IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 March 2024, accepted 18 April 2024, date of publication 24 April 2024, date of current version 13 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3393154

RESEARCH ARTICLE

Financial Fraud Detection Using Value-at-Risk With Machine Learning in Skewed Data

ABDULLAHI UBALE USMAN[1,3], SUNUSI BALA ABDULLAHI[2], (Member, IEEE), YU LIPING[1], BAYAN ALGHOFAILY[4], AHMED S. ALMASOUD[4], AND AMJAD REHMAN[4], (Senior Member, IEEE)

[1]School of Statistics and Mathematics, Zhejiang Gongshang University, Hangzhou 310018, China
[2]Department of Electronics and Telecommunication Engineering, Faculty of Engineering, King Mongkut's University of Technology Thonburi, Bang Mod, Thrung Khru, Bangkok 10140, Thailand
[3]Department of Statistics, Kano University of Science and Technology, Wudil 713281, Nigeria
[4]College of Computer & Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia

Corresponding author: Yu Liping (yvliping@zjgsu.edu.cn)

ABSTRACT The significant losses that banks and other financial organizations suffered due to new bank account (NBA) fraud are alarming as the number of online banking service users increases. The inherent skewness and rarity of NBA fraud instances have been a major challenge to the machine learning (ML) models and happen when non-fraud instances outweigh the fraud instances, which leads the ML models to overlook and erroneously consider fraud as non-fraud instances. Such errors can erode the confidence and trust of customers. Existing studies consider fraud patterns instead of potential losses of NBA fraud risk features while addressing the skewness of fraud datasets. The detection of NBA fraud is proposed in this research within the context of value-at-risk as a risk measure that considers fraud instances as a worst-case scenario. Value-at-risk uses historical simulation to estimate potential losses of risk features and model them as a skewed tail distribution. The risk-return features obtained from value-at-risk were classified using ML on the bank account fraud (BAF) Dataset. The value-at-risk handles the fraud skewness using an adjustable threshold probability range to attach weight to the skewed NBA fraud instances. A novel detection rate (DT) metric that considers risk fraud features was used to measure the performance of the fraud detection model. An improved fraud detection model is achieved using a K-nearest neighbor with a true positive (TP) rate of 0.95 and a DT rate of 0.9406. Under an acceptable loss tolerance in the banking sector, value-at-risk presents an intelligent approach for establishing data-driven criteria for fraud risk management.

INDEX TERMS Detection rate, fraud detection, K-nearest neighbor, skewed instances, value-at-risk.

I. INTRODUCTION

The Association of Certified Fraud Examiners (ACFE) 2022 released a financial fraud report stating that 2,110 fraud cases involving industries in financial sectors in 133 countries resulted in losses of around $3.6 billion [1]. Financial fraud can be termed as the deliberate employment of unlawful procedures or tactics to obtain financial gain [2]. The consequences of financial fraud can potentially disrupt economies, raise living expenses, and undermine consumer confidence [3]. Forms of financial fraud include insurance fraud, money laundering, new bank account fraud, credit and debit card fraud, mortgage fraud, and many more [4.5]. The act of opening an account to commit fraud at banks or other financial organizations is known as ''new bank account (NBA) fraud'' [6]. Fraud not only results in immediate financial losses and erodes public confidence in institutions, but has broader consequences, affecting customers and financial systems through market instability and contributing to larger macroeconomic downturns [7]. Fraud datasets typically exhibit some properties including skewness, evolving patterns, highly dimensional, and restricted access to relevant information. Specifically, fraud skewness which represents the majority fraud class over the non-fraud class has been a major concern to studies, as it affects the performance of fraud detection model. The Skewed fraud instances can

The associate editor coordinating the review of this manuscript and approving it for publication was Chao Tong.

have a bad influence on machine learning algorithms such as distance-based algorithms [8]. Previous efforts in tackling fraud involve developing rule-based expert systems, statistical methods, machine learning, and risk-based methods [9], [10]. Due to the cost of maintenance and the inefficiency of rule-based methods [10], decision-makers decide to utilize statistical methods such as autoregressive models to handle financial fraud [11], [12], [13]. The complex patterns and high dimensional nature of frauds make the statistical methods less effective, as such machine learning models were deployed [10], [14]. However, some of the studies that utilize machine learning techniques were found to have a high False Positive (FP) rate [15], [16], [17]. Machine learning models can potentially handle high-dimensional data and complex patterns of fraud instances.

To evaluate the effectiveness of machine learning model, Jesus et al. [18] presented the first domain-specific and real-world bank account fraud (BAF) dataset. The datasets were generated using generative adversarial networks (GANs) and evaluated using light gradient boosting method (LGBM).The study [18], [19] utilizes 25 sets of hyperparameter configurations to optimize the LGBM model, utility aware reweighing was used to handle the class skewness of BAF dataset. The study [15] utilizes stacking in ensembled learning with majority voting to evaluate the BAF dataset and address the changing fraud patterns. The study [20] uses federated learning in addressing data privacy issues of BAF dataset and deep neural networks to classify fraud instances. These studies achieve good performance in addressing BAF challenges; However, the studies do not consider the potential losses of fraud risk features. To our knowledge, little research exists that employs machine learning techniques in NBA fraud detection. The detection of NBA fraud is proposed in this paper within the context of risk management that uses value-at-risk to considers skewed fraud instances as a worst-case scenario. To adequately estimate the losses of fraud risks, value-at-risk was augmented with expected loss and expected shortfall of frauds which further quantifies the mean and extreme loss effects respectively. These risk measures combination will allow the quantification of risks across mean, worst-case, and extreme scenarios. Value-at-risk employs historical simulation to estimate potential losses of risk features. The risk-return features obtained from value-at-risk are based on assessing their risk exposure to fraud risk. The risk-return features are sent as input to the NBA fraud detection model. Different machine learning models were trained; However, the K-nearest neighbor outperformed other models. The contributions of this paper are:

- This paper used an extreme value theorem to model the tails (potential losses) instead of the fraud pattern.
- This paper used value-at-risk to model the skewness of fraud instances more efficiently.
- This paper utilized historical simulation to estimate value-at-risk as it makes no assumptions on any distribution.
- This paper used novel detection rate performance metrics to capture the overall performance in detection of NBA fraud instances that incorporate risk fraud factors.

The remainder of the paper is arranged as follows: The study's review of the literature is presented in Section II. The problem definition is presented in Section III. The materials and procedures are presented in Section IV. The experimental setup is presented in Section V. The results are presented in Section VI. The study's conclusions and discussions are presented in Section VII.

II. LITERATURE REVIEW

This section presents related studies in financial fraud detection. Different studies exist that utilize both statistical and artificial intelligence-based methods in the context of a risk and financial fraud perspective.

A. STATISTICAL METHODS OF FRAUD DETECTION

Many studies in the literature utilize statistical methods in evaluating financial fraud. Specifically, significant studies were found to utilize ordinary least squares (OLS) regression and autoregressive (AR) models for financial fraud evaluation. Using the Tehran Stock Exchange dataset, the study [21] uses a regression model to investigate the association between auditor characteristics and fraud detection in emerging economies. The authors provide useful information for improving the reliability of the findings. Using pooled OLS and panel regressions, the study [22] investigates the effect of political alignment on corporate fraud convictions, offering insights into the connection between politics and fraud. The authors use state-level data from 2003 to 2018 on US corporate fraud convictions and party affiliation. The study [23] utilizes OLS to investigate financial factors of financial fraud, which is attributed to the fraud triangle. The study [24] uses logistic regression to discover that external pressures and financial stability had a favorable impact on financial reporting fraud. On the other hand, collaboration, arrogance, changes in directors, incompetent oversight, and hubris have little bearing on false financial reporting. The study [25] provides evidence for the contribution of gender diversity to fraud commission and detection in Chinese listed businesses between 2007 and 2018 using bivariate probit model. The authors opined that female corporate executives are linked to a stronger ability to detect fraud, which lowers the likelihood that businesses to commit fraud. From the standpoint of external auditors, the study [26] sheds light on the causes of fraud and the function of forensic accounting using regression analysis to analyze Lebanese data. The study [4] discovered that while the overall number of employees engaged in fraud affects the performance of money banks in Nigeria, the number of fraud cases and the total amount lost to fraud had a favorable influence. The use of statistical methods by the author such as OLS regression, Pearson correlation, and descriptive analysis strengthens the findings by the authors. The sales growth index and the depreciation index factors

make up the M-score are used in the study [27] to analyze the possibility of profit management using the Athens Stock Exchange Market. It is pertinent to know that a large body of literature exists that utilizes the AR model. To handle [12] large-scale non-uniform transactions more quickly, the authors employ the AR model, which makes it appropriate for detecting money laundering operations. The study [11] uses factor analysis to generate the composite indicator, fractional integration (ARFIMA), and fractional cointegration VAR (FCVAR) approaches to evaluate the behavior of the composite suspicion tax fraud indicator about GDP and tax collection. The study [13] employs the AR model, which is appropriate for studying networks with such topologies and applying it to the detection of financial transaction fraud since it considers the block-wise structure of networks. The authors discovered that, in line with reality, there is a risk relationship between fraudulent groups and ordinary loan applicants. The study [28] outlined specific identification indicators that help with the detection of financial fraud using digital distribution laws, and the authors demonstrate that the probability of financial fraud increases significantly as the deviation of financial data distribution from Benford's law increases.

In summary, a large body of literature uses statistical methods to analyze the causes and effects that influence financial fraud, but due to the complex nature and scalability of fraud, statistical methods are not enough to adequately examine financial fraud.

B. RISK-BASED METHODS OF FRAUD DETECTION

This section presents the financial fraud assessment from the perspective of risk mitigation. The existing studies utilize different risk measures such as value-at-risk (VaR), expected loss, and expected shortfall to assess the level of risk of fraud. The study [29] offers strategies for breaking down the risk of fraud, identifying potential fraudsters, and enabling more targeted anti-fraud measures by tying the motivation of the fraud triangle to human tendencies that lead to specific actions as well as the meta-model of fraud together. Regression analysis is utilized in the study [30] to look at how enterprises manage risk to determine how control environments, risk assessments, control activities, information and communication, and monitoring contributed to fraud prevention and detection efforts in Indonesian firms. The study [31] defined additional security attributes that might have an impact on the cloud system and carried out an anomaly detection based on risk assessment named parallel processing (PP) that covers cyber threats and exploitation likelihoods. The model checker is then employed to determine the risk exposure rates associated with the respective attacks. The study [32] proposes a framework in which doubly-truncated severity distributions are used to estimate the operational risk and offered a framework that includes database construction and risk modeling. By applying value-at-risk and expected shortfall to identify operational risk sources like external fraud risk and legal risk sections, the authors were able to produce better and consistent results. The study [33] uses the number of compromised records to determine the cost of a data breach; the findings indicate that the total number of affected records has a Fréchet distribution, random forest is used for estimating the number of such records. The study [34] uses the estimate of generalized extreme value parameters to evaluates competency, digital technology abilities, and personality qualities that may improve the ability of external auditors to identify fraud risk, the efficiency of fraud risk assessment was linked to digital technology abilities through the application of the partial least-squares structural equation model (PLS-SEM). The study [35] identified a positive correlation between fraud risk assessment and management and the efficient use of forensic accounting using chi-square, fisher test, and correlation, however, there is no relationship between fraud risk assessment and management in terms of techniques causing fraud. The study [9] examines fraud using ensemble learners for anomaly detection and also handles data skewness, a triage model that receives input from the ensemble model, and a risk model that estimates the financial losses. The authors successfully provide an effective fraud risk-based detection, from machine learning techniques to risk assessment, but do not to evaluate fraud detection by first considering the risk component before subjecting it to machine learning detection.

In summary, risk measures are good in the assessment and management of the features associated with fraud for effective fraud prevention and control. However, due to the nonlinearity, high dimension, and complex nature of fraud, these risk measures need to be augmented with other techniques such as machine learning techniques that enable proper and efficient fraud prevention and detection.

C. MACHINE LEARNING METHODS IN FRAUD DETECTION

This section presents studies that utilize machine learning techniques for the classification of fraud applications. The majority of the presented studies consider the detection while addressing the skewed nature of fraud instances. Sampling methods, hybrid methods, and other novel methods are majorly used to overcome the skewed nature of fraud datasets. The study [36] addresses class skewness in credit card fraud using quantum machine learning (QML) and support vector machines (SVM). The results show that classic machine learning techniques are still useful for non-time series data, whereas QML applications can be used for time-series-based and highly skewed data. Quantum neural network (QNN) achieves good performance in fraud detection by the study [37]. The study [38] trained different machine learning models, all of which were using default implementations and parameters, XGBoost performed more accurately than any other models. The effectiveness of telecom fraud is assessed in the study [39] using a dynamic graph neural network (DGNN), the authors effectively present a suggested method for resolving the issue of telecom fraud detection in extensive phone social networks. To assess credit card fraud while

considering the skewness of fraud instances, the study [40] makes use of logistics regression (LR), K-nearest neighbor (KNN), decision tree (DT), random forest (RF), and autoencoder (AE) as they can handle skewed data better than other models, the AE model performs better. KNN, linear discriminant analysis (LDA), and linear regression are used in the study [41] to investigate credit card fraud, by addressing the skewed nature of the credit card fraud data and using cross-validation techniques, KNN showed higher performance. Using ARIMA model for fraud detection based on daily transaction counts, the study [14] carried out anomaly detection, the model is contrasted with four industry-standard anomaly detection algorithms: the box plot, isolation forest(IF), local outlier factor (LOF), and K-means models. An ensemble classifier (EC) [42] incorporating bagging and boosting has been used to address the issue of fraud class skewness, the approach are found to perform better when compared to the current methods. The study [43] addresses the issue of skewed datasets by using fuzzy C-means clustering and the selection of related instances. The authors address the issues with conventional under-sampling strategies to enhance the detection performance and accuracy. To identify fraudulent transactions, the study [44] suggested LSTM ensemble, SMOTE-ENN was used to address the problem of fraud skewness. The method outperformed other algorithms in terms of performance, but, SMOTE method may occasionally produce instances that are not typical instances of the minority class. A dynamic ensemble technique [45] for anomaly identification in the Internet of Things systems is proposed. To address the issue of fraud skewness, the borderline-synthetic minority over-sampling approach (Borderline-SMOTE), One-Sided Selection (OSS), and adaptive synthetic (ADASYN) were applied in the study [46], OSS were found to be optimal under-sampling technique and that adaptive synthetic (ADASYN) performs better when employing the gradient tree boosting (GTB) classifier. Random forest ensemble approach [47] performed exceptionally well on oversampling and under-sampling. Though under-sampling usually led to the loss of important information while on the other hand, oversampling brings information that may not be fully a representative of the training set.

It is widely acknowledged that the skewed distribution of fraud instances presents a significant challenge for many machine learning models. The resampling techniques that have been used in effective fraud skewness mitigation may not be free from certain shortcomings. The resampled instances usually suffer from non-representative of the dataset, overfitting, and the loss of important data. Hence, there is a need to augment the effort of machine learning algorithms with novel approach in overcoming this challenge.

D. RESEARCH PROBLEM

The problem of NBA fraud keeps increasing daily as the number of online banking service users keeps increasing [3].

TABLE 1. Table of related studies.

Cit.	Year	Title of the Study	Fraud types	Methods	Performance
[14]	2021	Anomaly and fraud detection in credit card transactions using the ARIMA model	Credit card fraud	Box plot, LOF, IF, and K-means	Recall = 0.6667
[21]	2022	The relationship between auditor characteristics and fraud detection	Financial statement fraud	OLS for regression	P-value = 0.45
[24]	2022	Hexagon fraud: Detection of fraudulent financial reporting in state-owned enterprises Indonesia	Financial statement fraud	LR for classification	P-value < 0.01
[25]	2022	Gender diversity and financial statement fraud	Financial statement fraud	Probit model for classification	P-value < 0.01
[36]	2022	Integrating machine learning algorithms with quantum annealing solvers for online fraud detection	Credit card fraud	SVM for classification	AUC = 0.99
[27]	2022	Detecting the probability of financial fraud due to earnings manipulation in companies listed in Athens Stock Exchange Market	Financial statement fraud	Beneish model for estimation	M-score= -2.22
[28]	2022	Detecting financial fraud using two types of Benford factors: evidence from China	Corporate fraud	OLS for regression	Error rate = 0.292
[11]	2022	A proposal of a suspicion of tax fraud indicator based on Google trends to foresee Spanish tax revenues	Tax fraud	Factor analysis for regression	Std error = 0.0868
[40]	2022	Digital payment fraud detection methods in digital ages and Industry 4.0	Credit card fraud	LR, KNN DT, RF & AE for classification	Specificity = 0.98
[13]	2022	A blockwise network autoregressive model with the application for fraud detection	Loan fraud	AR Model for regression	P-value < 0.01
[30]	2022	The effect of enterprise risk management on prevention and detection of fraud in Indonesia's local government	Financial statement fraud	OLS for regression	P-value < 0.01

TABLE 1. *(Continued.)* **Table of related studies.**

[31]	2022	Robust financial fraud alerting system based on the cloud environment	Credit card fraud	PP for classification	TP rate = 0.9709
[32]	2022	Operational risk assessment of third-party payment platforms: a case study of China	E-commerce fraud	VaR, ES for loss estimation	VaR = 724.46
[44]	2022	A neural network ensemble with feature engineering for improved credit card fraud detection	Credit card fraud	SVM, MLP, DT & LSTM for classification	Sensitivity = 0.996
[45]	2022	A dynamic ensemble algorithm for anomaly detection in IoT imbalanced data streams	Cyber fraud	EC for classification	Accuracy = 0.9406
[46]	2022	Data sampling strategies for click fraud detection using imbalanced user click data of online advertising: An empirical review	Mobile advertising	KNN, DT, DA, LR, SVM, GTB & RF for classification	Precision = 0.6432
[47]	2022	Credit card fraud detection under extreme imbalanced data: A comparative study of data-level algorithms	Credit card fraud	AdB, RF, XGB, KNN & SVM for classification	Recall =1.00
[19]	2023	Fairness-aware data valuation for supervised learning	NBA fraud	LGBM for classification.	TP rate = 0.8
[35]	2023	Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation	Financial statement fraud	Chi-square, Fisher test & Correlation for testing relationship	P-value < 0.05
[38]	2023	Estimating financial fraud through transaction-level features and machine learning	Credit card fraud	XGBoost for classification	Accuracy = 0.998
[39]	2023	Dynamic graph neural network-based fraud detectors against collaborative fraudsters	Telecommunication fraud	DGNN for classification	Precision = 0.9292
[41]	2023	Credit card fraud detection: an improved strategy for high recall using KNN, LDA, and linear regression	Credit card fraud	KNN, LDA, and regression	Recall = 1.00
[26]	2023	Fraud detection and prevention	Financial statement fraud	OLS for regression	P-value < 0.05
[4]	2023	Effect of fraud on commercial banks' performance in Nigeria	Financial fraud	OLS for regression	P-value < 0.05
[43]	2023	Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS)	Credit card fraud	ANN, LR, KNN, NB for classification	Accuracy = 0.966
[9]	2023	Online payment fraud: From anomaly detection to risk management	Identity theft fraud	EC for classification	FP rate = 0.004
[22]	2023	Political alignment and corporate fraud: evidence from the United States of America	Corporate fraud	Pooled OLS for regression	P-value < 0.01
[23]	2024	Fraud detection using fraud triangle theory: Evidence from China	Corporate fraud	OLS for regression	P-value < 0.05
[37]	2024	Financial fraud detection using quantum graph neural networks	Financial fraud	QNN for classification	AUC = 0.85

ML techniques applied in many researches shows a promising performance in overcoming NBA fraud. However, most ML struggles when the distribution fraud instances are skewed as in the case of BAF dataset. The studies [18], [19] utilize LGBM to address skewed fraud instances using the True Positive (TP) rate as a performance measure. The study [15] utilizes stacking in ensembled learning with majority voting to evaluate the BAF dataset and address the changing fraud patterns. The study [20] uses federated learning in addressing data privacy issues and deep neural networks to classify fraud with TP rate as a metric. These studies achieve good performance in addressing BAF challenges. However, the studies did not consider the potential losses of fraud risk features. Major problems this paper addresses include:

- Most existing studies do not consider potential losses of fraud risk features, but fraud instances happen rarely and cause big losses when they occur.

- Fraud instances are inherently skewed compared to non-fraud instances, producing a highly skewed distribution.
- Fraud patterns tends to have more irregular and extreme values, while models like logistics regression or regression assume normality and predictions may produce an inaccurate result.

III. PROBLEM DEFINITION

This paper considers $X_i = x_1, x_2, \ldots, x_n$ as a vector of observation in a respective raw feature. The X_i is transformed to log return $X_p = x_1, x_2, \ldots, x_m$ which is a vector of log returns. The log return X_p is computed using $log\left(1 + \frac{x_i}{x_{i-1}}\right)$. The log returns are assessed using value-at-risk to determine the risk of fraud for each respective feature. The fraud instances are considered as the worst-case scenario and beyond. The value-at-risk model is the tail of a distribution i.e., extreme quantiles where fraud occurs. The historical simulation was conducted to estimate potential losses distribution $\tilde{\ell}_p = \ell\left(X_p\right) = -(f\left(t+1, Z_t + x_p\right) - f\left(t, Z_t\right))$. The extreme value theorem is applied to estimate the tail distribution based on fraud instances skewness. The value-at-risk V as a risk measure that assesses the risk of the features is the sum of expected loss ℓ and expected shortfall C, as can be seen in (3). The risk-return features were obtained as log return passes through the formulation comprising ℓ, $\mathcal{V}$, and $\mathcal{C}$ as given in (9-12) and the equations are derived based on tree event of fraud instances. The value-at-risk quantified risks across mean, worst-case, and extreme scenarios. This study aims to detect NBA fraud based on risk-return features using the KNN model.

IV. MATERIALS AND METHODS

This section discusses the materials and methods adopted in this research.

A. PROPOSED METHOD

The proposed design of this research is illustrated in *Fig. 1* which describes the steps and process involved in NBA fraud detection. Value-at-risk being an important part of this research is designed to model the severe and extreme fraud risk features, it also focuses on rare fraud instances that are detrimental and very costly when occurred. However, the rare cases that are mostly skewed can distort machine learning algorithms [51] especially distance based like KNN. The value-at-risk can handle the fraud skewness through the utilization of adjustable threshold probability ranges (confidence level) unlike the conventional methods that employ constant fraud probability weight that's attached to the skewed fraud instances. The preprocessed, extracted and engineered features were sent as input to value-at-risk for simulation. Meanwhile, a distance based KNN is designed for adjustability to detect fraudulent features through identifying rare clusters with nearest neighbor distance k. The confidence level chosen considers the rare fraud cases as higher risk features that would result in fewer training sets,

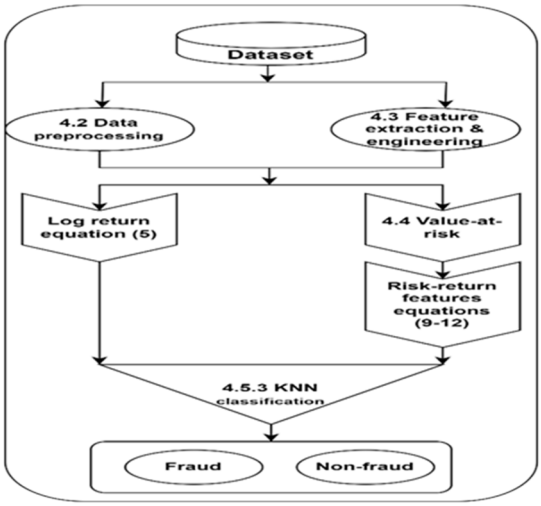

FIGURE 1. Proposed method.

particularly for the KNN model with hyperparameter k. The fraud detection model requires the optimization of k to a lower setting to sufficiently model the fraudulent features in the rare cluster. The distance weight of KNN is imperative in inhibiting fraud skewness by assigning a higher weight to near instances which in turn facilitates efficient detection of skewed instances.

Additionally, this paper put forward a novel approach to NBA fraud detection through the utilization of value-at-risk that appropriately models the fraud skewness. The selection of a 99.5% confidence level highlighted the need to capture 0.5% of extreme fraud risk instances which fit to fall under the subset of 1% fraud rate (detection effectiveness) as shown in *Fig. 2*. The value-at-risk which is finance and risk management tools model the tails of a fraud event that are extreme. Consequently, a novel detection rate performance metrics that incorporate the risk of skewed fraud instances into the overall performance measure of detecting rare instances were put forward which will later be seen in (21). The metrics provides the model with capacity to identify and attach more weight to rare and extreme fraud instances by including the fraud rate and confidence level in detection process. Therefore, this research put forward a single metrics that capture overall rate of fraud detection based on risk exposure. Under an acceptable loss tolerance in the banking sector, value-at-risk presents an intelligent approach for establishing data-driven criteria for fraud risk management.

B. DATA PREPROCESSING

This paper carries out preprocessing tasks to improve the quality of features and ensure model accuracy. The redundant feature *device_fraud_count* contains zero instances all of which were manually removed from the data making the model less complex. The categorical features *device_os*, *employment_status*, *payment_type*, and *housing_status* were labeled to make them easier to learn

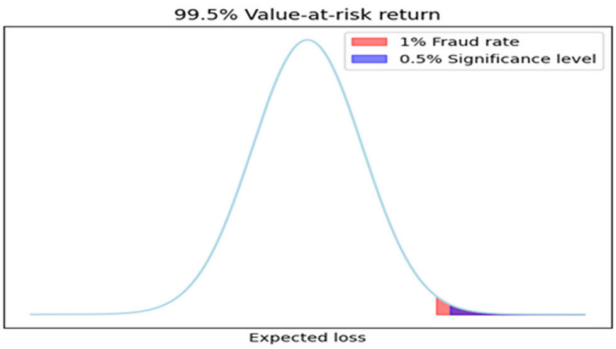

FIGURE 2. Value-at-risk return curve.

TABLE 2. Table of new features.

S/N	Description	New feature	Formulation
1	Total duration in a location	*total_dur*	= *prev_address_months_count* + *current_address_months_count*
2	Total velocity	*total_vel*	= *velocity_6h* + *velocity_24h* + *velocity_4w*
3	Phone consistency	*phone_con*	= *phone_home_valid* + *phone_mobile_valid*
4	Credit risk score	*credit_ratio*	= *intended_balcon_amount*/ *proposed_credit_limit*
5	Credit capacity	*credit_cap*	= *income* / *proposed_credit_limit*
6	Credit utilization	*credit_ut*	= *intended_balcon_amount*/ *credit_risk_score*
7	Transaction intensity	*trans_int*	= *total_vel* × *session_length_in_minutes*

because machine learning cannot process features that are non-numeric. The features *zip_count*, *keep_alive_session* and *bank_months_count* were eliminated to avoid noise and collinearity issues. The features *foreign_request*, *has_other_card*, and *email_is_free* were eliminated as they give too much undefined log returns.

C. FEATURE EXTRACTION AND ENGINEERING

The development of a NBA fraud detection model was based on the selection of relevant features from demographic, behavioral, risk management and transactional perspective. Demographic features such as *income*, *customer_age*, and *employment_status* were selected. Behavioral features such as *bank_branch_count_8w* and *housing_status* were selected. Risk-based features that include *credit_risk_score* and *proposed_credit_limit* were selected. Transactional features such as *days_since_request*, *total_velocity*, and *payment_type* were also selected. Additionally, two or more existing features are combined to form a new feature as given in Table 2. The features engineered are based on location, velocity of transactions, default risk, and ability to repay loans to determine the likelihood of fraudulent behaviors. The selected features were used along with the other raw features for accurate model training.

D. VALUE-AT-RISK $\mathcal{V}$

Because of the value-at-risk emphasis on statistically extreme but significant fraud instances, it is ideally more suitable for the development of efficient fraud detection models. In the financial sector, value-at-risk is a quantile of loss distribution that gives a range of potential losses and is one of the most frequently used measures of risk. $\mathcal{V}$ can also be termed as a statistical measure of the risk of loss over a specific time at a given confidence level. It also plays a significant part in the Basel regulatory framework. $\mathcal{V}$ has a confidence level $\alpha \in (0, 1)$ [48]. This experiment adopted the Solvency II framework which uses a one-year horizon with the level of confidence, α equal to 0.995. It can be written as in (1):

$$\mathcal{V} = \mu + \sigma Z^{-1}(\alpha) \tag{1}$$

where μ is the mean of a log loss returns and σ is the standard deviation of returns, Z represents the standard normal, and $Z^{-1}(\alpha)$ represent the $\propto$ quantile of Z. The value-at-risk [49] can also be written as in (2):

$$Value - at - risk = Expected\ loss + Unexpected\ loss \tag{2}$$

In this paper, we consider the unexpected loss to be the expected shortfall. Therefore, the general relationship will be written as given in (3):

$$\mathcal{V} = \ell + \mathcal{C} \tag{3}$$

Generally, expected loss alone does not sufficiently handle the tail risk of losses, applying $\mathcal{V}$ additionally quantifies the aggregate potential losses of fraud risk features. The addition of $\mathcal{C}$ will further quantify the extreme loss effects. This combination will allow quantification of risk across mean, worst-case, and extreme scenarios. The metrics will aggregate their strengths and overcome their weakness.

1) EXPECTED LOSS ℓ

Expected loss is an important risk measure for estimating the average or probable loss expected from a specific risk exposure. Intuitively, it indicates loss occurrence on average in a repeated situation. ℓ is measured usually based on 1 year, the higher value of ℓ indicates a high risk of exposure. ℓ does not sufficiently handle tail risks as it is considered more of an average risk measure, due to this limitation, there is a need for support by other risk measures like $\mathcal{V}$ and $\mathcal{C}$. The expected losses can be written mathematically in (4):

$$\ell = E\left(X_{p+1}\right) = \frac{\sum_{p=t-n+1}^{m} x_m}{p} = \mu \tag{4}$$

The X_p is a log return which was computed using the formula (5). The addition of 1 is to avoid having too much negative and undefined log returns.

$$X_p = \log\left(1 + \frac{x_i}{x_{i-1}}\right) \tag{5}$$

2) EXPECTED SHORTFALL $\mathcal{C}$

In other words, $\mathcal{C}$ is a conditional value-at-risk given that the loss ℓ exceeds the $\mathcal{V}$ threshold at the specified confidence level α. The $\mathcal{C}$ as given in (6,7) represents the level for the worst $100(1-\alpha)\%$ losses in the distribution. It focuses on the severity of the rare worst-case losses ignored by $\mathcal{V}$.

$$\mathcal{C} = \frac{1}{1-\alpha}\int_{\alpha}^{1} \mathcal{V}\left(X_p\right) dx \tag{6}$$

$$\mathcal{C} = \frac{1}{1-\alpha}\int_{\alpha}^{1} [\mathcal{V} = \mu + \sigma Z^{-1}(\alpha)] dx \tag{7}$$

However, the $\mathcal{V}$ can be computationally expensive and difficult to apply to complex financial portfolios. It does not also give information on the severity of loss. To augment such weakness of $\mathcal{V}$, expected shortfall $\mathcal{C}$ were employed to estimate the severity of losses in the worst cases. Historical simulation is adopted to estimate the losses of fraud risk features.

3) HISTORICAL SIMULATION

This is a non-parametric technique that uses past information to model possible loss in the future [50]. This utilizes empirical distribution to estimate the loss distribution of previous changes in risk features. The advantage of historical simulation over covariance method of loss estimation is its ability to adapt over time and can model dynamic conditions. The loss distribution $\tilde{\ell}_p$ measure the change in value between the returns $f\ (t, Z_t)$ at time t and returns $f\ \left(t{+}1, Z_t + x_p\right)$ at time $t+1$ in a specific confidence level, the negative value is indicating the interest in quantification of loss given in (8), Z_t denotes condition of returns at time t.

$$\tilde{\ell}_p = \ell\left(X_p\right) = -\left(f\left(t+1, Z_t + x_p\right) - f\left(t, Z_t\right)\right) \tag{8}$$

4) TREE EVENT OUTCOME

Even tree is employed in risk assessment and analysis to pinpoint different event sequences for both fraud and non-fraud that may result in a particular outcome. An event tree also known as an incidence response tree (IRT) [49] contains four possible outcomes as given (9-12) that are based on prevention, detection, and response. The event tree significantly tracks fraudulent activities and estimates the return outcomes of monitoring decisions, hence improving prediction and risk models. The formulation of this paper is based on Dan Gorton [49]: Fraud without detection, fraud despite detection, fraud detected and stopped, and high-risk fraud stopped. The detection effectiveness γ is the fraud rate:

1. Fraud without detection: γ is not regarded as fraud goes undetected as in (9). The worst-case scenario $\mathcal{V}$ of losses when fraud stays undetected is understood by using the ℓ which is the mean of returns μ. $\mathcal{C}$ aids in evaluating the tail risk related to undetected fraud.

$$Quantile\left(\mu, 99.5\%\right) = \ell + Average(X_p | X_p > \mathcal{V}) \tag{9}$$

where $\ell = \mu, \mathcal{V} = Quantile\left(\mu, 99.5\%\right)$, and $\mathcal{C} = Average(X_p | X_p > \mathcal{V})$

2. Fraud despite detection: When fraud occurs with (1 - γ) detection, there is a reduction in ℓ and $\mathcal{V}$ in proportion to γ, while C remains the same as given in (10).

$$Quantile(\mu, 99.5\%) \times (1-\gamma) = \mu \times (1-\gamma) + Average(X_p | X_p > \mathcal{V}) \tag{10}$$

where $\ell = \mu \times (1-\gamma)$, $\mathcal{V} = Quantile(\mu, 99.5\%) \times (1\gamma)$, and $\mathcal{C} = Average(X_p | X_p > \mathcal{V})$

3. Fraud detected and stopped: This stops detection before major damage as shown in (11). Fraud is detected by γ and ℓ are restricted to the expenses related to prevention and detection, both $\mathcal{V}$ and ℓ are proportional to γ, while $\mathcal{C}$ remains the same.

$$Quantile\left(\mu, 99.5\%\right) \times \gamma = \mu \times \gamma + Average(X_p | X_p > \mathcal{V}) \tag{11}$$

where $\ell = \mu \times \gamma$, $\mathcal{V} = Quantile\left(\mu, 99.5\%\right) \times \gamma$, and $\mathcal{C} = Average(X_p | X_p > \mathcal{V})$

4. High-risk fraud stopped: This refers to fraud that is avoided because of potential risk exposure as given in (12). The ℓ is the associated cost of prevention and detection of high-risk fraud, it is assumed that the associated costs are relatively lower than the mean loss. $\mathcal{V}$ is the 99.5 percentile of loss returns, $\mathcal{C}$ quantifies average loss beyond $\mathcal{V}$.

$$Quantile\left(\gamma, 99.5\%\right) = \mu(1-\alpha) + Average(X_p | X_p > \mathcal{V}) \tag{12}$$

where $\ell = \mu(1-\alpha)$, $\mathcal{V} = Quantile\left(\gamma, 99.5\%\right)$, and $\mathcal{C} = Average(X_p | X_p > \mathcal{V})$

In each of the four scenarios, these risk measures have distinct and significant roles played in managing the costs and risks related to fraud detection and prevention strategies.

E. NBA FRAUD DETECTION MODEL SELECTION

Machine learning models can utilize high dimensional data to analyze complex fraud patterns that humans or rule-based systems would not. Supervised ML has unique significance in employing labeled data to find the patterns, anomalies, and fraudulent activity. Binary logistic regression (BLR) is suitable in handling categorical data and is good due its interpretability. Naïve bayes (NB) has efficiency and simplicity in terms of cost and time. K-nearest neighbor (KNN) has high effectiveness in fraud detection when managing transactional information, adaptability, and as well as its potential use in hybrid form.

1) BINARY LOGISTIC REGRESSION

BLR is a supervised ML [50] that is very effective in fraud detection capability due to its suitability in handling categorical data and its interpretability [51]. The solution for the fraud detection model is constructed by utilizing the binary fraud class y and features X_i [52]. X_i is a vector of features $(x_1, x_2, \ldots, x_n)$ capable of influencing the decision

of fraud detection model to classify features as either fraud or non-fraud class $y \in (0, 1)$. BLR function uses the sigmoid function on $y \in (0, 1)$. The mathematical expression is given in (13,14):

$$\log(y) = \beta_0 + \sum X_i \beta_i \tag{13}$$

$$logit = \frac{Probability\ of\ fraud}{Probability\ of\ non-fraud} = log\left(\frac{y}{1-y}\right) \tag{14}$$

2) NAÏVE BAYES CLASSIFIER

Based on the Bayes theorem, the Naive Bayes is a supervised machine learning algorithm [53]. The NB is very suitable in fraud detection for its efficiency in terms of cost, time, and high accuracy [54]. When given the fraud class, the NB classifier assumes that all fraudulent features are independent of each other. Assume the target feature tobe $Y_j \in (0,1)$ and that X_i is a vector of fraudulent features. The $P(Y_j/X_i)$ is the generic conditional probability X_i given Y_j. The Gaussian function of NB is given in (15), where σ^2 and $\bar{x}$ are the variance and mean of probabilities.

$$P\left(\frac{X_i}{Y_j}\right) = \frac{1}{\sqrt{2\pi\sigma_j^2}} e^{-\left(\frac{(x_i-\bar{x})^2}{2\sigma_j^2}\right)} \tag{15}$$

3) K-NEAREST NEIGHBOR

KNN is a supervised machine learning algorithm that is useful for problem classification [55] and is good for its better detection and lower FP rate. KNN has high effectiveness in fraud detection when managing transactional information, adaptability, and as well as its potential use in hybrid form [56]. To determine whether there has been fraudulent behavior in fraudulent features X_i, studies employ KNN to classify X_i into fraud class $Y_j \in (0,1)$. Two estimates are needed for the KNN fraud detection technique: The transaction correlation and the distance between the transaction's occurrence of the fraud features. The indicator function is given in (16):

$$E\left(Y_j, X_i\right) = \begin{cases} 1, & if\ Y_j = X_i \\ 0, & elsewhere \end{cases} \tag{16}$$

V. EXPERIMENTAL SETUP

The simulation of value-at-risk was conducted in a Microsoft Excel environment, and the development of fraud detection models was conducted using Python. Experimental procedures that are carried out for developing a fraud detection model.

A. DATASET

A real-world BAF dataset is accessible to the public [18]. It contains 32 features with 1 million instances. The dataset contains details about the demographic, behavioral, risk, and transactional features. The dataset is highly skewed with a fraud class of 11029 and a non-fraud class of 988971 as shown in Fig. 3. The primary obstacle to the detection of NBA fraud is the scarcity of datasets. The BAF dataset remain the only data in this domain. As such, the evaluation of this research paper is forced to rely on the BAF dataset.

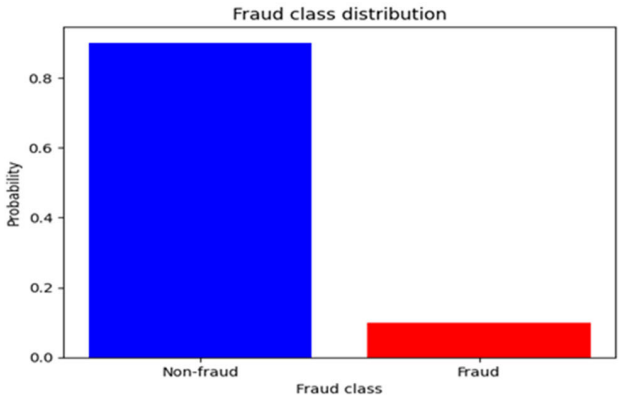

FIGURE 3. Fraud class distribution.

B. PERFORMANCE METRICS

The confusion matrix is used to evaluate the performance of a classification model and contains the values of true positive (TP), false positive (FP), true negative (TN), and false negative (FN) [52]. The majority of studies in the literature utilize the true positive (TP) rate, to give room for comparison, evaluation metrics such as accuracy, f-score, TP rate, and FP rate. A novel detection rate was additionally proposed that integrate the overall detection performance with associated risk exposure. The Accuracy measures the overall performance of the model, F-score integrates precision (1-FP rate) and recall (TP rate) in a skewed dataset that struggles to balance between minimizing FN and FP. The TP rate measure the proportion of correct detection performance. The FP rate measure the proportion of incorrect detection. The metrics are given mathematically in (17-20).

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{17}$$

$$TPrate = \frac{TP}{TP + FN} \tag{18}$$

$$FPrate = \frac{FP}{FP + TN} \tag{19}$$

$$F-score = \frac{2 \times TP}{2 \times TP + FP + FN} \tag{20}$$

The novel detection rate measures the overall rate of detection that incorporate the risk of detecting extreme instances. The γ denotes the fraud rate and α denotes the confidence level as given in (21). The component $\frac{(1+\gamma(1-\alpha))}{(1+\gamma)}$ is proportional to the proportion of extreme fraud instances exceeding α. It has the advantage of integrating the capacity to detect rare but extremely significant fraud cases with the overall detection performance. The detection rate ranges from 0 to 1.

$$Detection\ rate = \frac{(1 + \gamma(1-\alpha))TP}{(1+\gamma)(TP + FN)} \tag{21}$$

C. NBA FRAUD DETECTION MODEL DEVELOPMENT

This section discusses the procedure for the development of NBA fraud detection model using raw features. Raw features refer to the features in the initial stage that went through pre-processing, feature extraction, and engineering steps before transformation to either logarithmic or risk-return features. The datasets contain different format types and features in number type were converted to integers for simplicity and efficiency in processing the fraud detection model. Features that cause noise and collinearity were removed from the datasets to increase the performance of the model. Relevant features that facilitate accuracy were selected from demographic, behavioral, transactional, and risk perspectives. New features are engineered based on location, the velocity of transactions, default risk, and ability to repay loans to determine the risk of fraudulent behaviors. The processed features and newly engineered features were used to form the set of raw features and is highly skewed. The raw features were sent as input to the machine learning models to classify features as either fraud or non-fraud. BLR, KNN, and NB models are employed to build a fraud detection model.

D. EXECUTIONN OF THE PROPOSED APPROACH

The NBA fraud detection model presented in section C is achieved through the utilization of raw features. The raw features undergo preprocessing and feature selection. The engineered features along with other features were sent for training using different machine learning models. However, the results obtained are not very good for NBA fraud detection. Hence, the poor performance of raw features which is attributed to skewed data distribution highlighted the need for model improvement. The raw features were modeled by value-at-risk for improvement. Initially, raw features were transformed into a log return, the log returns were then passed through (3) of value-at-risk $\mathcal{V}$. The risk-return features were obtained from $\mathcal{V}$, ℓ and $\mathcal{C}$ as seen in (9-12). The risk-return features were then subjected to classification by machine learning models. Machine learning models such as BLR, NB, and KNN were employed to develop the NBA fraud detection model. BLR is essentially a probability prediction model that needs to be turned into binary values. The maximum likelihood estimate is used to estimate the weights of BLR. A real-valued set of risk-return features is mapped into a binary class of fraud and non-fraud using the sigmoid function. A model that predicts a value very close to 1 is produced by using the best weights. Using the risk-return features in Naïve bayes, the conditional probability of fraud feature and the prior probability of fraud class are computed. To predict the fraud class based on new features, the posterior probability of the fraud class is obtained by combining the learning of probability distributions with Bayes' rule. The K-NN algorithm detects the K nearest neighbors, using a distance metric, to a given data point. The majority vote of the K neighbors is then used to establish the fraud class. Using this method enables the algorithm to classify outcomes based on the local structure of the data and adjust to various patterns.

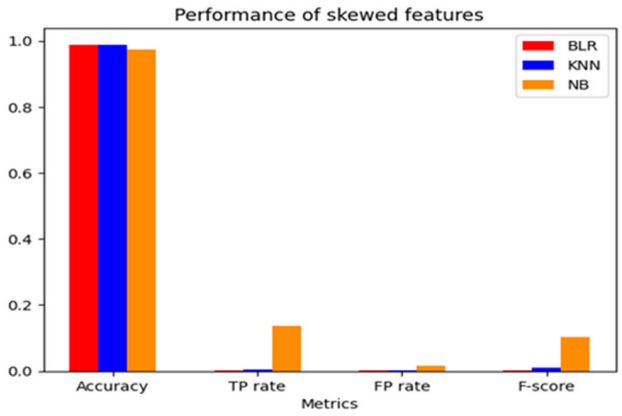

FIGURE 4. Performance evaluation of fraud detection model with skewed features.

VI. RESULTS ANALYSIS AND DISCUSSION

This section presents the general results obtained from experimental research with skewed fraud instances and risk-return features with their validation. The 10-fold cross validation was used to evaluate NBA fraud detection models.

A. RESULT OF NBA FRAUD DETECTION MODEL WITH SKEWED FRAUD INSTANCES

This section presents the result of the NBA fraud detection model with skewed instances using BLR, KNN, and NB. The results are presented in Table 3, the best metric results among the models were written in bold number. The accuracy result of BLR, KNN, and NB are 0.9869, 0.9884, and 0.9743 respectively. The TP rate results of BLR, KNN, and NB are 0.0016, 0.0061, and 0.1355 respectively. The FP rate results of BLR, KNN, and NB are 0.002, 0.0007, and 0.0163 respectively. The f-score results of BLR, KNN, and NB are 0.0028, 0.0115, and 0.1042 respectively. The illustrations of the metric results are demonstrated in Fig. 4. It can be observed that the results of accuracy and FP rate were good. However, the results of the TP rate and f-score were not very good. The TP rate is a very important metric especially in fraud detection, robust and accurate fraud detection must attain a good TP rate. The poor performance of the fraud detection model, particularly in TP rate and f-score, using fraud skewed instances highlighted the need for model improvement. We employ to improve the fraud detection model using value-at-risk augmented features which is presented in section B.

B. RESULT OF AN IMPROVED NBA FRAUD DETECTION MODEL USING VALUE-AT-RISK

This section presents the results of an improved NBA fraud detection model using BLR, KNN, and NB. The result indicated good performance by KNN and the results are written

TABLE 3. Result of fraud detection model with raw features.

Metrics	BLR	KNN	NB
Accuracy	0.9869	**0.9884**	0.9743
TP rate	0.0016	0.0061	**0.1355**
FP rate	0.0020	**0.0007**	0.0163
F-score	0.0028	0.0115	**0.1042**

TABLE 4. Result of an improved fraud detection model.

Metrics	BLR	KNN	NB
Accuracy	0.8000	**0.9167**	0.8667
TP rate	0.7500	**0.9500**	0.8750
DT rate	0.7426	**0.9406**	0.8580
F- score	0.7333	**0.9333**	0.8333

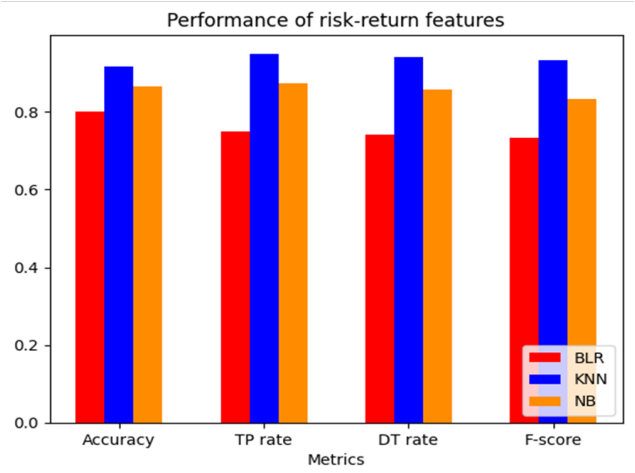

FIGURE 5. Performance evaluation of risk-return features.

in bold number as shown in Table 4. The accuracy results of BLR, KNN, and NB are 0.8, 0.9167, and 0.8667 respectively. The TP rate results of BLR, KNN, and NB are 0.75, 0.95, and 0.875 respectively. The detection (DT) rate results of BLR, KNN, and NB are 0.7426, 0.9406, and 0.8580 respectively. The f-score results of BLR, KNN, and NB are 0.7333, 0.9333, and 0.8333 respectively. The illustrations of the metric results are demonstrated in Fig. 5. The results show that KNN has better performance in accuracy, TP rate, DT rate, and f-score. Overall, it can be concluded that the KNN model outperforms other models to emerge as the best NBA fraud detection model.

The Receiver operating curve (ROC) in *Fig. 6* presents the classification capability, it indicates a high TP rate and low FP rate across different threshold values. The KNN model demonstrates high robustness in fraud detection as compared to BLR and NB.

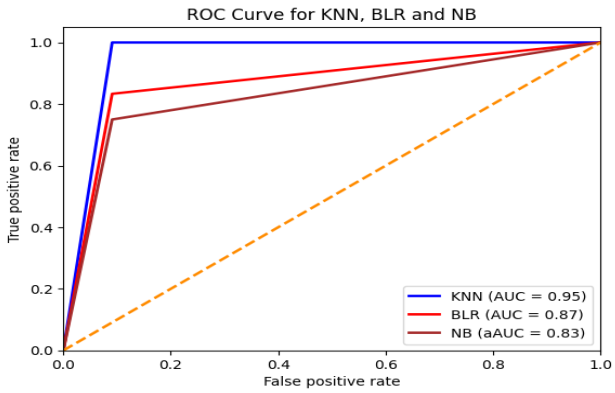

FIGURE 6. Receiver operating curve for the fraud models.

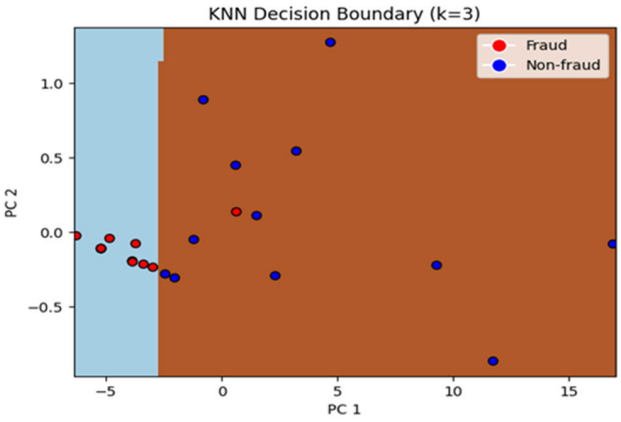

FIGURE 7. Decision boundary for KNN.

The risk-return features were reduced using principal component analysis to map the KNN decision boundary. The principal components (PC) were utilized to plot the KNN decision boundary. *Fig. 7* indicates that the KNN model identifies the fraud risk patterns based on its exhibited linear boundary which translates to a relatively simple relationship among fraud risk features. Also, the dominance of one class in a particular region may signal a distinct fraudulent feature through smaller $k = 3$ which successfully reduce the influence of skewed instances which is manifested by a high TP rate.

C. RELIABILITY ANALYSIS

The reliability analysis of the value-at-risk-based fraud detection model is done using the Kupiec test. Kupiec proposed an additional failure rate-based test in 1995 [57]. The test measures the frequency with which a value-at-risk is violated over a specified period. The test null hypothesis is when the expected violation rate by the value-at-risk model and the observed violation rate are equal and is given in (22) as h. The test statistic follows chi-square with 1 degree of freedom

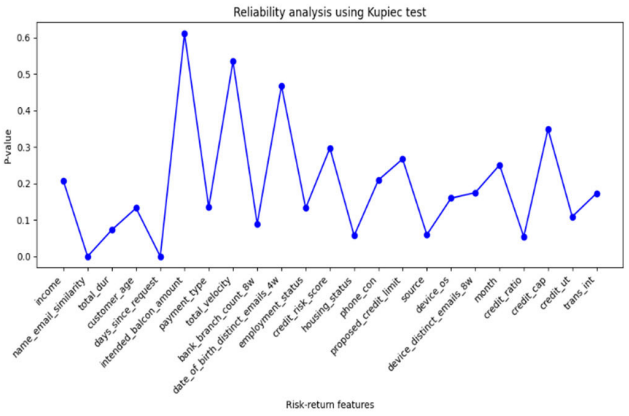

FIGURE 8. Reliability analysis.

is given in (23) as the likelihood ratio (LR):

$$h = \frac{number\ of\ violations}{total\ numbr\ of\ observations} = \frac{v}{t} \tag{22}$$

$$LR^2 = -2ln\left(\frac{(1-h_{exp})^{t-v}\, h_{exp}^{v}}{(1-h_{obs})^{t-v}\,(h_{obs})^{t}}\right) \sim X_1^2 \tag{23}$$

The result for the test at a 5% significance level is given in *Fig. 8*. It can be seen that only *name_email_similarity* and *days_since_request* were found not to be consistent the observed violation rate. The rest of the features were found to be consistent and reliable. Hence, the incorporation of value-at-risk were adequate and reliable.

D. COMPARISON WITH THE STATE-OF-THE-ART METHODS IN NBA FRAUD DETECTION

The results of our experiment are compared with the state-of-the-art methods for NBA fraud. The study [18] used 100 sets of hyperparameters for parameter configuration to optimize the LGBM model performance and obtained a TP rate result of about 0.6, under-sampling techniques for handling class skewness were used as part of hyperparameters. The study [19] utilizes 25 sets of hyperparameter configurations to optimize the LGBM model and obtained a TP rate result of almost 0.8, utility aware reweighing is used to handle the class skewness. Additionally, the study [15] uses ensemble learning techniques in which stacking was specifically applied to handle class skewness, the strengths of the weaker models trained were aggregated using majority voting to address evolving patterns and achieved a 0.9 TP rate result. Another study [20] combined federated learning to handle data privacy and SHAP value to ensure interpretability of feature importance by human experts, the deep neural network was used to recognize patterns of fraud, and a TP rate of about 0.75 was achieved, SMOTE were employed to handle class skewness. Our paper uses KNN with k hyperparameter to detect fraud with a TP rate of 0.95. We overcome fraud skewness using value-at-risk that considers fraud instances as a worst-case scenario through the utilization of adjustable threshold probability ranges weight that's attached to the skewed fraud instances. The results for comparison are given in Table 5. Also, while our paper reached an accuracy of 0.9167, another study [58] employed the BAF in evaluation with 0.677 of an accuracy. Our approach was particularly better than the methods that are currently in existence.

TABLE 5. Comparison with the state-of-the-art methods.

Methods	TP rate
LGBM[18]	0.6000
LGBM[19]	0.8000
Ensemble Learning[15]	0.9000
DNN[20]	0.7500
Our Proposed method	**0.9500**

TABLE 6. Ablation study using F-score.

Log return	BLR	KNN	NB
$log\left(1+\frac{x_i}{x_{i-1}}\right)$	**0.7333**	**0.9333**	**0.7667**
$log\left(\frac{x_i}{x_{i-1}}\right)$	0.7273	0.7000	0.6667

TABLE 7. Parameter analysis involving learning rate *lr* of BLR.

Learning rate (*lr*)	0.01	0.02	0.03	0.055	0.09
Accuracy	0.8000	0.8000	0.8000	0.8333	0.8333

E. ABLATION STUDY

This paper conducted an ablation study to determine the contribution of components that influence the performance of the NBA fraud detection model. The choice of logarithmic return is among the components that impacted our result. Given log return $X_p = log\left(1+\frac{x_i}{x_{i-1}}\right)$, 1 is removed from log return formulae to become $X_p = \log\left(\frac{x_i}{x_{i-1}}\right)$. The result which can be seen in Table 6 shows F-score of new bank account fraud detection models. The removal of 1 resulted in decreased performance for BLR, KNN, and NB.

F. PARAMETER ANALYSIS

This paper examines hyperparameter space to determine the setup that led to optimum model efficiency and performance. The experiment utilizes different parameter ranges in BLR, KNN, and NB. For BLR, learning rate *lr* are examined, and the accuracy results of different parameter configurations are shown in Table 7. For KNN, the number of nearest neighbors *k* are evaluated and the accuracy results of parameter settings are shown in Table 8. For NB, the different probability

TABLE 8. Parameter analysis involving a number of nearest neighbors *k* of KNN.

Nearest neighbors (k)	1	2	3	4	5	6
Accuracy	0.9000	0.8167	0.9167	0.8333	0.8667	0.8333

TABLE 9. Parameter analysis involving a distribution assumption of NB.

Distribution	Gaussian	Multinomial	Binary
Accuracy	0.8333	0.8666	0.4500

distributions were evaluated and the accuracy results as given in Table 9.

VII. DISCUSSIONS AND CONCLUSION

This section presents a discussion of the results and the conclusion of our findings.

A. DISCUSSIONS

This paper explored improving the performance of NBA fraud detection model by employing value-at-risk. The performance of the fraud detection models was measured based on the removal of redundant features to lower the complexity of the model, the selection of an important feature capable of influencing fraud detection to avoid noise and collinearity, and the engineering of features from the contextual perspective that increase the model performance. The raw features were sent to BLR, KNN, and NB models for classification. KNN model outperforms other models as shown in Table 3 with an accuracy result of 0.9884, TP rate result of 0.0061, FP rate result of 0.0007, and f-score result of 0.0115. The performance of fraud detection is not very good and reliable as evidenced by the TP rate and f-score, hence, necessitating the need for the model improvement. Given that, value-at-risk was employed to improve the model. To improve NBA fraud detection model, raw features were simulated through value-at-risk. The risk-return features obtained from value-at-risk were sent to BLR, KNN, and NB models for classification. Among the models, the KNN model performs better as shown in Table 4 with an f-score result of 0.9333, TP rate result of 0.95, accuracy result of 0.9167, and DT rate result of 0.9406. The NBA fraud detection model based on value-at-risk features appears to have good performance. The reliability test conducted using the Kupiec test proved to be reliable and consistent as shown in Fig. 8. This indicates that the value-at-risk engineered features led to the improvement of K-nearest neighbor fraud detection model.

B. CONCLUSION

The value-at-risk-based fraud detection model presented in this paper enables the quantification and mitigation of fraud risk features and at the same time overcome the influence of skewed fraud instances which is very crucial in solving financial fraud challenges. The value-at-risk attach confidence probability weight to the rare fraud cases with nearest neighbor distance k. The distance weight of KNN is imperative in inhibiting class skewness by assigning a higher weight to near instances which in turn facilitates efficient detection of skewed instances. The deployment of expected shortfall and expected loss by value at risk allows quantification of risk across mean, worst-case, and extreme scenarios enabling aggregation of their strengths. Therefore, an accurate fraud detection system assists organizations in making effective choices and reducing the overall expense of fraud detection and prevention. This paper does not consider the time windows in the experiment. However, the major challenge is the lack of data availability in NBA fraud detection.

CONFLICT OF INTEREST

There are no competing interests disclosed by the authors.

AVAILABILITY OF DATA AND MATERIALS

The data used in this research is publicly available at https://github.com/feedzai/bank-account-fraud

ACKNOWLEDGMENT

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication and also would like to thank the School of Statistics & Mathematics, Zhejiang Gongshang University, China.

REFERENCES

[1] ACFE. *Association of Certified Fraud Examiners (ACFE) 2022 Report to the Nations*. Accessed: 2023. [Online]. Available: https://legacy.acfe.com/report-to-the-nations/2022/

[2] T. Ashfaq, R. Khalid, A. S. Yahaya, S. Aslam, A. T. Azar, S. Alsafari, and I. A. Hameed, "A machine learning and blockchain based efficient fraud detection mechanism," *Sensors*, vol. 22, no. 19, p. 7162, Sep. 2022.

[3] N. S. Alfaiz and S. M. Fati, "Enhanced credit card fraud detection model using machine learning," *Electronics*, vol. 11, no. 4, 662, 2022.

[4] A. Alfaadhel, I. Almomani, and M. Ahmed, "Risk-based cybersecurity compliance assessment system (RC2AS)," *Appl. Sci.*, vol. 13, no. 10, p. 6145, May 2023.

[5] D. Sarma, W. Alam, I. Saha, M. N. Alam, M. J. Alam, and S. Hossain, "Bank fraud detection using community detection algorithm," in *Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Jul. 2020, pp. 642–646.

[6] A. Pagano, "Digital account opening fraud on demand deposit accounts: An assessment of available technology," Ph.D. thesis, Utica College, Utica, NY, USA, 2020.

[7] Shuftipro. *New Account Fraud—A New Breed of Scams*. Accessed: 2023. [Online]. Available: https://shuftipro.com/reports-whitepapers/new-account-fraud.pdf

[8] R. Sasirekha, B. Kanisha, and S. Kaliraj, "Study on class imbalance problem with modified KNN for classification," in *Intelligent Data Communication Technologies and Internet of Things*, vol. 101. Singapore: Springer, 2022, pp. 207–217, doi: https://doi.org/10.1007/978-981-16-7610-9_15.

[9] P. Vanini, S. Rossi, E. Zvizdic, and T. Domenig, "Online payment fraud: From anomaly detection to risk management," *Financial Innov.*, vol. 9, no. 1, p. 66, Mar. 2023, doi: 10.1186/s40854-023-00470-w.

[10] X. Zhu, X. Ao, Z. Qin, Y. Chang, Y. Liu, Q. He, and J. Li, "Intelligent financial fraud detection practices in post-pandemic era," *Innovation*, vol. 2, no. 4, Nov. 2021, Art. no. 100176, doi: 10.1016/j.xinn.2021.100176.

[11] M. Monge, C. Poza, and S. Borgia, "A proposal of a suspicion of tax fraud indicator based on Google Trends to foresee Spanish tax revenues," *Int. Econ.*, vol. 169, pp. 1–12, May 2022, doi: 10.1016/j.inteco.2021.11.002.

[12] S. Kannan and K. Somasundaram, "Autoregressive-based outlier algorithm to detect money laundering activities," *J. Money Laundering Control*, vol. 20, no. 2, pp. 190–202, May 2017, doi: 10.1108/jmlc-07-2016-0031.

[13] B. Xiao, B. Lei, W. Lan, and B. Guo, "A blockwise network autoregressive model with application for fraud detection," *Ann. Inst. Stat. Math.*, vol. 74, no. 6, pp. 1043–1065, Dec. 2022, doi: 10.1007/s10463-022-00822-w.

[14] G. Moschini, R. Houssou, J. Bovay, and S. Robert-Nicoud, "Anomaly and fraud detection in credit card transactions using the ARIMA model," in *Proc. 7th Int. Conf. Time Forecasting*, Jul. 2021, p. 56, doi: 10.3390/engproc2021005056.

[15] A. A. Alhashmi, A. M. Alashjaee, A. A. Darem, A. F. Alanazi, and R. Effghi, "An ensemble-based fraud detection model for financial transaction cyber threat classification and countermeasures," *Eng., Technol. Appl. Sci. Res.*, vol. 13, no. 6, pp. 12433–12439, Dec. 2023, doi: 10.48084/etasr.6401.

[16] R. M. Aziz, R. Mahto, K. Goel, A. Das, P. Kumar, and A. Saxena, "Modified genetic algorithm with deep learning for fraud transactions of ethereum smart contract," *Appl. Sci.*, vol. 13, no. 2, p. 697, Jan. 2023, doi: 10.3390/app13020697.

[17] M. Hegazy, A. Madian, and M. Ragaie, "Enhanced fraud miner: Credit card fraud detection using clustering data mining techniques," *Egyptian Comput. Sci. J.*, vol. 40, no. 3, pp. 1–10, 2016.

[18] S. Jesus, J. Pombal, D. Alves, A. Cruz, P. Saleiro, R. Ribeiro, J. Gama, and P. Bizarro, "Turning the tables: Biased, imbalanced, dynamic tabular datasets for ML evaluation," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 35, 2022, pp. 33563–33575.

[19] J. Pombal, P. Saleiro, M. A. T. Figueiredo, and P. Bizarro, "Fairness-aware data valuation for supervised learning," 2023, *arXiv:2303.16963*.

[20] T. Awosika, R. Mani Shukla, and B. Pranggono, "Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection," 2023, *arXiv:2312.13334*.

[21] J. Khaksar, M. Salehi, and M. Lari DashtBayaz, "The relationship between auditor characteristics and fraud detection," *J. Facilities Manage.*, vol. 20, no. 1, pp. 79–101, Jan. 2022, doi: 10.1108/jfm-02-2021-0024.

[22] A. Cordis, "Political alignment and corporate fraud: Evidence from the United States of America," *J. Appl. Accounting Res.*, Oct. 2023, doi: 10.1108/jaar-06-2022-0159.

[23] M. J. Rahman and X. Jie, "Fraud detection using fraud triangle theory: Evidence from China," *J. Financial Crime*, vol. 31, no. 1, pp. 101–118, Jan. 2024, doi: 10.1108/jfc-09-2022-0219.

[24] T. Achmad, I. Ghozali, and I. D. Pamungkas, "Hexagon fraud: Detection of fraudulent financial reporting in state-owned enterprises Indonesia," *Economies*, vol. 10, no. 1, p. 13, Jan. 2022.

[25] Y. Wang, M. Yu, and S. Gao, "Gender diversity and financial statement fraud," *J. Accounting Public Policy*, vol. 41, no. 2, Mar. 2022, Art. no. 106903.

[26] J. Hendieh, M. Schneider, and T. Sakr, "Fraud detection and prevention," *Middle-East J. Sci. Res.*, vol. 31, no. 1, pp. 44–52, 2023.

[27] A. Maniatis, "Detecting the probability of financial fraud due to earnings manipulation in companies listed in Athens stock exchange market," *J. Financial Crime*, vol. 29, no. 2, pp. 603–619, Mar. 2022.

[28] Y. Gong, J. Li, Z. Xu, and G. Li, "Detecting financial fraud using two types of Benford factors: Evidence from China," *Proc. Comput. Sci.*, vol. 214, pp. 656–663, Jan. 2022, doi: 10.1016/j.procs.2022.11.225.

[29] P. Kagias, A. Cheliatsidou, A. Garefalakis, J. Azibi, and N. Sariannidis, "The fraud triangle – an alternative approach," *J. Financial Crime*, vol. 29, no. 3, pp. 908–924, May 2022, doi: 10.1108/jfc-07-2021-0159.

[30] T. Tarjo, H. V. Vidyantha, A. Anggono, R. Yuliana, and S. Musyarofah, "The effect of enterprise risk management on prevention and detection fraud in Indonesia's local government," *Cogent Econ. Finance*, vol. 10, no. 1, Dec. 2022, Art. no. 2101222, doi: 10.1080/23322039.2022.2101222.

[31] B. Stojanović and J. Božić, "Robust financial fraud alerting system based in the cloud environment," *Sensors*, vol. 22, no. 23, p. 9461, Dec. 2022, doi: 10.3390/s22239461.

[32] Y. Yao and J. Li, "Operational risk assessment of third-party payment platforms: A case study of China," *Financial Innov.*, vol. 8, no. 1, p. 19, Dec. 2022, doi: 10.1186/s40854-022-00332-x.

[33] J. S. Kamdem and D. Selambi, "Cyber-risk forecasting using machine learning models and generalized extreme value distributions," *Hal Sci.*, vol. 1, pp. 1–23, Jan. 2022.

[34] N. I. Mat Ridzuan, J. Said, F. M. Razali, D. I. Abdul Manan, and N. Sulaiman, "Examining the role of personality traits, digital technology skills and competency on the effectiveness of fraud risk assessment among external auditors," *J. Risk Financial Manage.*, vol. 15, no. 11, p. 536, Nov. 2022, doi: 10.3390/jrfm15110536.

[35] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "Application of forensic accounting techniques in the south African banking industry for the purpose of fraud risk mitigation," *Cogent Econ. Finance*, vol. 11, no. 1, Dec. 2023, Art. no. 2153412, doi: 10.1080/23322039.2022.2153412.

[36] H. Wang, W. Wang, Y. Liu, and B. Alidaee, "Integrating machine learning algorithms with quantum annealing solvers for online fraud detection," *IEEE Access*, vol. 10, pp. 75908–75917, 2022.

[37] N. Innan, A. Sawaika, A. Dhor, S. Dutta, S. Thota, H. Gokal, N. Patel, M. A.-Z. Khan, I. Theodonis, and M. Bennai, "Financial fraud detection using quantum graph neural networks," *Quantum Mach. Intell.*, vol. 6, no. 1, pp. 1–18, Jun. 2024.

[38] A. Alwadain, R. F. Ali, and A. Muneer, "Estimating financial fraud through transaction-level features and machine learning," *Mathematics*, vol. 11, no. 5, p. 1184, Feb. 2023.

[39] L. Ren, R. Hu, D. Li, Y. Liu, J. Wu, Y. Zang, and W. Hu, "Dynamic graph neural network-based fraud detectors against collaborative fraudsters," *Knowl.-Based Syst.*, vol. 278, Oct. 2023, Art. no. 110888.

[40] V. Chang, L. M. T. Doan, A. Di Stefano, Z. Sun, and G. Fortino, "Digital payment fraud detection methods in digital ages and industry 4.0," *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 107734, doi: 10.1016/j.compeleceng.2022.107734.

[41] J. Chung and K. Lee, "Credit card fraud detection: An improved strategy for high recall using KNN, LDA, and linear regression," *Sensors*, vol. 23, no. 18, p. 7788, Sep. 2023, doi: 10.3390/s23187788.

[42] V. S. S. Karthik, A. Mishra, and U. S. Reddy, "Credit card fraud detection by modelling behaviour pattern using hybrid ensemble model," *Arabian J. Sci. Eng.*, vol. 47, no. 2, pp. 1987–1997, Feb. 2022, doi: 10.1007/s13369-021-06147-9.

[43] H. Ahmad, B. Kasasbeh, B. Aldabaybah, and E. Rawashdeh, "Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS)," *Int. J. Inf. Technol.*, vol. 15, no. 1, pp. 325–333, Jan. 2023, doi: 10.1007/s41870-022-00987-w.

[44] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access*, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[45] J. Jiang, F. Liu, Y. Liu, Q. Tang, B. Wang, G. Zhong, and W. Wang, "A dynamic ensemble algorithm for anomaly detection in IoT imbalanced data streams," *Comput. Commun.*, vol. 194, pp. 250–257, Oct. 2022, doi: 10.1016/j.comcom.2022.07.034.

[46] D. Sisodia and D. S. Sisodia, "Data sampling strategies for click fraud detection using imbalanced user click data of online advertising: An empirical review," *IETE Tech. Rev.*, vol. 39, no. 4, pp. 789–798, Jul. 2022, doi: 10.1080/02564602.2021.1915892.

[47] A. Singh, R. K. Ranjan, and A. Tiwari, "Credit card fraud detection under extreme imbalanced data: A comparative study of data-level algorithms," *J. Exp. Theor. Artif. Intell.*, vol. 34, no. 4, pp. 571–598, Jul. 2022, doi: 10.1080/0952813x.2021.1907795.

[48] A. J. McNeil, R. Frey, and P. Embrechts, "Quantitative risk management: Concepts, techniques and tools, Revised edition," in *Princeton Series in Finance*. Princeton, NJ, USA: Princeton Univ. Press, 2015.

[49] D. Gorton, "Modeling fraud prevention of online services using incident response trees and value at risk," in *Proc. 10th Int. Conf. Availability, Rel. Secur.*, Toulouse, France, Aug. 2015, pp. 149–158, doi: 10.1109/ARES.2015.17.

[50] Y. Lyu, F. Qin, R. Ke, Y. Wei, and M. Kong, "Does mixed frequency variables help to forecast value at risk in the crude oil market?" *Resour. Policy*, vol. 88, Jan. 2024, Art. no. 104426, doi: 10.1016/j.resourpol.2023.104426.

[51] S. B. Abdullahi and K. Chamnongthai, "IDF-sign: Addressing inconsistent depth features for dynamic sign word recognition," *IEEE Access*, vol. 11, pp. 88511–88526, 2023.

[52] A. Mahajan, V. S. Baghel, and R. Jayaraman, "Credit card fraud detection using logistic regression with imbalanced dataset," in *Proc. 10th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2023, pp. 339–342.

[53] F. Aslam, A. I. Hunjra, Z. Ftiti, W. Louhichi, and T. Shams, "Insurance fraud detection: Evidence from artificial intelligence and machine learning," *Res. Int. Bus. Finance*, vol. 62, Dec. 2022, Art. no. 101744, doi: 10.1016/j.ribaf.2022.101744.

[54] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *J. Big Data*, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.
[55] P. Atchaya and K. Somasundaram, "Novel logistic regression over Naive Bayes improves accuracy in credit card fraud detection," *J. Surv. Fisheries Sci.*, vol. 10, no. 1S, pp. 2172–2181, 2023.
[56] R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," *Hum.-Centric Intell. Syst.*, vol. 2, nos. 1–2, pp. 55–68, Jun. 2022, doi: 10.1007/s44230-022-00004-0.
[57] A. Kannagi, J. Gori Mohammed, S. Sabari Giri Murugan, and M. Varsha, "Intelligent mechanical systems and its applications on online fraud detection analysis using pattern recognition K-nearest neighbor algorithm for cloud security applications," *Mater. Today: Proc.*, vol. 81, pp. 745–749, 2023, doi: 10.1016/j.matpr.2021.04.228.
[58] P. H. Kupiec, "Techniques for verifying the accuracy of risk measurement models," in *Division of Research and Statistics, Division of Monetary Affairs, Federal Reserve Board*, vol. 95. USA: Journal of Derivatives, 1995.
[59] K. Kireev, M. Andriushchenko, C. Troncoso, and N. Flammarion, "Transferable adversarial robustness for categorical data via universal robust embeddings," 2023, *arXiv:2306.04064*.

ABDULLAHI UBALE USMAN received the B.Sc. degree in statistics from Kano University of Science and Technology, Wudil, Nigeria, in 2012, and the M.Sc. degree in statistics from Jodhpur National University, India, in 2016. He is currently pursuing the Ph.D. degree with the School of Statistics and Mathematics, Zhejiang Gongshang University, Hangzhou, China. His current research interests include financial fraud detection and machine learning.

SUNUSI BALA ABDULLAHI (Member, IEEE) received the B.Sc. and M.Sc. degrees in electronics from Bayero University Kano (BUK), Nigeria, and the Ph.D. degree in electrical and computer engineering from the King Mongkut's University of Technology Thonburi, Thailand. His research interests include computer vision, artificial intelligence, digital image processing, nonlinear optimization and their applications in human motion analysis, multimodal data interaction analysis, and social signal processing.

YU LIPING received the Ph.D. degree. He is currently a Professor with Zhejiang Gongshang University. He mainly involved in scientific and technological evaluation, technological innovation, and information management. He has six monographs. He is the first author for more than 170 articles. He has authored three articles in SCI and SSCI, 40 articles in first-class journals and 140 articles in CSSCI. The academic achievements were collected by Xinhua digest and seven copies of the NPC. An article was selected as Leader 5000-Top Academic Articles Platform for China's Top Sci-Tech Journals (F5000).

BAYAN ALGHOFAILY received the master's and Ph.D. degrees in computer science from Toronto Metropolitan University, Toronto, Canada. During that period, she was a member of the Distributed Applications and Broadband Networks Laboratory (DABNEL). She focused on studying how the performance of machine learning models is affected by dataset features. She is currently an Assistant Professor with the Department of Information System, CCIS, Prince Sultan University (PSU). She is also a member of the Artificial Intelligence and Data Analytics (AIDA) Laboratory, CCIS, PSU. Her research interests include AI, NLP, ML, and neural networks. She continues to explore this further in her research.

AHMED S. ALMASOUD received the degree from the University of Technology Sydney. He has been with Prince Sultan University (PSU), Riyadh, Saudi Arabia, since 2014, where he is currently an Assistant Professor with the College of Computer and Information Sciences. He has published original articles in the finest journals in the area of his studies. His research interests include (but not limited to) artificial intelligence, machine learning, security architecture, and the Internet of Things.

AMJAD REHMAN (Senior Member, IEEE) received the Ph.D. degree from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia, specializing in information security using image processing techniques, in 2010. He is currently an Associate Professor with CCIS, Prince Sultan University, Riyadh, Saudi Arabia. He is also a PI in several projects and completed projects funded by MoHE Malaysia, Saudi Arabia. His research interests include bioinformatics, the IoT, information security, and pattern recognition. He received a Rector Award for the 2010 Best Student from UTM Malaysia.