data held by different organisations without directly sharing the underlying customer records [138]. In federated learning, each institution keeps its data locally and trains the model using its own records. The trained model information is then shared with a central server, where the information from the participating institutions is combined to update a shared model [139]. This allows the institutions to collaborate while keeping the original customer data within their respective systems. In credit risk assessment, this approach can help institutions make use of a wider range of data while reducing the need to transfer sensitive customer information [138]. However, federated learning does not remove all privacy concerns, since information exchanged during model training can still be exposed to certain attacks if appropriate protection is not applied [140].

Other privacy-preserving techniques have also been considered for financial applications. These include secure computation and homomorphic encryption, which allow computations to be performed on protected data without requiring the original information to be directly exposed. Such techniques are particularly relevant to financial institutions that need to collaborate across organisations or jurisdictions while meeting data-protection requirements [141]. Privacy concerns have also become more important with the increasing use of cloud computing, fifth-generation (5G) networks, and generative artificial intelligence in banking. Recent work has therefore emphasised the need to consider privacy when financial risk models are designed and deployed, rather than treating it only as a concern after the model has been developed [142].

6.3.4 Deployment, Latency, and Compliance Costs

Another challenge is the computational cost of ML and DL models when they are deployed in real-time financial systems. Although deep-learning models can provide accurate predictions, their complexity may result in slower response times, particularly on devices with limited computing resources such as point-of-sale terminals and ATMs. A hybrid approach combining deep learning with a lightweight regression model was proposed to reduce this problem while maintaining prediction performance [143]. Another challenge is the high number of false-positive alerts in anti-money laundering (AML) systems. Traditional rule-based methods can generate false-positive alerts and struggle to detect new laundering patterns. Hybrid ML/DL approaches, including VAE-GNN models, have been proposed to capture behavioural and relational patterns and reduce unnecessary alerts [144], [145], [146]. Reducing false positives can lower the workload and cost of investigating legitimate transactions.



Table 5. Challenges in Loan Default Prediction and Fraud Detection and Approaches Reported in the Review

Identified Challenge from the Review	Implication for Loan Default	Implication for Fraud Detection	ML/DL Response	Key Attention/Observation
Interpretability / Explainability	Difficulty explaining default predictions.	Difficulty explaining fraud predictions.	XAI techniques such as SHAP and time-series visualisation are used to explain predictions from ML/DL and other advanced financial models.”	XAI improves the transparency of financial risk models by providing interpretable reasons for predictions. However, the underlying complexity of deep-learning models can still limit full interpretability.
Class Imbalance	Default cases are much fewer than non-default cases.	Fraud cases are a small fraction of transactions.	SMOTE, weighted SMOTE, resampling, ensemble methods, GANs.	These methods improve minority-class representation, but their effectiveness depends on the dataset and model.
Data Scarcity	Limited loan data for training complex DL models.	Limited fraud records, especially labelled cases.	GANs, VAEs, Gaussian-noise augmentation, and hybrid generative methods.	Synthetic data increases the available training samples, particularly for loan-default and fraudulent transaction cases, but the generated data must remain representative of real financial data.
Synthetic Data Quality	Synthetic records may not reflect real borrower behaviour.	Synthetic records may contain bias or unrealistic fraud patterns.	Validation of synthetic data; evaluation of data utility and privacy; subsequent validation/fine-tuning with real-world data.	Poor synthetic data can introduce bias and unrealistic patterns, so quality and usefulness must be assessed before use.
Privacy / Data Sharing	Loan records contain sensitive customer and financial information, limiting data sharing.	Transaction records contain sensitive information and cannot freely be shared.	Federated learning, secure computation, homomorphic encryption.	Federated learning supports collaboration without centralising records, but does not eliminate privacy risks during model training and information exchange.
Deployment / Computational Cost	Complex DL models may require high computational resources.	Real-time fraud/AML systems may face latency and computational constraints.	Lightweight and hybrid DL models.	These approaches aim to Reducing cost and latency may affect model performance.
Poor Minority-Class Detection	Defaults may be incorrectly classified despite high overall accuracy.	Fraud cases may be missed despite high overall accuracy.	Precision, recall, F1-score, ROC-AUC and confusion matrix alongside accuracy.	High accuracy does not necessarily indicate good classification performance; multiple metrics such as precision, recall, F1-score and ROC-AUC are therefore needed to provide a more complete assessment.
Interpretability / Explainability	Difficulty explaining default predictions.	Difficulty explaining fraud predictions.	XAI techniques such as SHAP and time-series visualisation are used to explain predictions from ML/DL and other advanced financial models.”	XAI improves the transparency of financial risk models by providing interpretable reasons for predictions. However, the underlying complexity of deep-learning models can still limit full interpretability.



6.4 Research Gaps

The review also shows areas that have received limited attention in the existing literature. These gaps provide a basis for further research and are discussed below.

6.4.1 Fragmentation Between Credit Risk and Fraud Detection Research

As noted in the earlier sections, an important gap in the existing literature is that many reviews treat loan default prediction and fraud detection as separate research problems. Reviews also tend to focus on specific techniques or particular areas of financial risk assessment. For example, some reviews have focused mainly on credit risk assessment methods [33], while others have examined statistical credit scoring techniques [34]. These are examples of a broader pattern in the literature, where credit risk and fraud detection are often discussed separately and recent ML and DL approaches are not considered within the same framework. As a result, there is limited research that examines loan default prediction and fraud detection together and compares ML and DL across both areas. The evidence on the strengths and limitations of the two approaches is therefore spread across different studies. This review addresses this gap by examining both areas within a common comparative framework.

6.4.2 Variation in ML/DL Adoption Across Financial Sectors

The literature also shows uneven adoption of ML and DL across different areas of financial risk assessment. While advanced ML and DL methods are now widely studied in areas such as consumer credit and fraud detection, some other financial sectors still rely mainly on traditional statistical techniques. For example, one study on commercial mortgage default prediction used probit models and linear discriminant analysis rather than the more recent ML and DL approaches [114]. This is an example of the wider difference in the adoption of predictive techniques across financial sectors. It also raises the question of whether the performance improvements reported for ML and DL in consumer credit and fraud detection would also be achieved in areas such as commercial mortgage lending, where the number of available cases may be smaller and the value of individual loans is much higher.

6.4.3 Emerging and Under-Studied Risk Dimensions

The review points to some areas that have received less attention in ML and DL based financial risk assessment, including cybersecurity-related fraud in cloud-based banking, fraud and cybersecurity risks in digital-only banks, and the effect of big-data characteristics on credit risk assessment. Studies have examined cyber risks and fraud in cloud-based banking systems [56] and fraud and cybersecurity threats in digital-only banks [57], while another study examined how the volume, variety, speed, reliability, and value of financial data can affect credit risk assessment [147]. A review of AI-based credit scoring also highlighted the need to better understand which predictive techniques perform reliably under different data conditions [148]. These studies show that financial risk assessment is becoming more complex as financial institutions increasingly adopt digital technologies and the amount and type of available data continue to change. However, much of the existing research still focuses on individual risks or specific datasets. It is therefore difficult to determine whether the performance of ML and DL models remains consistent across

different types and conditions of financial data. More comparative research is needed to examine how these models perform when the risk type, data source, and data characteristics change.

6.4.4 Distribution and Focus of Financial Risk Research

A large bibliometric study covering 2,760 FinTech articles reported a strong increase in FinTech research [149], but did not identify loan default prediction and fraud detection as a distinct area that has been jointly examined, suggesting that these two important financial risks remain largely separated in the existing research landscape. Bibliometric studies also show that financial technology research is not evenly distributed across different risk areas and regions. Some studies have focused on specific areas such as customer due diligence and emerging FinTech risks, with particular attention given to selected countries and regions [66], [150]. A separate bibliometric analysis of 849 FinTech studies also showed that research attention is uneven across regions and topics, with areas such as regional differences, gender disparities, and green finance receiving comparatively less attention [151]. Although the study focused on FinTech adoption rather than financial risk prediction, its findings indicate that FinTech research is not evenly distributed across different regions and application areas. These studies indicate that FinTech research is growing, but remains divided across different topics, regions, and research areas. This supports the need to give greater attention to financial risk assessment research in less-represented regions.

This issue is particularly relevant to Africa, where financial institutions are rapidly adopting digital technologies while facing growing fraud and credit-risk challenges [152], [153], [154]. A systematic review of financial crime research in Africa found that financial crimes are increasing across the continent, including credit-card fraud, cybercrime, mobile-money fraud, financial-statement fraud, and other forms of financial crime [155]. Evidence from Nigerian banks has also shown that digital-payment fraud has a significant effect on bank fragility [156]. Credit risk remains an important concern as well. A study covering 493 banks across 31 Sub-Saharan African countries examined the factors associated with non-performing loans, while another study of African commercial banks found that periods of higher economic-policy uncertainty were associated with increases in non-performing loans [24], [153], [157].

Despite these challenges, much of the ML and DL literature on financial risk assessment is based on datasets and financial systems outside Africa. This creates a need for greater attention to African financial data and institutions. In particular, it remains important to determine whether ML and DL models developed and tested in other regions perform similarly when applied to African loan default and fraud detection data, where differences in financial systems, data availability, customer behaviour, and institutional practices may affect model performance.

7. CONCLUSION

This review examined how machine learning and deep learning techniques are being used in financial risk assessment, with particular attention to loan default prediction and fraud detection. Loan default and fraud are among the most common financial risks faced by financial institutions, as they can result in financial losses, affect institutional stability, and reduce customer confidence. Using a structured PRISMA-informed



process, the review covered 109 studies and traced the shift from traditional risk assessment methods to the increasing use of ML and DL techniques.

Among the machine learning techniques reviewed, Random Forest, XGBoost, Gradient Boosting, LightGBM, and other ensemble methods generally showed strong performance, particularly when applied to structured financial data. Deep learning techniques, such as ANN, CNN, LSTM, GRU, BiLSTM, attention-based networks, and hybrid models, have shown immense ability to capture complex patterns in financial data. Recurrent architectures such as LSTM, GRU, and BiLSTM, as well as hybrid CNN models, showed particular benefits when the risk information was sequential or temporal in nature, such as changes in repayment behaviour over time or patterns across transaction sequences in fraud detection. However, the findings show that the effectiveness of deep learning varies across datasets and financial risk applications, rather than being consistently superior across all cases. Some studies also reported improved results when ML and DL techniques were combined at different stages of the risk assessment process. For example, deep learning can be used to learn complex features or patterns from the data, while machine learning techniques can subsequently be applied for classification or prediction. These suggest that the choice of approach should be guided by the nature of the data, the financial risk being assessed, the evaluation metric, and the way the data are prepared and balanced.

The review also identified several challenges that continue to affect the application of ML and DL in financial risk assessment. These include class imbalance, limited financial data, model interpretability, privacy, computational requirements, and real-time deployment costs. Techniques such as resampling, ensemble learning, explainable AI, federated learning, and synthetic data generation have been used to address these challenges. Synthetic data are particularly useful when financial datasets are limited or highly imbalanced. However, synthetic data should not be treated as a replacement for real financial data. It is better viewed as a means of supplementing available data and supporting the research process, while models developed with synthetic data should ultimately be evaluated and, where necessary, fine-tuned using real financial data before deployment. The review further shows that explainability is becoming increasingly important in financial risk assessment. Although complex ML and DL models may provide strong predictive performance, financial institutions also need to understand the factors responsible for a prediction, particularly when the outcome affects lending decisions, fraud investigations, or regulatory processes. The growing use of techniques such as SHAP therefore provides a means of improving the understanding of model predictions and addressing some of the concerns associated with complex models.

A major observation from the review is that loan default prediction and fraud detection have largely developed as separate areas of research, despite both being major sources of financial risk for financial institutions. This separation makes it difficult to obtain a broader understanding of how ML and DL techniques perform across the two risk areas. The review also found that much of the existing research is based on financial datasets from outside Africa, with comparatively limited attention given to African financial institutions and their data. This is important because differences in financial systems, customer behaviour, data availability, lending practices, and fraud patterns may influence model performance. There is

therefore a need for further empirical studies using real financial datasets, particularly from under-represented regions such as Africa, to compare different ML and DL techniques for both loan default prediction and fraud detection. Such studies would provide stronger evidence on which approaches are most suitable for different financial risk assessment situations and help bridge the gap between research findings and their practical application in financial institutions.

8. REFERENCES

- [1] E. L. Desarrollo, D. E. L. A. Amazonia, B. Una, and D. F. Carvalho, "The Importance Of Financial Institutions For The Development Of The Brazilian Amazon: An Application Of The Social Accounting Matrix," *Rev. Análisis Económico*, vol. 30, no. Octubre, pp. 45–78, 2015.
- [2] U. Adeline, A. E. Emeka, and O. E. Okoi, "Importance of Nigerian Financial Institutions Compliance with the Corporate Governance," *Int. J. Econ. Commer. Manag.*, vol. VIII, no. 10, pp. 123–134, 2020.
- [3] R. Jayalakshmi and T. Gokulnath, "A Study on the Role of Financial Institutions in Economic Development," *Int. J. Foreign Trade Int. Bus.*, vol. 6, no. 2, pp. 208–213, 2025, doi: 10.33545/26633140.2024.v6.i2c.135.
- [4] C. Light and G. E. Nwaobia, "Impact of Financial Institutions on Economic Activities in Nigeria (A Case Study of Commercial Banks Located in Owerri Municipal, Nigeria)," *J. Econ. Allied Res.*, vol. 9, no. 4, pp. 239–254, 2024, [Online]. Available: <https://jearecons.com/index.php/jearecons/article/view/464>
- [5] C. Pazarbasioglu, A. G. Mora, M. Uttamchandani, H. Natarajan, E. Feyen, and M. Saal, "Digital Financial Services," 2020. [Online]. Available: <https://www.worldbank.org/en/topic/financialsector/publication/digital-financial-services>
- [6] P. Sonar and P. KishorJagad, "Financial Institutions and their Role in the Development and Financing of Small Individual Projects.," *NeuroQuantology*, vol. 20, no. 10, pp. 2333–2340, 2022, doi: 10.14704/nq.2022.20.10.NQ55200.
- [7] O. S. Adeusi, N. I. Akeke, O. S. Adebisi, and O. Oladunjoye, "Risk Management and Financial Performance Of Banks In Nigeria," *IOSR J. Bus. Manag.*, vol. 14, no. 6, pp. 52–56, 2013, doi: 10.9790/487x-1465256.
- [8] H. Ahir, G. Dell'Ariccia, D. Furceri, C. Papageorgiou, and H. Qi, "Financial Stress and Economic Activity: Evidence from a New Worldwide Index," 2023. doi: 10.5089/9798400257636.001.
- [9] T. Adamowicz, "Types of Risk in Banking Operations – Categorization and Definitions," *Econ. Reg. Stud.*, vol. 11, no. 4, pp. 37–56, 2018, doi: 10.2478/ers-2018-0034.
- [10] D. Oyetade and P. F. Muzindutsi, "Country Risk and Financial Stability: A Focus on Commercial Banks in Africa," *Risks*, vol. 11, no. 11, 2023, doi: 10.3390/risks11110198.
- [11] A. O. Ademola and K. A. Adegoke, "Understanding the Factors influencing Loan Repayment Performance of Nigerian Microfinance Banks," *J. Manag. Sci.*, vol. 4, no.



- 3, pp. 89–99, 2021.
- [12] T. Jones and G. S. Sirmans, “Understanding Subprime Mortgage Default,” *J. Real Estate Lit.*, vol. 27, no. 1, pp. 27–52, 2019, [Online]. Available: <https://www.jstor.org/stable/26771064>
- [13] A. Yahaya, F. Mahat, M. H. Yahya, and B. T. Matemilola, “Liquidity risk and bank financial performance: an application of system GMM approach,” *J. Financ. Regul. Compliance*, vol. 30, no. 3, pp. 312–334, 2022, doi: 10.1108/JFRC-03-2021-0019.
- [14] S. L. Mairafi, S. Hassan, and S. B. Mohamed-Arshad, “Systematic review of literature on effect of liquidity on bank,” *Acad. Account. Financ. Stud. J.*, vol. 22, no. 4, pp. 1–7, 2018.
- [15] S. Mohammad, M. Asutay, R. Dixon, and E. Platonova, “Liquidity risk exposure and its determinants in the banking sector: A comparative analysis between Islamic, conventional and hybrid banks,” *J. Int. Financ. Mark. Institutions Money*, vol. 66, no. May 2020, 2020, doi: 10.1016/j.intfin.2020.101196.
- [16] S. A. Oluwadare, A. F.-B. Thompson, O. Owolafe, and A. O. Orogun, “Comparative Review of Credit Card Fraud Detection using Machine Learning and Concept Drift Techniques,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 12, no. 7, pp. 24–48, 2023, doi: 10.47760/ijcsmc.2023.v12i07.004.
- [17] J. S. Alaba, S. J. Ahmed, A. P. Farida, and O. V. Oluwatosin, “Adoption of AI-Driven Fraud Detection System in the Nigerian Banking Sector: An Analysis of Cost, Compliance, and Competency,” *Financ. Econ. Lett.*, vol. 4, no. 2, pp. 40–53, 2025, doi: 10.58567/fel04020004.
- [18] M. Afjal, A. Salamzadeh, and L. P. Dana, “Financial Fraud and Credit Risk: Illicit Practices and Their Impact on Banking Stability,” *J. Risk Financ. Manag.*, vol. 16, no. 9, 2023, doi: 10.3390/jrfm16090386.
- [19] G. Alagöz and E. Çanakoglu, “Credit Risk Analysis using Machine-Learning Algorithms,” in *2021 29th Signal Processing and Communications Applications Conference (SIU)*, Istanbul: IEEE, 2021. [Online]. Available: <https://ieeexplore.ieee.org/document/9477873>
- [20] O. K. Natufe and E. I. Evbayiro-Osagie, “Credit Risk Management and the Financial Performance of Deposit Money Banks: Some New Evidence,” *J. Risk Financ. Manag.*, vol. 16, no. 7, 2023, doi: 10.3390/jrfm16070302.
- [21] P. K. Kahihu, D. M. Wachira, and S. M. Muathe, “Managing Market Risk for Financial Performance: Experience from Microfinance Institution in Kenya,” *J. Financ. Regul. Compliance*, vol. 29, no. 5, pp. 561–579, 2021, doi: 10.1108/JFRC-02-2021-0014.
- [22] W. Donghua, “A comparative analysis of operational risk of Chinese listed commercial bank based on the income model,” in *2011 International Conference on E-Business and E-Government (ICEE)*, SHanghai, China, Shanghai, 2011, pp. 1–3. doi: 10.1109/ICEBEG.2011.5887014.
- [23] P. Malik, A. Chourasia, R. Pandit, S. Bawane, and J. Surana, “Credit Risk Assessment and Fraud Detection in Financial Transactions Using Machine Learning,” *J. Electr. Syst.*, vol. 10, no. 5, pp. 2061–2069, 2024, doi: 10.61137/ijrsret.vol.10.issue5.240.
- [24] B. Qi, M. Marie, A. S. Abdelwahed, I. N. Khatatbeh, M. Omran, and A. A. S. Fayad, “Bank Risk Literature (1978–2022): A Bibliometric Analysis and Research Front Mapping,” *Sustain.*, vol. 15, no. 5, p. 4508, 2023, doi: 10.3390/su15054508.
- [25] I. I. Akuji, B. O. Ahmed, T. A. Ahmed, I. B. Adeyemi, and A. J. Alabi, “Loan Default Prediction System Using Forward and Backward Propagation Techniques: A Comparative Study,” *Int. J. Appl. Inf. Syst.*, vol. 13, no. 3, pp. 22–32, 2026, doi: 10.5120/ijais8bfa29462311.
- [26] P. Gupta, “Leveraging Machine Learning and Artificial Intelligence for Fraud Prevention,” *Int. J. Comput. Sci. Eng.*, vol. 10, no. 5, pp. 47–52, 2023, doi: 10.14445/23488387/ijcse-v10i5p107.
- [27] J. N. Taiwo, M. E. Agwu, A. A. Babajide, T. C. Okafor, and A. A. Isibor, “Growth of Bank Frauds and the impact on the Nigerian Banking Industry,” *J. Bus. Manag. Econ.*, vol. 4, no. 12, pp. 1–10, 2016.
- [28] D. Mangala and L. Soni, “A systematic literature review on frauds in banking sector,” *J. Financ. Crime*, vol. 30, no. 1, pp. 285–301, 2023, doi: 10.1108/JFC-12-2021-0263.
- [29] E. M. Alotaibi, “Risk Assessment Using Predictive Analytics,” *Int. J. Prof. Bus. Rev.*, vol. 8, no. 5, p. e01723, 2023, doi: 10.26668/businessreview/2023.v8i5.1723.
- [30] H. Idris, “Exploring Financial Risk Management: A Qualitative Study on Risk Identification, Evaluation, and Mitigation in Banking, Insurance, and Corporate Finance,” *Golden Ratio Financ. Manag.*, vol. 4, no. 2, pp. 213–225, 2024, doi: 10.52970/grfm.v4i2.651.
- [31] A. Mashrur, W. Luo, N. A. Zaidi, and A. Robles-Kelly, “Machine learning for financial risk management: A survey,” *IEEE Access*, vol. 8, pp. 203203–203223, 2020, doi: 10.1109/ACCESS.2020.3036322.
- [32] I. D. Mienye, E. Esenogho, and C. Modisane, “Deep Learning for Credit Risk Prediction : A Survey of Methods , Applications , and Challenges,” *Information*, vol. 17, no. 4, p. 395, 2026, doi: 10.3390/info17040395.
- [33] N. Chen, B. Ribeiro, and A. Chen, “Financial credit risk assessment: a recent review,” *Artif. Intell. Rev.*, vol. 45, no. 1, pp. 1–23, 2016, doi: 10.1007/s10462-015-9434-x.
- [34] H. A. Abdou and J. Pointon, “Credit Scoring , Statistical Techniques and Evaluation Criteria : A Review of the Literature,” *Intell. Syst. Accounting, Financ. Manag.*, vol. 18, no. 2–3, pp. 59–88, 2011, [Online]. Available: <https://doi.org/10.1002/isaf.325>
- [35] A. O. Akinwumi, A. O. Akingbesote, O. O. Ajayi, and F. O. Aranuwa, “Detection of Distributed Denial of Service (DDoS) attacks using convolutional neural networks,” *Niger. J. Technol.*, vol. 41, no. 6, pp. 1017–1024, 2022, doi: 10.4314/njt.v41i6.12.
- [36] O. A. Ayegbusi *et al.*, “A Deep Learning-based Model for Traffic Signal Control using the YOLO Algorithm,” *Int. J. Comput. Appl.*, vol. 186, no. 63, pp. 43–54, 2025.
- [37] D. Krasovytskyi and A. Stavitsky, “Predicting Mortgage Loan Defaults Using Machine Learning Techniques,” *Ekonomika*, vol. 103, no. 2, pp. 140–160, 2024, [Online]. Available:



<https://www.journals.vu.lt/ekonomika/article/view/34809>

- [38] Y. Yang *et al.*, “Transforming Credit Risk Analysis: A Time-Series-Driven ResE-BiLSTM Framework for Post-Loan Default Detection,” *Information*, vol. 17, no. 5, 2026, [Online]. Available: <https://doi.org/10.3390/info17010005>
- [39] J. Jin and Y. Ma, “Digital Financial Risk Assessment Method based on Machine Learning Algorithm,” *Procedia Comput. Sci.*, vol. 262, pp. 1094–1100, 2025, doi: 10.1016/j.procs.2025.05.146.
- [40] K. Peng and G. Yan, “A survey on Deep Learning for Financial Risk Prediction,” *Quant. Financ. Econ.*, vol. 5, no. 4, pp. 716–737, 2021, doi: 10.3934/qfe.2021032.
- [41] I. Bahammou, S. Ziti, and K. El Bouchti, “Machine Learning for Financial Market Prediction: A Systematic Literature Review,” *Stat. Optim. Inf. Comput.*, vol. 16, no. August, pp. 1697–1715, 2026, doi: 10.19139/soic-2310-5070-3490.
- [42] V. O. Olaleye, O. A. Odeniyi, and B. K. Alese, “Ensemble-based Predictive Model for Financial Fraud Detection,” *Int. J. Appl. Inf. Syst.*, vol. 12, no. 42, pp. 54–62, 2024, [Online]. Available: <https://www.ijais.org/archives/volume12/number42/olaleye-2024-ijais-451961.pdf>
- [43] N. T. Duong, D. Thi, T. Ha, and N. B. Ngoc, “The Application of Discriminant Model in Managing Credit Risk for Consumer Loans in Vietnamese Commercial Bank,” *Asian Soc. Sci.*, vol. 13, no. 2, pp. 176–186, 2017, doi: 10.5539/ass.v13n2p176.
- [44] H. Wang, Q. Xu, and L. Zhou, “Large Unbalanced Credit Scoring Using Lasso-Logistic Regression Ensemble,” *PLoS One*, vol. 10, no. 2, pp. 1–20, 2015, doi: 10.1371/journal.pone.0117844.
- [45] A. Negi and D. Kumar, “Fraud Detection in Financial Transactions Using Machine Learning Techniques,” in *International Conference on Networks and Cryptology*, 2025, pp. 745–750. doi: 10.1109/NETCRYPT65877.2025.11102785.
- [46] H. M. Hadi and O. S. Kareem, “Fraud Detection in Transaction Based on Artificial Intelligence,” 2025. [Online]. Available: <https://www.sciencepubco.com/index.php/IJSW/article/view/33929/18388>
- [47] R. Bin Sulaiman, V. Schetinin, and P. Sant, “Review of Machine Learning Approach on Credit Card Fraud Detection,” *Human-Centric Intell. Syst.*, vol. 2, pp. 55–68, 2022, doi: 10.1007/s44230-022-00004-0.
- [48] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, “Credit Card Fraud Detection - Machine Learning methods,” in *2019 18th International Symposium INFOTEH-JAHORINA*, IEEE, 2019, pp. 1–5. doi: 10.1109/INFOTEH.2019.8717766.
- [49] J. Cherus, J. Githeko, J. Siror, and K. Njagi, “Identity Fraud: A Literature Review and Future Research Directions,” *Africa Dev. Resour. Res. Institute J.*, vol. 5, no. 2, pp. 36–53, 2014, [Online]. Available: <https://journals.adrri.org/index.php/adrri/article/view/47>
- [50] A. Kumar, K. Sethi, and A. Verma, “A Comprehensive Review of Machine Learning Techniques in Fraud Detection,” in *Proceedings of the 2025 12th International Conference on Computing for Sustainable Global Development, INDIACom 2025*, 2025, pp. 1875–1881. doi: 10.23919/INDIACom66777.2025.11115819.
- [51] A. Batan, “A Brief Introduction to Know Your Customer (KYC),” 2021.
- [52] P. Meesala and U. D. Prasan, “A Novel Behavioral Based Fraud Detection System Using Machine Learning,” *Cuest. Fisioter.*, vol. 54, no. 4, pp. 1591–1599, 2025.
- [53] A. A. Compagnino *et al.*, “An Introduction to Machine Learning Methods for Fraud Detection,” *Appl. Sci.*, vol. 15, no. 21, pp. 1–32, 2025, doi: 10.3390/app152111787.
- [54] C. Damian Ikemefuna, O. Okusi, A. Chibuzor, and S. Yusuf, “Adaptive Fraud Detection Systems: Using ML To Identify and Respond To Evolving Financial Threats,” *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 6, no. 09, pp. 2077–2092, 2024, [Online]. Available: <https://www.doi.org/10.56726/IRJMETS61738>
- [55] T. A. Khan, J. Tulsi, M. Alam, K. Kadir, K. M. Ali, and M. S. Mazliham, “Analysis and visualization of fraud detection patterns through data mining and classification using MLP and hybrid deep learning model,” *Egypt. Informatics J.*, vol. 32, no. May, p. 100829, 2025, doi: 10.1016/j.eij.2025.100829.
- [56] M. N. Hossain, “Statistical Analysis of Cyber Risk Exposure and Fraud Detection in Cloud-Based Banking Ecosystems,” *Glob. Perspect. Sci. Scholarsh.*, vol. 02, no. 01, pp. 289–331, 2022, doi: 10.63125/9wtf91068.
- [57] O. C. Metibemu, “Financial Risk Management in Digital-Only Banks: Addressing Fraud and Cybersecurity Threats in a Cashless Economy,” *Asian J. Res. Comput. Sci.*, vol. 18, no. 3, pp. 434–455, 2025, doi: 10.9734/ajrcos/2025/v18i3603.
- [58] K. Patel, “Credit Card Analytics: A Review of Fraud Detection and Risk Assessment Techniques,” *Int. J. Comput. Trends Technol.*, vol. 71, no. 10, pp. 69–79, 2023, doi: 10.14445/22312803/ijctt-v71i10p109.
- [59] O. B. Oyelakun, A. A. Abdul-azeez, A. A. Ibrahim, E. A. Julius, and O. O. Olayemi, “Credit Bureau: An Aid to Credit Risk Management,” *J. Int. Money, Bank. Financ.*, vol. 6, no. 1, pp. 1–16, 2025, [Online]. Available: [https://www.artjournals.com/image/catalog/Journals/Papers/JIMBF/2025/No 1 \(2025\)/1_Oyetola Bukunmi.pdf](https://www.artjournals.com/image/catalog/Journals/Papers/JIMBF/2025/No 1 (2025)/1_Oyetola Bukunmi.pdf)
- [60] B. A. Kusi, A. Gyeke-Dako, K. Ansah-Adu, and E. K. Agbloyor, “Bank credit risk and credit information sharing in Africa: Does credit information sharing institutions and context matter?,” *Res. Int. Bus. Financ.*, vol. 42, pp. 1123–1136, 2017, doi: 10.1016/j.ribaf.2017.07.047.
- [61] S. Fosu, A. Danso, H. Agyei-Boapeah, C. G. Ntim, and E. Adegbite, *Credit information sharing and loan default in developing countries: the moderating effect of banking market concentration and national governance quality*, vol. 55, no. 1. Springer US, 2019. doi: 10.1007/s11156-019-00836-1.
- [62] O. B. Oyelakun, O. O. Olayemi, and A. A. Ibrahim, “Credit Scoring: A Tool for Credit Risk Reduction,” *J. Int. Money, Bank. Financ.*, vol. 5, no. 2, pp. 127–138,



2024.

- [63] C. M. Omenihu, S. Brahma, E. Katsikas, D. Vrontis, E. Siachou, and I. Krasonikolakis, "Financial Inclusion and Poverty Alleviation: A Critical Analysis in Nigeria," *Sustainability*, vol. 16, no. 19, pp. 1–21, 2024, doi: 10.3390/su16198528.
- [64] G. Nwachukwu, "Enhancing Credit Risk Management Through Revalidation and Accuracy in Financial Data: The Impact of Credit History Assessment on Procedural Financing," *Int. J. Res. Publ. Rev.*, vol. 5, no. November, pp. 631–644, 2024.
- [65] A. Olowe, "Investigating the accuracy of credit bureau data in predicting borrowers' repayment of consumer loans in Nigeria," *Data Sci. Financ. Econ.*, vol. 6, no. 1, pp. 31–57, 2026, doi: 10.3934/dsfe.2026002.
- [66] W. Gaviyau and A. B. Sibindi, "Customer Due Diligence in the FinTech Era: A Bibliometric Analysis," *Risks*, vol. 11, no. 1, 2023, doi: 10.3390/risks11010011.
- [67] R. Rusman and A. Budianto, "Strengthening Know Your Customer (KYC) and Anti-Money Laundering (AML) Policies in the Fintech Industry to Prevent Money Laundering Crimes," *J. World Sci.*, vol. 4, no. 7, pp. 871–881, 2025, doi: 10.58344/jws.v4i7.1446.
- [68] R. Arasa and L. Ottichilo, "Determinants of Know Your Customer (KYC) Compliance among Commercial Banks in Kenya," *J. Econ. Behav. Stud.*, vol. 7, no. 2, pp. 162–175, 2015.
- [69] H. Chitimira and S. Munedzi, "An evaluation of customer due diligence and related anti-money laundering measures in the United Kingdom," *J. Money Laund. Control*, vol. 26, no. 7, pp. 127–137, 2023, doi: 10.1108/JMLC-01-2023-0004.
- [70] S. Aidoo Citibank Europe PLC, "Customer Due Diligence (CDD) and Know Your Customer (KYC)," 2025. [Online]. Available: <https://www.researchgate.net/publication/393884914>
- [71] B. Oztas, D. Cetinkaya, F. Adedoyin, M. Budka, G. Aksu, and H. Dogan, "Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry," *Futur. Gener. Comput. Syst.*, vol. 159, no. January, pp. 161–171, 2024, doi: 10.1016/j.future.2024.05.027.
- [72] O. K. Agboola, "AI-Driven Fraud Detection and Biometric KYC: Enhancing Ethical Compliance in U.S. Digital Banking," *Int. J. Comput. Appl. Technol. Res.*, vol. 14, no. 08, pp. 112–121, 2025, doi: 10.7753/ijcatr1408.1010.
- [73] A. A. Omoseebi, G. Ola, and J. Tyler, "Rule-Based Systems in AML [Unpublished Manuscript]," 2023. [Online]. Available: https://www.researchgate.net/publication/389869404_Rule-Based_Systems_in_AML
- [74] N. S. Nnam, O. R. Okonkwo, I. Johnson, and G. Akawuku, "Money Laundering Detection System with Intelligent Agents," *Res. Invent. J. Eng. Phys. Sci.*, vol. 4, no. 1, pp. 112–120, 2025, doi: 10.59298/RIJEP/2025/41112120.
- [75] O. D. Iguodala and A. Oyiborhoro, "AI-Powered Anti-Money Laundering (AML) and fraud detection - enhancing financial security through intelligent fraud detection," *World J. Adv. Res. Rev.*, vol. 26, no. 02, pp. 3702–3714, 2025, doi: 10.30574/wjarr.2025.26.2.0637.
- [76] Z. Khemais, D. Nesrine, and M. Mohamed, "Credit Scoring and Default Risk Prediction: A Comparative Study between Discriminant Analysis & Logistic Regression," *Int. J. Econ. Financ.*, vol. 8, no. 4, pp. 39–53, 2016, doi: 10.5539/ijef.v8n4p39.
- [77] Z. Runchi, X. Ligu, and W. Qin, "An ensemble credit scoring model based on logistic regression with heterogeneous balancing and weighting effects," *Expert Syst. Appl.*, vol. 212, 2023, doi: 10.1016/j.eswa.2022.118732.
- [78] N. Ghatasheh, "Business Analytics using Random Forest Trees for Credit Risk Prediction: A Comparison Study," *Int. J. Adv. Sci. Technol.*, vol. 72, pp. 19–30, 2014, doi: 10.14257/ijast.2014.72.02.
- [79] A. Alagic et al., "Machine Learning for an Enhanced Credit Risk Analysis: A Comparative Study of Loan Approval Prediction Models Integrating Mental Health Data," *Mach. Learn. Knowl. Extr.*, vol. 6, no. 1, pp. 53–77, 2024, doi: 10.3390/make6010004.
- [80] C. L. Perera and S. C. Premaratne, "An Ensemble Machine Learning Approach for Forecasting Credit risk of Loan Applications," *WSEAS Trans. Syst.*, vol. 23, pp. 31–46, 2024, doi: 10.37394/23202.2024.23.4.
- [81] Y. Wang, Y. Zhang, M. Liang, R. Yuan, J. Feng, and J. Wu, "National Student Loans Default Risk Prediction: A Heterogeneous Ensemble Learning Approach and the SHAP method," *Comput. Educ. Artif. Intell.*, vol. 5, no. May, p. 100166, 2023, doi: 10.1016/j.caeai.2023.100166.
- [82] L. I. Souadda, A. R. Halitim, B. Benilles, J. M. Oliveira, and P. Ramos, "Optimizing Credit Risk Prediction for Peer-to-Peer Lending Using Machine Learning," *Forecasting*, vol. 7, no. 3, pp. 1–31, 2025, doi: 10.3390/forecast7030035.
- [83] A. Akinjole, O. Shobayo, J. Popoola, O. Okoyeigbo, and B. Ogunleye, "Ensemble-Based Machine Learning Algorithm for Loan Default Risk Prediction," *Mathematics*, vol. 12, no. 21, 2024, doi: 10.3390/math12213423.
- [84] A. A. Egwa, "Default Prediction for Loan Lenders Using Machine Learning Algorithms," *SLUJ. Sci. Technol.*, vol. 5, no. 1&2, pp. 1–12, 2022, doi: 10.56471/slujst.v5i.222.
- [85] M. Zhou, "Credit Risk Assessment Modeling Method Based on Fuzzy Integral and SVM," *Mob. Inf. Syst.*, vol. 2022, 2022, doi: 10.1155/2022/3950210.
- [86] A. Irshad, K. Hussain, S. A. Hashmi, A. Akram, and J. Munir, "Comparative Analysis of Various Credit Card Fraud Techniques," *Spectr. Eng. Sci.*, vol. 4, no. 5, pp. 2397–2404, 2026, [Online]. Available: <https://thesesjournal.com/index.php/1/article/view/2975/2209>
- [87] M. G. Wijaya, M. F. Pinaringgi, A. Y. Zakiyyah, and Meiliana, "Comparative Analysis of Machine Learning Algorithms and Data Balancing Techniques for Credit Card Fraud Detection," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 677–688. doi:



10.1016/j.procs.2024.10.294.

- [88] Y. Peng and B. Wen, “Building Financial Enterprise Risk Assessment System Based on Big Data and Integrated Learning Technology,” *Procedia Comput. Sci.*, vol. 247, pp. 900–907, 2024, doi: 10.1016/j.procs.2024.10.109.
- [89] I. Aruleba and Y. Sun, “Effective Credit Risk Prediction Using Ensemble Classifiers With Model Explanation,” *IEEE Access*, vol. 12, no. June, pp. 115015–115025, 2024, doi: 10.1109/ACCESS.2024.3445308.
- [90] Y. Lei, H. Qiaoming, and Z. Tong, “Research on Supply Chain Financial Risk Prevention Based on Machine Learning,” *Comput. Intell. Neurosci.*, vol. 2023, 2023, doi: 10.1155/2023/6531154.
- [91] Y. Dendramis, E. Tzavalis, and A. Cheimarioti, “Measuring the Default Risk of Small Business Loans: Improved Credit Risk Prediction Using Deep Learning,” *J. Forecast.*, vol. 44, no. 7, pp. 2277–2297, 2025, doi: 10.1002/for.70005.
- [92] V. Pacelli and M. Azzollini, “An Artificial Neural Network Approach for Credit Risk Management,” *J. Intell. Learn. Syst. Appl.*, vol. 03, no. 02, pp. 103–112, 2011, doi: 10.4236/jilsa.2011.32012.
- [93] Y. Hu and J. Su, “Research on Credit Risk Evaluation of Commercial Banks Based on Artificial Neural Network Model,” *Procedia Comput. Sci.*, vol. 199, pp. 1168–1176, 2021, doi: 10.1016/j.procs.2022.01.148.
- [94] D. Kumar Gupta and S. Goyal, “Credit Risk Prediction Using Artificial Neural Network Algorithm,” *Int. J. Mod. Educ. Comput. Sci.*, vol. 10, no. 5, pp. 9–16, 2018, doi: 10.5815/ijmecs.2018.05.02.
- [95] S. Shi, R. Tse, W. Luo, S. D’Addona, and G. Pau, “Machine Learning-driven Credit Risk: A Systemic Review,” *Neural Comput. Appl.*, vol. 34, no. 17, pp. 14327–14339, 2022, doi: 10.1007/s00521-022-07472-2.
- [96] N. Bussmann, P. Giudici, D. Marinelli, and J. Papenbrock, “Explainable AI in Fintech Risk Management,” *Front. Artif. Intell.*, vol. 3, no. April, pp. 1–5, 2020, doi: 10.3389/frai.2020.00026.
- [97] D. Chen, J. Ye, and W. Ye, “Interpretable Selective Learning in Credit Risk,” *Res. Int. Bus. Financ.*, vol. 65, no. April, 2023, doi: 10.1016/j.ribaf.2023.101940.
- [98] Y. Sheng, “Temporal Dependency Modeling in Loan Default Prediction with Hybrid LSTM-GRU Architecture,” *Trans. Comput. Sci. Methods*, vol. 4, no. 8, 2024, [Online]. Available: <https://pspress.org/index.php/tcsm/article/view/213>
- [99] Z. Xie and X. Huang, “Loan Default Prediction Method Based on Sample Optimisation and Bagging Integration With CatBoost-GRU,” *IET Softw.*, vol. 2026, no. 1, pp. 1–13, 2026, doi: 10.1049/sfw2/9309999.
- [100] S. Xie, L. Liu, G. Sun, B. Pan, L. Lang, and P. Guo, “Enhanced E-commerce Fraud Prediction Based on a Convolutional Neural Network Model,” *Comput. Mater. Contin.*, vol. 75, no. 1, pp. 1107–1117, 2023, doi: 10.32604/cmc.2023.034917.
- [101] D. Cheng, X. Wang, Y. Zhang, and L. Zhang, “Graph Neural Network for Fraud Detection via Spatial-Temporal Attention,” *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 8, pp. 3800–3813, 2022, doi: 10.1109/TKDE.2020.3025588.
- [102] H. Fnu *et al.*, “Blockchain-Assisted Transformer CNN Framework with Optimal Feature Selection for Real-Time Digital Payment Fraud Detection,” *Int. J. Comput. Intell. Syst.*, vol. 19, no. 1, 2026, doi: 10.1007/s44196-025-01126-6.
- [103] M. Suganthi, G. Revathy, S. Gokulraj, and A. Y. Felix, “DEFENSE-BANK: Sea Horse Optimized Deep Learning Framework for Fraud Detection in the Banking Sector,” *Int. J. Comput. Intell. Syst.*, vol. 19, no. 1, 2026, doi: 10.1007/s44196-026-01277-0.
- [104] R. A. Darmawan, A. Musyafa, and M. Handayani, “Optimization of RNN and Tree-Based Models with Imbalance Handling for Fraud Detection in Digital Banking Transactions,” *J. Ilm. Multidisiplin Indones.*, vol. 5, no. 02, pp. 347–366, 2026, [Online]. Available: <https://ejournal.seaninstitute.or.id/index.php/esaprom/article/view/8057>
- [105] A. Gaurav, B. B. Gupta, S. Bansal, and K. E. Psannis, “Bankruptcy forecasting in enterprises and its security using hybrid deep learning models,” *Cyber Secur. Appl.*, vol. 3, no. March 2024, p. 100070, 2025, doi: 10.1016/j.csa.2024.100070.
- [106] Y. Luo, “ExHybridNet: An Explainable Hybrid Machine Learning Model for Corporate Financial Risk Prediction,” in *Proceedings of 2025 International Conference on Generative Artificial Intelligence for Business*, Association for Computing Machinery, 2025, pp. 172–178. doi: 10.1145/3766918.3766947.
- [107] M. A. Chohan, T. Li, M. Abrar, and S. Butt, “Deep Hybrid CNN-LSTM-GRU Model for a Financial Risk Early Warning System,” *Risks*, vol. 14, no. 1, pp. 1–20, 2026, doi: 10.3390/risks14010014.
- [108] M. Z. Abedin, C. Guotai, P. Hajek, and T. Zhang, “Combining weighted SMOTE with ensemble learning for the class-imbalanced prediction of small business credit risk,” *Complex Intell. Syst.*, vol. 9, no. 4, pp. 3559–3579, 2023, doi: 10.1007/s40747-021-00614-4.
- [109] I. Mapfumo and T. Shongwe, “Performance Evaluation of Machine Learning and Deep Learning Models for Credit Risk Prediction,” *J. Risk Financ. Manag.*, vol. 19, p. 210, 2026, doi: 10.3390/jrfm19030210.
- [110] N. T. H. Thuy, N. T. V. Ha, N. N. Trung, V. T. T. Binh, N. T. Hang, and V. T. Binh, “Comparing the Effectiveness of Machine Learning and Deep Learning Models in Student Credit Scoring: A Case Study in Vietnam,” *Risks*, vol. 13, no. 5, pp. 1–26, 2025, doi: 10.3390/risks13050099.
- [111] P. Ramachandra and S. Vaithyanathan, “Fed-DPSDG-WGAN: Differentially Private Synthetic Data Generation for Loan Default Prediction via Federated Wasserstein GAN,” *IEEE Access*, vol. 13, pp. 52069–52084, 2025, doi: 10.1109/ACCESS.2025.3552487.
- [112] R. Ming, O. Abdelrahman, N. Innab, and M. H. K. Ibrahim, “Enhancing fraud detection in auto insurance and credit card transactions: a novel approach integrating CNNs and machine learning algorithms,” *PeerJ Comput. Sci.*, vol. 10, pp. 1–35, 2024, doi: 10.7717/peerj-cs.2088.



- [113] C. T. Chen, C. Lee, S. H. Huang, and W. C. Peng, "Credit Card Fraud Detection via Intelligent Sampling and Self-supervised Learning," *ACM Trans. Intell. Syst. Technol.*, vol. 15, no. 2, pp. 1–29, 2024, doi: 10.1145/3641283.
- [114] T. Albalawi and S. Dardouri, "Enhancing credit card fraud detection using traditional and deep learning models with class imbalance mitigation," *Front. Artif. Intell.*, vol. 8, no. October, pp. 1–10, 2025, doi: 10.3389/frai.2025.1643292.
- [115] J. Ge, L. Yin, S. Zhang, and X. Zhao, "Gated attention based generative adversarial networks for imbalanced credit card fraud detection," *PeerJ Comput. Sci.*, vol. 11, p. 2972, 2025, doi: 10.7717/peerj-cs.2972.
- [116] F. L. Becerra-Suarez, H. Alvarez-Vasquez, and M. G. Forero, "Improvement of Bank Fraud Detection Through Synthetic Data Generation with Gaussian Noise," *Technologies*, vol. 13, no. 4, 2025, doi: 10.3390/technologies13040141.
- [117] J. Jurgovsky *et al.*, "Sequence classification for credit-card fraud detection," *Expert Syst. Appl.*, vol. 100, pp. 234–245, 2018, doi: 10.1016/j.eswa.2018.01.037.
- [118] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model," *J. Big Data*, vol. 8, p. 151, 2021, doi: 10.1186/s40537-021-00541-8.
- [119] E. K. Y. Yapp and H. Y. Yeh, "An extensive experimental comparison of machine and deep learning methods for credit and bank fraud detection," *Financ. Res. Lett.*, vol. 88, p. 1643292, 2026, doi: 10.1016/j.frl.2025.109190.
- [120] W. J. Yeo, W. Van Der Heever, R. Mao, E. Cambria, R. Satapathy, and G. Mengaldo, "A comprehensive review on financial explainable AI," *Artif. Intell. Rev.*, vol. 58, no. 6, pp. 1–49, 2025, doi: 10.1007/s10462-024-11077-7.
- [121] J. Černevičienė and A. Kabašinskas, *Explainable artificial intelligence (XAI) in finance: a systematic literature review*, vol. 57, no. 8. Springer Netherlands, 2024. doi: 10.1007/s10462-024-10854-8.
- [122] F. M. Talaat, A. Aljadani, M. Badawy, and M. Elhosseini, "Toward Interpretable Credit Scoring: Integrating Explainable Artificial Intelligence with Deep Learning for Credit Card Default Prediction," *Neural Comput. Appl.*, vol. 36, no. 9, pp. 4847–4865, 2024, doi: 10.1007/s00521-023-09232-2.
- [123] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Secure and Transparent Banking: Explainable AI-Driven Federated Learning Model for Financial Fraud Detection," *J. Risk Financ. Manag.*, vol. 18, no. 4, p. 179, 2025, doi: 10.3390/jrfm18040179.
- [124] R. Qi, *Enterprise Financial Distress Prediction Based on Machine Learning and SHAP Interpretability Analysis*, vol. 1, no. 1. Association for Computing Machinery, 2025. doi: 10.1145/3764727.3764740.
- [125] C. Ni, K. Qian, J. Wu, and H. Wang, "Contrastive Time-Series Visualization Techniques for Enhancing AI Model Interpretability in Financial Risk Assessment," 2025. doi: 10.20944/preprints202504.1984.v2.
- [126] K. C. Yao *et al.*, "Application of Generative AI in Financial Risk Prediction: Enhancing Model Accuracy and Interpretability," *Information*, vol. 16, no. 10, pp. 1–21, 2025, doi: 10.3390/info16100857.
- [127] S. R. Lenka, S. K. Bisoy, R. Priyadarshini, and M. Sain, "Empirical Analysis of Ensemble Learning for Imbalanced Credit Scoring Datasets: A Systematic Review," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/6584352.
- [128] Z. Zhao, T. Cui, S. Ding, J. Li, and A. G. Bellotti, "Resampling Techniques Study on Class Imbalance Problem in Credit Risk Prediction," *Mathematics*, vol. 12, p. 701, 2024, doi: 10.3390/math12050701.
- [129] Y. Long, S. Kroeger, M. F. Zaeh, and A. Brintrup, "Leveraging synthetic data to tackle machine learning challenges in supply chains: challenges, methods, applications, and research opportunities," *Int. J. Prod. Res.*, vol. 7543, 2025, doi: 10.1080/00207543.2024.2447927.
- [130] T. Malankar, O. Pathare, Y. Shah, and B. Jadhav, "Enhancing Credit Card Fraud Detection through Adversarial Learning : A Generative Adversarial Network Approach," in *International Conference on "Large Language Models and Use cases"*, 2023, pp. 19–24. [Online]. Available: <https://www.ijcaonline.org/media/proceedings/LLMUC202412.pdf>
- [131] Y. Yang, C. Xu, and G. Tian, "Lightweight Financial Fraud Detection Using a Symmetrical GAN-CNN Fusion Architecture," *Symmetry (Basel)*, vol. 17, no. 8, pp. 1–20, 2025, doi: 10.3390/sym17081366.
- [132] S. Z. Aftabi, A. Ahmadi, and S. Farzi, "Fraud detection in financial statements using data mining and GAN models," *Expert Syst. Appl.*, vol. 227, no. October, 2023, doi: 10.1016/j.eswa.2023.120144.
- [133] L. Zhi and W. Wang, "Research on modeling of the imbalanced fraudulent transaction detection problem based on embedding-aware conditional GAN," *Big Data Res.*, vol. 41, no. August, 2025, doi: 10.1016/j.bdr.2025.100557.
- [134] M. U. Safder, S. S. Naveed, K. Khurshid, A. Salman, and I. F. Nizami, "Optimizing imbalanced learning with genetic algorithm," 2025. doi: 10.1038/s41598-025-09424-x.
- [135] J. Jordon *et al.*, "Synthetic Data -- what, why and how?," 2022, [Online]. Available: <http://arxiv.org/abs/2205.03257>
- [136] Financial Conduct Authority, "Report on using synthetic data in financial services," 2024. [Online]. Available: <https://www.fca.org.uk/publication/corporate/report-using-synthetic-data-in-financial-services.pdf>
- [137] Financial Conduct Authority, "Generating and Using Synthetic Data for Models in Financial Services: Governance Considerations The Synthetic Data Expert Group," 2025. [Online]. Available: <https://www.fca.org.uk/publication/corporate/synthetic-data-models-financial-services-governance.pdf>
- [138] D. Kawa, S. Punyani, P. Nayak, A. Karkera, and V.



- Jyotinagar, “Credit Risk Assessment from Combined Bank Records using Federated Learning,” *Int. Res. J. Eng. Technol.*, vol. 6, no. 4, pp. 1355–1358, 2019, [Online]. Available: <https://www.irjet.net/archives/V6/i4/IRJET-V6I4288.pdf>
- [139] N. Khan *et al.*, “Federated Learning: Concepts, Challenges and Implementation,” *Expert Syst.*, vol. 42, no. 8, 2025, doi: 10.1111/exsy.70096.
- [140] J. Zhao *et al.*, “The Federation Strikes Back: A Survey of Federated Learning Privacy Attacks, Defenses, Applications, and Policy Landscape,” *ACM Comput. Surv.*, vol. 57, no. 9, p. Article 230, 2025, doi: 10.1145/3724113.
- [141] V. R. R. Gottimukkala, “Privacy-Preserving Machine Learning Models for Transaction Monitoring in Global Banking Networks,” *Int. J. Financ.*, vol. 36, no. 6, pp. 633–652, 2023, doi: 10.5281/zenodo.17454046.
- [142] M. Rajasekar, “Risk - Aware Generative AI and Machine Learning Frameworks for Privacy - Preserving Banking and Trade Analytics over Cloud and 5G Networks,” *Int. J. Comput. Technol. Electron. Commun.*, vol. 8, no. 4, pp. 11078–11086, 2025, doi: 10.15680/IJCTECE.2025.0804011.
- [143] M. P. Ahmed, S. A. Tisha, and M. M. R. Sweet, “Journal of Business and Management Studies Determinants of Employee Retention in Pharmaceutical Companies: Case of Saudi Arabia,” *Real-Time Hybrid Optim. Model. Edge-Based Financ. Risk Assess. Integr. Deep Learn. with Adapt. Regres. Low-Latency Decis. Mak.*, no. 2709–0876, pp. 38–52, 2025, doi: 10.32996/jbms.
- [144] C. O. Kungu, K. Senagi, and E. Omondi, “Hybrid deep learning for anti-money laundering: Unsupervised detection of emerging schemes via feature fusion and explainable artificial intelligence,” *Mach. Learn. with Appl.*, vol. 23, no. October 2025, p. 100856, 2026, doi: 10.1016/j.mlwa.2026.100856.
- [145] J. R. Oliveira and A. G. Leal, “Enhancing Anti-Money Laundering Protocols: Employing Machine Learning to Minimise False Positives and Improve Operational Cost Efficiency,” in *8th International Conference on Advances in Artificial Intelligence*, Association for Computing Machinery, 2025, pp. 8–13. doi: 10.1145/3704137.3704156.
- [146] A. N. Bakry, A. S. Alsharkawy, M. S. Farag, and K. R. Raslan, “Automatic Suppression of False Positive Alerts in Anti-Money Laundering Systems Using Machine Learning,” *J. Supercomput.*, vol. 80, no. 5, pp. 6264–6284, 2024, doi: 10.1007/s11227-023-05708-z.
- [147] A. Karami and C. Igbokwe, “The impact of big data characteristics on credit risk assessment,” *Int. J. Data Sci. Anal.*, vol. 20, no. 5, pp. 4239–4259, 2025, doi: 10.1007/s41060-025-00753-8.
- [148] M. H. Bari, S. Juthi, A. M. Mistry, and M. Kamrujjaman, “A Systematic Literature Review of Predictive Models and Analytics in AI-Driven Credit Scoring,” *Non Hum. J.*, vol. 1, no. 01, pp. 01–18, 2024, doi: 10.70008/jmldeds.v1i01.36.
- [149] M. R. M. Salem and S. Shahimi, “A comprehensive analysis of FinTech (1968–2025): a bibliometric approach,” *Futur. Bus. J.*, vol. 11, no. 1, pp. 1–20, 2025, doi: 10.1186/s43093-025-00652-1.
- [150] W. Gaviyau and J. Godi, “Emerging Risks in the Fintech-Driven Digital Banking Environment: A Bibliometric Review of China and India,” *Risks*, vol. 13, no. 10, 2025, doi: 10.3390/risks13100186.
- [151] S. R. T. da Silva, A. F. de Matos Coelho, and C. A. N. Proença, “Drivers of FinTech adoption: a bibliometric approach,” *Financ. Innov.*, vol. 12, no. 1, 2026, doi: 10.1186/s40854-025-00855-z.
- [152] J. Abdulkadir, H. Mohammed, and A. L. Balarabe, “Digital Lending Platforms , Fintech Partnerships , and Credit,” *J. Bus. Dev. Manag. Res.*, vol. 11, no. 7, pp. 165–180, 2026.
- [153] E. Akuoko-Konadu and A. Mahmud, “Corruption, Economic Growth, and Non-performing Loans in Sub-Saharan Africa: An Empirical Analysis (2011–2019),” *J. Quant. Econ.*, vol. 23, no. 1, pp. 233–251, 2025, doi: 10.1007/s40953-024-00420-y.
- [154] A. Yahaya, A. Balarabe Musa, and O. Jayeola, “Non-Performing Loans, Interest Effect and Bank Performance in Sub Saharan African Economies,” *Niger. J. Bus. Adm.*, vol. 19, no. 1, pp. 46–59, 2021.
- [155] K. K. Arthur, S. A. Asongu, P. Darko, M. O. Ansah, S. Adom, and O. Hlortu, “Financial crimes in Africa and Economic Growth: Implications for achieving Sustainable Development Goals (SDGs),” *J. Econ. Surv.*, vol. 39, no. 3, pp. 1212–1251, 2025, doi: 10.1111/joes.12652.
- [156] R. A. Folami, G. O. Yinusa, and A. K. Toriola, “Digital Payment Fraud and Bank Fragility: Evidence from Deposit Money Banks in Nigeria,” *African J. Econ. Rev.*, vol. 12, no. 4, pp. 21–37, 2024.
- [157] D. Oyetade and P.-F. Muzindutsi, “The impact of Economic policy Uncertainty on the Performance of African Banks,” *J. Accounting, Financ. Audit. Stud.*, vol. 10, no. 2, pp. 105–118, 2024, doi: 10.56578/jafas100205.