Bayesian Network Modelling of Detecting Bank Fraudulent Transaction in Nigeria

Abstract

Bank fraud is an increasingly prevalent issue, causing substantial financial losses for both financial institutions and customers. Also, with the increasing prevalence of bank fraud, especially facilitated by online banking and digital payments, there is a pressing need for advanced fraud detection techniques. This study specified the Bayesian Network models for detecting fraudulent bank transactions. Bayesian Networks offer a probabilistic graphical modeling approach that can effectively capture complex relationships and dependencies within financial data. Thus, the research aimed at developing a custom Bayesian network model trained on a large dataset of bank transactions comprising over one million bank transactions to classify instances as fraudulent or non-fraudulent. Down-sampling was employed to reduce the dataset from its initial size of 1 million observations to 17,650 observations, ensuring a balanced representation of both fraud and non-fraud instances. Various estimation techniques: Maximum Likelihood, Bayesian Estimation, and Expectation Maximization were employed and evaluated to learn the model parameters. The model's performance was measured using metrics: accuracy, precision, recall, F1-score, and ROC-AUC. The Bayesian Estimator achieved an overall Accuracy of 66.18%, Precision of 67.73%, F1-score of 64.06%, ROC-AUC of 66.13%, Recall of 60.77%, Sensitivity of 60.77% and Specificity of 71.50%. Also, the Maximum Likelihood achieved an overall Accuracy of 66.77%, Precision of 69.22%, F1-score of 63.96%, ROC-AUC of 66.71%, Recall of 59.45%, Sensitivity of 59.45% and Specificity of 73.97%. Likewise, the Expectation Maximization achieved an overall Accuracy of 66.83%, Precision of 69.31%, F1-score of 64.00%, ROC-AUC of 66.77%, Recall of 59.45%, Sensitivity of 59.45% and Specificity of 74.09%. On the confusion matrix, the model correctly classified 1272 instances as Non-Fraudulent transactions (True Negative). Also, it was observed that the model incorrectly classified 507 instances as fraudulent transactions when they were Non-Fraudulent (False Positive). The model similarly incorrectly classified 687 instances as Non-Fraudulent transactions when they were Fraudulent (False Negative). Finally, it correctly classified 1064 instances as fraudulent transactions (True Positive). These results demonstrated the Bayesian Network's ability to identify fraudulent transactions while minimizing false alarms accurately. The findings highlight the potential of Bayesian Networks as a robust framework for fraud detection in the banking sector, contributing to enhanced security and reduced financial losses. The developed model can be introduced into existing banking systems to strengthen fraud prevention strategies.

Keywords: Probabilistic graphical modelling, Maximum likelihood estimation, Down-sampling, Fraudulent transaction, Confusion matrix

UNDER PEER REVIEW

1 Introduction

Fraud is an intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim. Types of fraud include tax fraud, credit card fraud, wire

fraud, securities fraud, and bankruptcy fraud. Fraudulent activity can be carried out by one individual, multiple individuals, or a business firm. In recent years, there has been a significant increase in the volume of financial transactions (Akanbi O. B. et al, 2018)due to the expansion of financial institutions and the popularity of web-based e-commerce (Yaya O. S. et al, 2019). Fraudulent transactions have become a growing problem in online banking and fraud detection has always been challenging However, technology can be a tool to combat fraud. To prevent further possible fraud, it is important to detect the fraud immediately after its occurrence. Fraud can be defined as wrongful or criminal deception intended to result in financial or personal gain. There are two mechanisms, fraud prevention and fraud detection, that can be exploited to avoid fraud-related losses. Fraud prevention is a proactive method that stops fraud from happening in the first place. On the other hand, fraud detection is needed when a fraudster attempts a fraudulent transaction. Fraud detection in banking is considered a binary classification problem in which data is classified as legitimate or fraudulent. This is because banking data is large in volume and with datasets containing a large amount of transaction data.

Bank fraudulent transactions have been changing; financial institutions are required by federal law to send customers notice if their accounts show potential fraud or activity that looks suspiciously similar. This is known as the Expedited Funds Availability Act (EFAA). The EFAA was enacted because of common occurrences such as when banks would hold consumer deposits for days before they were posted and made available. However, due to technological advancement and changes in banking regulations over the last few decades, fraudulent activities have become increasingly sophisticated like cybercrime perpetrated mainly through debit cards issued without customer consent (Yablon, 2020; Sajjad et al, 2023; Jiang et al, 2022; Mukhanov Lev, 2008). Therefore, it has become more important than ever for banks and other financial institutions to remain vigilant against any suspicious behavior from both external parties and internally motivated bad actors alike; otherwise, they may find themselves liable for costly penalties related to not complying with existing laws which make them responsible for compensating victims whose funds had been inappropriately accessed due to unforeseen security vulnerably or human negligence.

The prevalence of bank fraud has increased in recent years due to the rise of online banking (Muhammad et al, 2022; Mytnyk et al, 2023; Weiging Wan et al, 2020) and digital payment

technologies (Taneja, 2019). Banks are becoming increasingly vulnerable to fraudulent transactions as a result of these changes, which can occur through means such as phishing attacks or account takeovers (Hoang et al, 2023). To prevent this type of crime, banks must implement stronger security measures such as two-factor authentication and advanced anti-fraud tools that monitor customer activity for suspicious behavior (Khor and Omar, 2018). Additionally, banks should provide education on financial literacy (Akanbi O. B., 2023) and cyber safety practices so customers understand how to recognize signs of potential fraud attempts. Furthermore, governments may create new legislation or regulations centered on consumer protection against bank fraud by instituting requirements like minimum password length (Singh et al., 2020). Implementation of these policies will help reduce the rate at which fraudulent transactions occur and lessen their impact when they do.

Bayesian network models are probabilistic graphical models that have been used for a variety of tasks such as forecasting (Olubusoye and Akanbi, 2015; Akanbi and Fawole, 2024), feature selection, and data analytics (Akanbi O. B., 2023). The Bayesian Network model is composed of nodes that represent random variables, and directed edges between the related nodes which indicate their conditional dependence structure and probabilities associated with each node. Each node has a set of values (parents or children) achievable in different contexts when dealing with real-world problems; these context-specific states carry information to update prior beliefs about future steps assumed from past observations or experiences. A Bayesian network model depicts interrelationships in the form of conditional distributions for a collection of random variables. The model is described as a directed acyclic graph in which the nodes are random variables and the directed arcs spell out the structure of the conditional distribution. Bayesian Networks (BNs) represent systems as a network of interactions between variables from primary cause to outcome, with all cause-effect assumptions made explicit. BNs are often considered suitable for modelling environmental systems(Akanbi and Oladoja, 2019) due to their ability to integrate multiple issues, interactions, and outcomes and investigate tradeoffs (Afriyie et al, 2023; Elsevier, 2022; Zhang et al, 2020; Aakriti et al, 2022; Sanchez Aguayo et al, 2021). Furthermore, they are apt for utilizing data and knowledge from different sources and handling missing data. BNs readily incorporate and explicitly represent uncertain information, which is propagated through and expressed in the model outputs (Akanbi O. B. et al, 2018; Olubusoye and Akanbi, 2015). BNs are based on a relatively simple causal graphical structure, meaning

they can be built without highly technical modelling skills and be understood by non-technical users and stakeholders (Voinov and Bousquet, 2010).

The main advantage of the Bayesian Network lies in its ability to quantify uncertain knowledge by encoding the probability distributions over random variables to infer unknown relationships accurately through statistical inference algorithms while allowing them to be robust enough even after introducing new sets of data into consideration. Bayesian networks prove popular because they not only provide numerical answers but also rely on qualitative analysis derived from experts' opinions concerning critical domains where uncertainty rises. Their stability towards noises ensures reliable outputs without needing lots of resources necessary diets will predict quantitative results via exhaustive search due to their sound mathematical basis established on graph theory making it so powerful, especially when incorporated within advanced planning systems being able often to anticipate potential emergent phenomena effectively acting proactively under many circumstances overshadowing other existing well-known heuristics reliant paradigms (Milad et al, 2023). Bayesian networks are nowadays well established as a modeling tool for expert systems in domains with uncertainty (Russell et al, 2003). The reasons are their powerful but conceptually transparent representation of probabilistic models in terms of a network (Kitson et al 2023). Their graphical representation, showing the conditional independencies between variables, is easy to understand for humans.

Bank fraud is a severe offense with potentially disastrous repercussions for both victims and financial organizations. Bank fraud has become much more common in recent years, and crooks are employing new and increasingly sophisticated techniques. The objective of this study is to assess the feasibility of probabilistic graphical models for enhanced fraud detection and prevention in the finance industry by building and evaluating a custom Bayesian network model to detect bank fraud (Yaya O. S. et al, 2019). The new and sophisticated techniques that fraudsters employ are sometimes too complex for the fraud detection technologies that are currently in place. This indicates that new and improved fraud detection technologies are also required. Thus, this study aimed at developing a Bayesian Network Model for detecting bank's fraudulent transactions.

2. Methodology

This section provides an overview of the approach and techniques taken to meet the goals of this study. It outlines the process for developing classification models and evaluating them. Eighty percent of the data was set aside for training, while the remaining twenty percent was considered for testing.

2.1 Data Pre-processing

Min max Scaling

Min-max scaling is a common preprocessing and normalization technique for data. Scaling characteristics to a defined range, usually between 0 and 1, is how it transforms them. For Min-Max scaling, the formula is:

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Where:

- X is the original feature value.
- X_{min} is the minimum value of the feature in the dataset.
- X_{max} is the maximum value of the feature in the dataset.
- X_{scaled} is the scaled value of the feature after normalization.

Near Miss (Down-sampling)

Down-sampling is a technique for dealing with imbalanced classification problems in which one class is significantly more prevalent than the others. To balance the class distribution, it explicitly uses a down-sampling method, which lowers the number of instances in the majority class (the over-represented class). Using a distance measure, the Near Miss method chooses examples from the majority class that are "near" the instances in the minority class. Instances belonging to the majority class that are near the class decision boundary are to be kept.

Principal Component Analysis (PCA)

This technique reduces the size of the original set of variables in the large data sets while retaining more of its information. One way to formulate PCA involves finding the eigenvectors of the covariance matrix (Σ) of the data:

$$\Sigma * v = \lambda * v \quad (2)$$

Where:

- Σ is the covariance matrix, which captures the linear relationships between the original variables.
- v is an eigenvector representing a principal component direction.

UNDER PEER REVIEW

- λ is the corresponding eigenvalue, indicating the variance explained by that principal component.

Hill Climb

Hill climbing is a mathematical optimization method used in numerical analysis that is a member of the local search family. It is an iterative method that begins with a haphazard solution to a problem and then makes little adjustments to the solution to find a better one. If the modification results in a superior answer, the new solution is modified incrementally once again, and so on, until no more advancements are possible.

K2 Score

G. F. Cooper and E. Herskovits introduced the score-based K2 algorithm in 1992. The K2 score is a scoring function used in Bayesian network structure learning. It is often referred to as the K2 metric or the K2 heuristic. It represents a substitute for the Minimum Description Length (MDL) and Bayesian Information Criterion (BIC) scoring systems. A network structure's quality can be assessed using the K2 score about a dataset and prior information. It enables one to discover the most likely belief network structure or the topology of a Bayesian network.

2.2 Bayesian Network Model

Bayesian networks, which are probabilistic graphical models that use a Directed Acyclic Graph (DAG) to represent a set of variables and their conditional dependencies, are sometimes referred to as belief networks or causal networks. While the network's parameters measure the strength of the relationships between the variables, the graph's structure embodies the conditional independence assumptions among the variables. The conditional independence presumptions inherent in the graph structure and the chain rule of probability serve as the foundation for the formula for a Bayesian network. It is possible to factor the joint probability distribution of all the network's variables in the following way:

$$P(X_1, X_2, \dots, X_n) = \prod_{i=1}^{n} P\left(X_i \middle| Pa(X_i)\right) \qquad (3)$$

Where:

- X_1, X_2, ..., X_n are the random variables in the network.
- Pa(X_i) represents the parent nodes of the variable X_i in the network.
- $P\left(X_i \middle| Pa(X_i)\right)$ is the conditional probability distribution of X_i given its parent nodes.

UNDER PEER REVIEW

2.3 Bayesian Estimation

A statistical method called Bayesian estimation is used to estimate unknown parameters in a model by combining observed data and past information about the parameters. Bayesian estimation yields a posterior distribution for the parameters, which reflects the updated belief about the parameters following observation of the data, in contrast to maximum likelihood estimation (MLE), which aims to obtain a point estimate of the parameters.

The Bayes theorem is the basic formula in Bayesian estimation:

$$P(\theta \mid y) = \frac{P(y \mid \theta) * P(\theta)}{P(y)} \qquad (4)$$

Where:

- $P(\theta \mid y)$ is the posterior probability of "fraud parameter" (θ) given evidence (y)
- $P(y \mid \theta)$is the likelihood function of observing evidence (y) given "fraud parameter" (θ)
- $P(\theta)$is the prior probability of the parameter "fraud parameter" (θ)

$P(y)$ is the marginal likelihood representing the probability of observing evidence (y)

2.4 Maximum Likelihood Estimation

These are the parameter values that maximize the likelihood functionwhich expresses the likelihoodprovided data under the presumptive statistical modelis the fundamental notion behind multiple linear estimation. The likelihood function $L(\theta|X)$, where θ denotes the model's parameters and X the observed data, can be found by multiplying the probability density function (PDF)or probability mass function (PMF) that is assessed at each data point:

$$L(\theta|X) = \prod_{i=1}^{n} f(X_i|\theta) \qquad (5)$$

Where:

- L $(\theta|X)$ is the likelihood function, representing the probability of observing the data given the parameter values θ.
- θ is a vector of parameters that define the statistical model.
- X is the observed data.
- $f(X_i|\theta)$ is the PDF or PMF of the model evaluated at the ith data point.

The values of θ that maximize this likelihood function are the ones that MLE looks for. The likelihood function's natural logarithm, or log-likelihood function $L(\theta|X)$, is frequently simpler to work with in practice:

UNDER PEER REVIEW

$$L(\theta|X) = \log(\theta|X) = \sum_{i=1}^{n} \log f(X_i|\theta) \quad (6)$$

Since the natural logarithm is a monotonic function, maximizing the log-likelihood function is equalto maximizing the likelihood function.The value of θ that maximizes the likelihood function is the formula for the maximum likelihood estimator $\hat{\theta}$:

$$\hat{\theta}_{MLE} = \text{argmax}\_\theta L(\theta; x) \quad (7)$$

Where:

- $\hat{\theta}$_MLE is the maximum likelihood estimate of the parameter θ
- L(θ; x) is the likelihood function, which is the joint probability density/mass function of the data x, considered as a function of the parameter θ
- argmax_θ means "the value of θ that maximizes the expression that follows"

2.5 Expectation Maximization

The maximum likelihood estimates of parameters are found iteratively using the Expectation-Maximization (EM) process. The Expectation (E) step and the Maximization (M) step are the two steps that the algorithm alternates between for the EM process. The E-step calculates the posterior probability $P(Z|X, \theta^{(t)})$for each data point X, where Z denotes the latent variables, and $\theta^{(t)}$,represents the current estimate of the parameters at iteration t.By maximizing the expected log-likelihood, the M-step updates the parameter estimates θmathematically is:

$$\theta^{(t+1)} = \text{argmax}_\theta \, E_{Z,X,\theta^{(t)}}[\log P(X, Z, |\theta)] \quad (8)$$

Where; $E_{Z,X,\theta^{(t)}}[\cdot]$with respect to the observed data and the current parameter estimations, $[\cdot]$ represents the expectation operator over the posterior distribution of the latent variables.When the parameter estimations no longer significantly vary across iterations, the EM method converges. Iterations between the E-step and the M-step occur subsequently.

UNDER PEER REVIEW

3. Results and Discussion

This section focused on the data analysis, results, and discussion of the study. The data used contained bank transactions highlighting both, fraudulent and non – fraudulent transactions. The data consists of 1 million cases and 32 features/variables. The description of the features in the dataset in this study is presented in Table 1

Table 1: Variables used for Modelling

S/N	Features	Meaning	Instances
1	income (numeric)	Annual income of the applicant (in decile form)	Ranges between [0.1, 0.9].
2	name_email_similarity (numeric)	Metric of similarity between email and applicant's name. Higher values represent higher similarity.	Ranges between [0, 1].
3	prev_address_months_count	Number of months in previous registered address of the applicant, i.e. the applicant's previous residence, if applicable.	Ranges between [−1, 380] months (-1 is a missing value).
4	current_address_months_count (numeric)	Months in currently registered address of the applicant.	Ranges between [−1, 429] months (-1 is a missing value).
5	customer_age (numeric)	Applicant's age in years, rounded to the decade.	Ranges between [10, 90] years.
6	days_since_request (numeric)	Number of days passed since transaction was done.	Ranges between [0, 79] days.
7	intended_balcon_amount (numeric)	Initial transferred amount for transaction.	Ranges between [−16, 114] (negatives are missing values).
8	payment_type (categorical)	Credit payment plan type.	5 possible (annonymized) values.
9	zip_count_4w (numeric)	Number of transactions within same zip code in last 4 weeks.	Ranges between [1, 6830]
10	velocity_6h (numeric)	Velocity of total transactions made in last 6 hours i.e., average number of transactions per hour in the last 6 hours.	Ranges between [−175, 16818]
11	velocity_24h (numeric)	Velocity of total transactions made in last 24 hours i.e., average number of transactions per hour in the last 24 hours.	Ranges between [1297, 9586]
12	velocity_4w (numeric)	Velocity of total transaction made in last 4 weeks, i.e., average number of transactions per hour in the last 4 weeks.	Ranges between [2825, 7020]
13	bank_branch_count_8w (numeric)	Number of total transactions in the selected bank branch in last 8 weeks.	Ranges between [0, 2404]
14	date_of_birth_distinct_emails_4w (numeric)	Number of emails for applicants with same date of birth in last 4 weeks.	Ranges between [0, 39]
15	employment_status (categorical)	Employment status of the applicant.	7 possible (annonymized) values.
16	credit_risk_score (numeric)	Internal score of transaction risk. Ranges between [−191, 389]	Ranges between [−191, 389]
17	email_is_free (binary)	Domain of transaction email (either free or paid)	email_is_free (binary): Domain of transaction email (either free or paid)

UNDER PEER REVIEW

18	housing_status (categorical)	Current residential status for applicant.	7 possible (anonymized) values.
19	phone_home_valid (binary)	Validity of provided home phone.	Validity of provided home phone.
20	phone_mobile_valid (binary)	Validity of provided mobile phone.	Validity of provided mobile phone.
21	bank_months_count (numeric)	How old is previous account (if held) in months.	Ranges between [−1, 32] months (-1 is a missing value)
22	has_other_cards (binary)	if applicant has other cards from the same banking company.	If applicant has other cards from the same banking company.
23	proposed_credit_limit (numeric)	Applicant's proposed credit limit.	Ranges between [200, 2000]
24	foreign_request (binary)	If origin country of request is different from bank's country.	If origin country of request is different from bank's country.
25	source (categorical)	Online source of transaction.	Either browser (INTERNET) or app (TELEAPP)
26	session_length_in_minutes (numeric)	Length of user session in banking website in minutes.	Ranges between [−1, 107] minutes (-1 is a missing value)
27	device_os (categorical)	Operative system of device that made request.	Possible values are: Windows, macOS, Linux, X11, or other.
28	keep_alive_session (binary)	User option on session logout.	User option on session logout.
29	device_distinct_emails (numeric)	Number of distinct emails in banking website from the used device in last 8 weeks.	Ranges between [−1, 2] emails (-1 is a missing value)
30	device_fraud_count (numeric)	Number of fraudulent transactions with used device.	Ranges between [0, 1]
31	month (numeric)	Month where the transaction was made.	Ranges between [0, 7]
32	fraud_Cases (binary)	If the transaction is fraudulent or not.	If the transaction is fraudulent or not.

3.1 Distribution of Fraudulent Transactions

The chart below illustrates that of about 1 million transactions, approximately 98.9% (988,971 transactions) are categorized as non-fraudulent, while about 1.1% (11,029 transactions) are identified as fraudulent. This distribution suggests that the incidence of fraudulent transactions is relatively low compared to non-fraudulent transactions. Figure 1 represents the distribution of Fraudulent Transactions.

UNDER PEER REVIEW

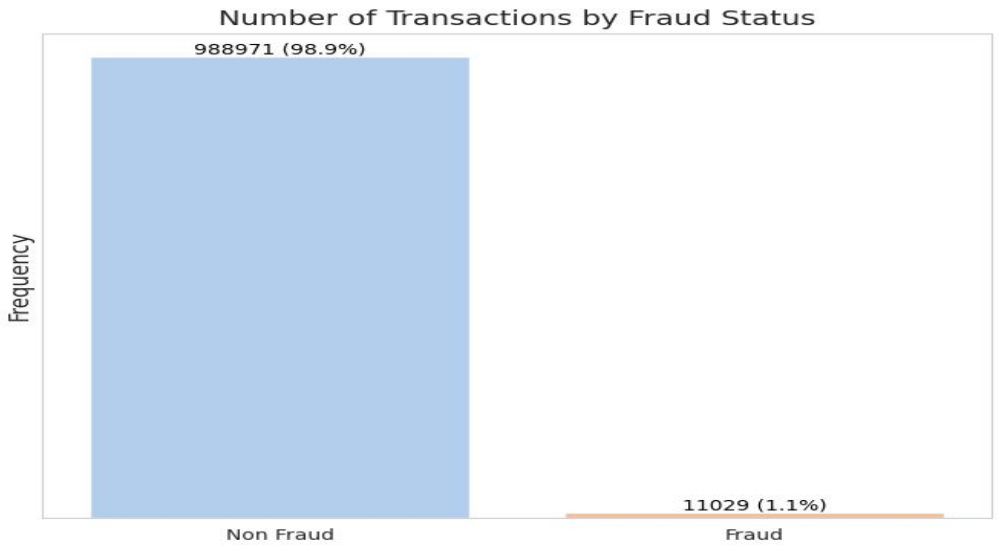

Figure 1: Bar chart of Fraudulent and Non Fraudulent Transactions

3.2 Data Preprocessing

During the preprocessing phase, the numerical variables such as income, name_email_similarity, and customer_age were first standardized using the Min-max Scaler to ensure that features were on the same scale. One-hot encoding was applied to categorical variables to convert them into a binary format suitable for machine learning algorithms. The down-sampling technique was employed since the number of non-fraudulent transactions far exceeds the number of fraudulent transactions. The down-sampling reduced the dataset from its initial size of 1 million observations to 17,650 observations, ensuring a balanced representation of both fraud and non-fraud instances. Subsequently, the down-sampled datasets were splitted into a training set (80%) and a testing set (20%). However, due to the high dimensionality resulting from one-hot encoding, the Principal Component Analysis (PCA) was applied to reduce the number of features from 32 to 7 while retaining the most relevant information. Finally, the Bayesian Network model was fitted using the Maximum Likelihood, Bayesian Estimator, and Expectation Maximization. These choices ensure that the model parameters were estimated in a Bayesian framework, considering prior knowledge and producing more robust results.

UNDER PEER RE

3.3 The Bayesian Network Model Learned Structure

Figure 2 visually represents the learned structure graph of the Bayesian Network model derived from the Transaction dataset. It showed how the Bayesian Network comprehends the intricate relationships and dependencies among variables within the dataset. The model gains insights into how different variables influence each other and can effectively predict outcomes based on this understanding.

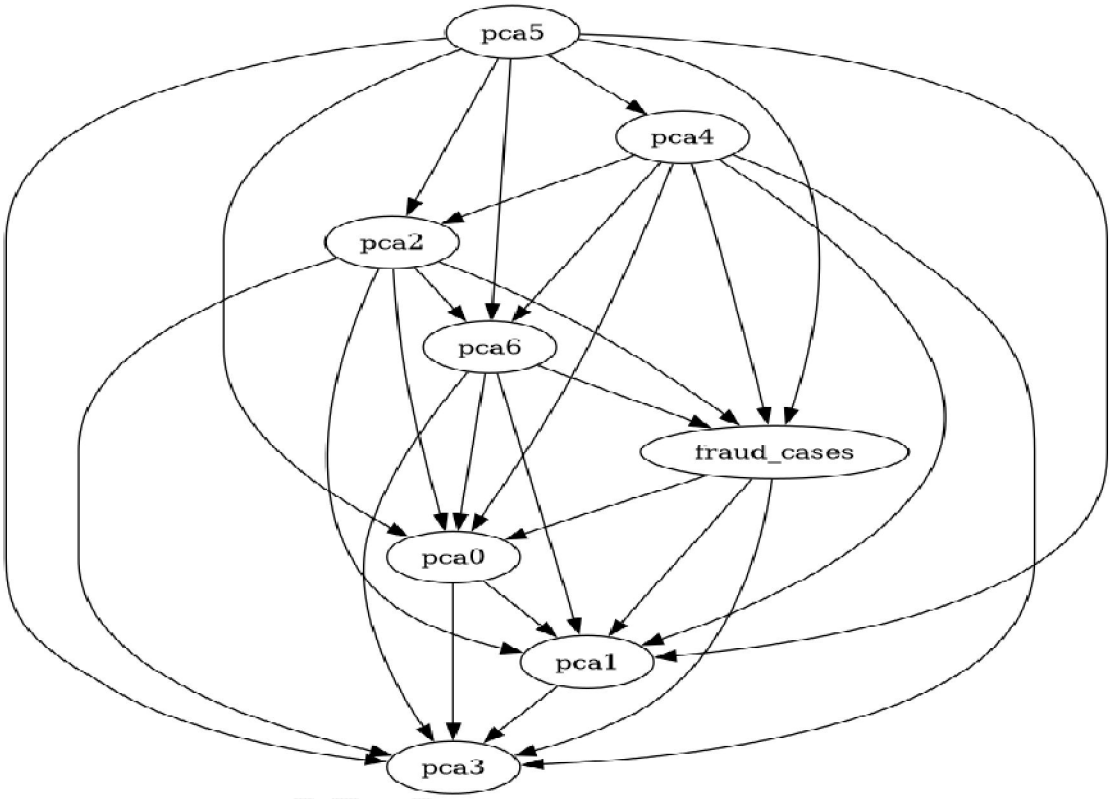

Figure 2: Bayesian Network Model (Probability Graphical Modelling)

3.4 Prior and Posterior Probability

3.4.1 Prior Probability

Figure 3 showed the Prior Probabilities of each variableboth,for fraudulent and non-fraudulent transactionsused for the Bayesian Network model.The PCA_5 and PCA_6 tends to zero.

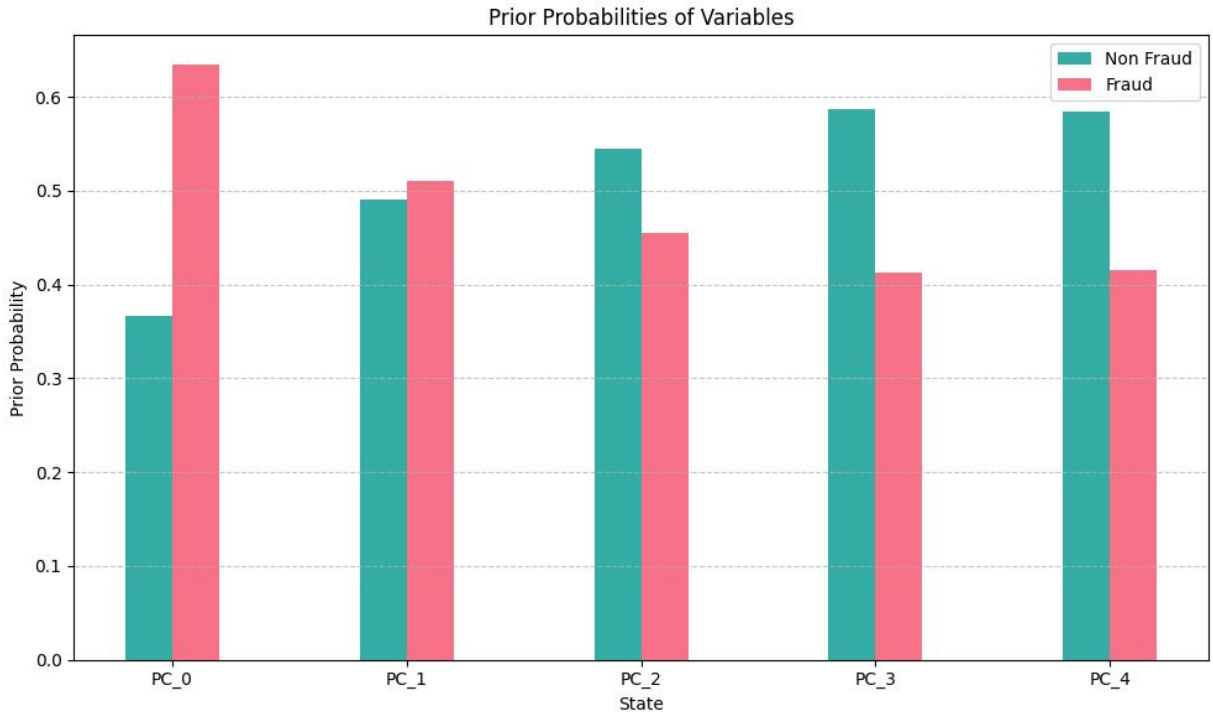

Figure 3: Prior Probabilities for the Transaction

3.4.2 Posterior Probability

Figure 4represented the distribution of posterior probability which showed the Average Posterior Probability of all the transactions (fraudulent and non fraudulent) used in evaluating the model.

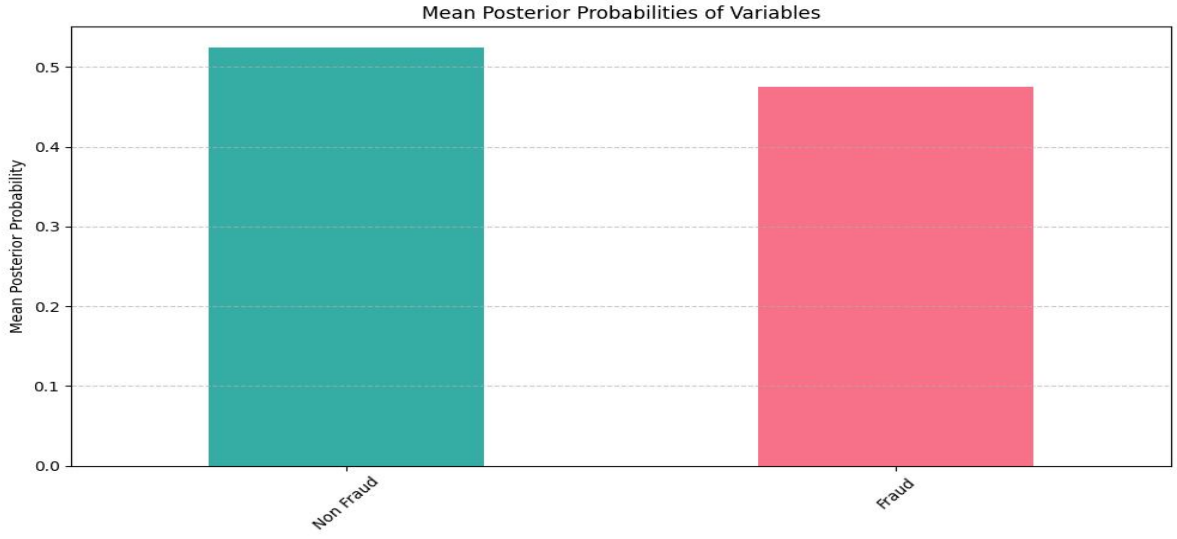

Figure 4: Posterior Probabilities for the Transactions

3.5 Comparison among Bayesian Estimators, Maximum Likelihood and Expectation Maximization

Table 2 and Figure 5 observed that the Bayesian Estimator achieved an accuracy of 0.6618, denoting its ability to correctly classify approximately 66.18% of all transactions (fraudulent and non-fraudulent) in the datasets. Similarly, the Maximum Likelihood and Expectation Maximization approaches achieved slightly higher accuracies of 66.80%. Moreover, the Bayesian Estimator exhibited a precision of 0.6773, indicating that when it predicted a transaction as fraudulent, approximately 67.73% of the time, it was correct. This underscores the model's proficiency in minimizing false positives. Likewise, both Maximum Likelihood and Expectation Maximization approaches yielded comparable precision scores of 69.30%.

Furthermore, the Bayesian Estimator achieved an F1-score of 64.06%, which is a harmonic mean of precision and recall. Higher values of the F1-score indicate better performance in capturing fraudulent transactions while minimizing false alarms. Similarly, the Maximum Likelihood and Expectation Maximization approaches also yielded similar F1 scores of 64.00%. For the recall (sensitivity), the Bayesian Estimator, demonstrated a score of 0.6077%, indicating its ability to correctly identify approximately 60.77% of all actual fraudulent transactions. This metric highlights the model's effectiveness in capturing fraudulent transactions. Similarly, both Maximum Likelihood and Expectation Maximization approaches achieved recall scores of 59.45% and 59.45%, respectively. Regarding specificity, the Bayesian Estimator achieved a score of 0.7150%, denoting its ability to correctly identify approximately 71.50% of all actual non-fraudulent transactions. This metric underscores the model's capability to avoid misclassifying non-fraudulent transactions as fraudulent. Similarly, both Maximum Likelihood and Expectation Maximization approaches achieved specificity scores of 73.97% and 74.09%, respectively.

Table 2: Comparison among Bayesian Estimators, Maximum Likelihood and Expectation Maximization

Estimator	Accuracy	Precision	F1-score	ROC - AUC	Recall	Sensitivity	Specificity
Bayesian Estimator	0.6618	0.6773	0.6406	0.6613	0.6077	0.6077	0.7150
Maximum Likelihood	0.6677	0.6922	0.6396	0.6671	0.5945	0.5945	0.7397
Expectation Maximization	0.6683	0.6931	0.6400	0.6677	0.5945	0.5945	0.7409

UNDER PEER REVIEW

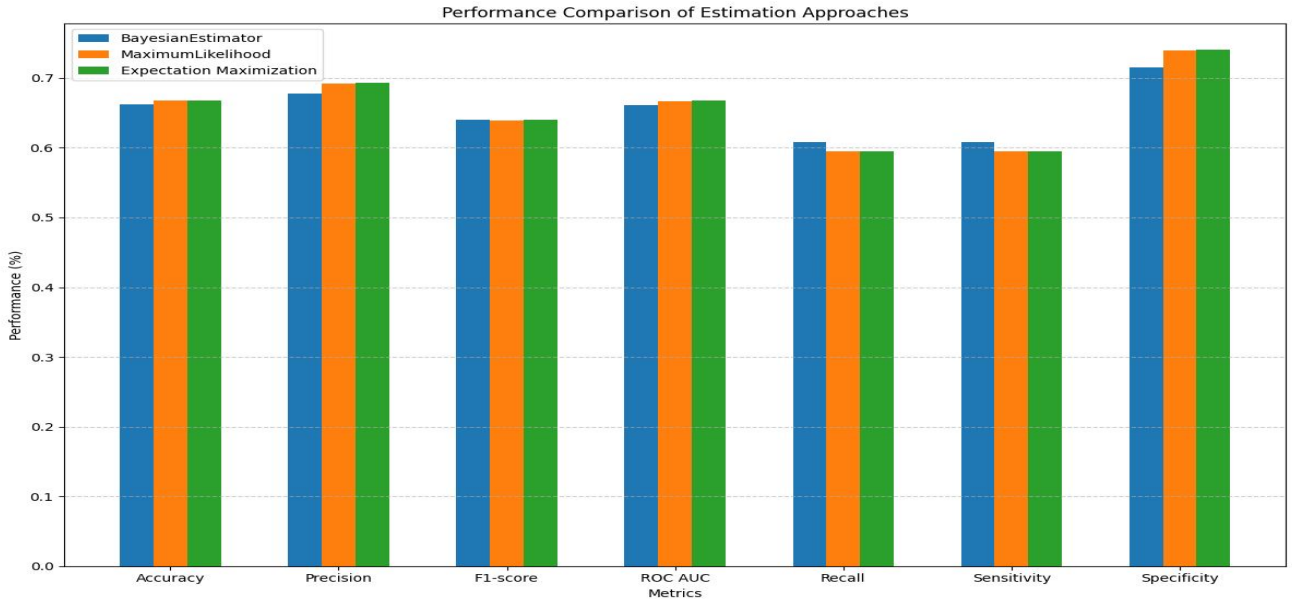

Figure 5: Distribution of Comparison among Bayesian Estimator,Maximum Likelihood Estimation, and Expectation Maximization

Figure 6 which is the ROC-AUC (Receiver Operating Characteristic - Area Under the Curve) showed a value of 0.66 for the Bayesian Estimator indicating that the model has moderate discriminatory power in distinguishing between fraudulent and non-fraudulent transactions across various threshold settings.Specifically, it means that the Bayesian Estimator performs better the than random guessing (0.5).

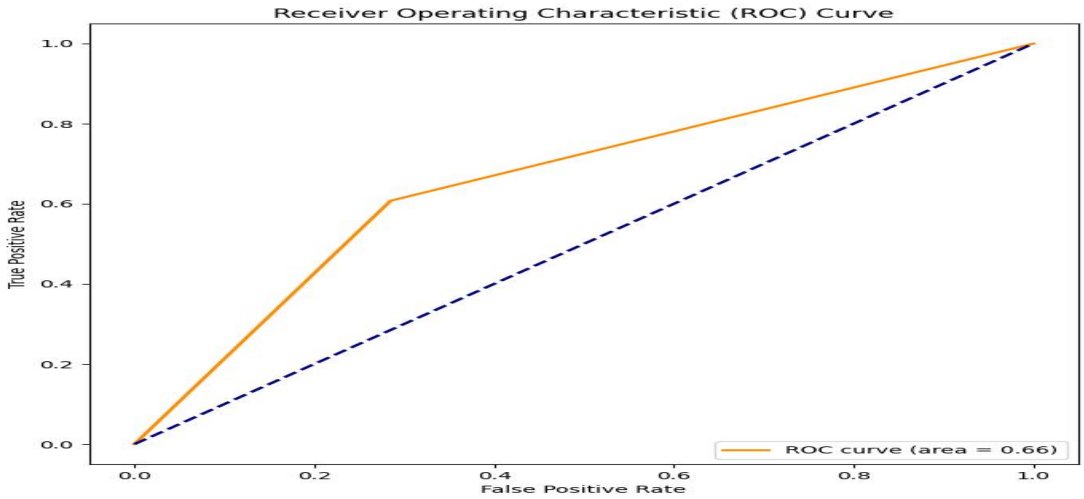

Figure 6: ROC Curve

3.6 Classification Report

Table 3 shows the classification report for the Non-Fraudulent transactions; the model achieved a precision value of 0.65, which indicates that 65% of the instances predicted as non-fraud were non-fraud, and a recall of 0.74, which means that 74% of the actual non-fraud transactions was correctly classified, as non-fraud. Also, the model obtained an F1-score of 69%, and the total non-fraud transactions used for testing were 1779. Also, for the fraudulent transactions, the model achieved a Precision value of 0.69, which indicates that 69% of the transactions predicted as fraud were true fraud. It also obtained an F1-score of 64% with the total transactions in the test dataset for fraudulent transactions of 1751.

Table 3: Classification Report

	Precision	**Recall**	**F1-Score**	**Support**
Non-Fraud	0.65	0.74	0.69	1779
Fraud	0.69	0.59	0.64	1751
Accuracy			0.67	3530
Macro Avg	0.67	0.67	0.67	3530
Weighted Avg	0.67	0.67	0.67	3530

3.7 Confusion Matrix

Figure 7 shows the classification of the confusion matrix for the Bayesian model. The model correctly classified 1272 instances as Non-Fraudulent transactions (True Negative) and also observed that the model incorrectly classified 507 instances as fraudulent transactions when they were non-fraudulent (False Positive). The model also incorrectly classified 687 instances as non-fraudulent transactions when they were fraudulent (False Negative). Finally, it correctly classified 1064 instances as fraudulent transactions (True Positive).

UNDER PEER REVIEW

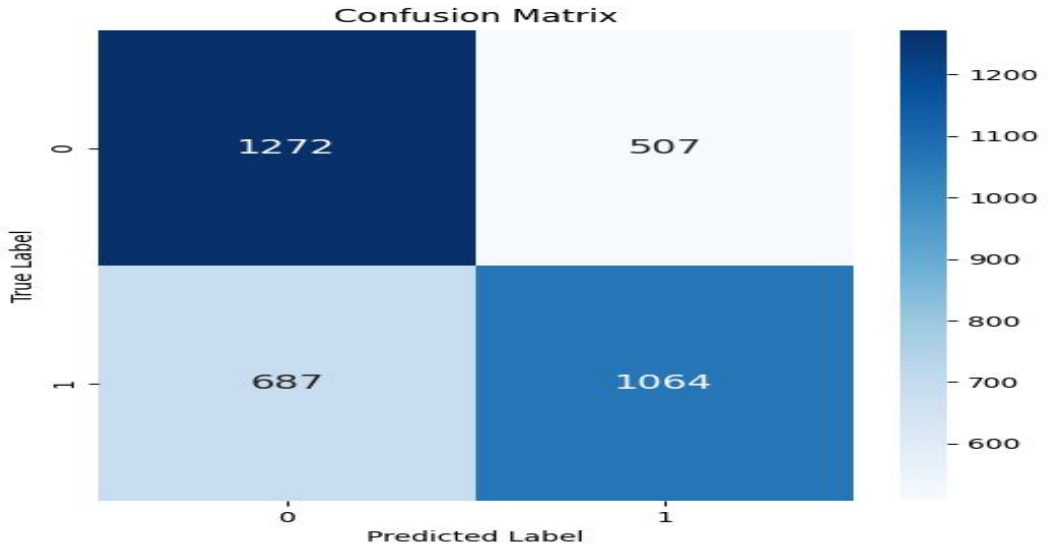

Figure 7: Distribution of Confusion Matrix

4. Conclusion

This study has provided valuable insights into the detection and classification of fraudulent transactions within the dataset. Through comprehensive data exploration, preprocessing, and Bayesian Network modeling, it has gained a deeper understanding of the underlying patterns and relationships among key variables. The Bayesian Network model was trained using various estimation methods including Maximum Likelihood Estimation, Bayesian Estimator, and Expectation Maximization, which exhibited promising results in accurately classifying transactions and minimizing false alarms. Performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC indicated the model's effectiveness in distinguishing between fraudulent and non-fraudulent instances. The Bayesian Network model demonstrated a precision value of 0.69, signifying that 69% of transactions flagged as fraudulent are indeed fraudulent. Despite a slightly lower F1 score of 64%, the model performs reasonably well in identifying fraudulent instances. With 1751 transactions in the test dataset, its predictions provided valuable insights into fraud detection. Moreover, the classification report and confusion matrix provided detailed insights into the model's strengths and areas for improvement, highlighting its ability to correctly identify both non-fraudulent and fraudulent transactions while also identifying instances of misclassification.

UNDER PEER REVIEW

5. Recommendation

This study recommended integrating the developed fraud detection Bayesian Network Model into the existing banking and financial systems. This integration should reduce disruption to daily operations while maximizing the model's impact on fraud prevention. It encouraged banks and financial institutions to conduct regular assessments of the model's performance and effectiveness in detecting fraudulent activities, which includes monitoring key metrics such as accuracy, precision, recall, and an F1-score and comparing them against predefined benchmarks to gauge the model's efficacy. Moreover, financial institutions should provide comprehensive training and awareness programs for bank employees, including frontline staff, fraud analysts, and senior management, to educate them about the model's capabilities, limitations, and best practices for fraud prevention.

6. References

Aakriti Sharma, Vivek Sharma, and Ashish Verma (2022) "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review ".

Akanbi, Olawale Basheer (2023). Application of Naïve bayes to students performance classification.Asian Journal of Probability and Statistics.106724,Volume 25,Issue 1,pp 35-47.

Akanbi O. B., and Fawole O. A. (2024). Forcasting Stock Prices in Nigeria Using Bayesian Vector Autoregression. Journal of Scientific Research and Reports 30 (10), 197-210

Akanbi O. B., Ojo J. F., and Oluneye M. O. (2018). Modelling GDP in Nigeria using Bayesian Model Averaging. International Journal of Applied Science and Mathematics 5 (3), 22-27

Akanbi O. B., and Oladoja O. M. (2019). Application of a modified g- parameter prior ($g = \frac{1}{n^5}$) in Bayesian model averaging to CO2 emissions in Nigeria. Journal of Mathematical Theory and Modeling. 9(11): 57 – 71.

Elsevier B.V (2022). Credit card fraud detection in the era of disruptive technologies 11.008 1319-1578, https://doi.org/10.1016/j.jksuci.

Hoang, T., Mosheni, R., & Yin, J. (2023). Detecting account takeover fraud with graph neural networks. In Proceedings of the Web Conference (pp. 1523-1531).

Jiang, W., Wang, Y., & Wu, D. (2022). Fraud transaction detection using machine learning in financial credit card services. Journal of Financial Crime, 29(3), (pp. 925-936).

AfriyieJ.K.,Tawiah K., Pels W. A. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions.https://doi.org/10.1016/j.dajour.2023.100163.

UNDER PEER REVIEW

Khor, K. C.and Omar, A. N. (2018). A review of data mining and machine learning techniques in bank fraud detection. In Proceedings of the 4th International Conference on Information Systems Management and Innovation (ICISMI) (pp. 1-8).

Kitson, N. K., Constantinou, A. C., Guo, Z., Liu, Y., & Chobtham, K. (2023). A survey of Bayesian Network structure learning. *Artificial Intelligence Review*, *56*(8), 8721–8814. https://doi.org/10.1007/s10462-022-10351-w

Milad Soltani, Alexios Kythreotis, and Arash Roshanpoor. (2023), "Two decades of financial statement fraud detection literature review; combination of bibliometric analysis and topic modeling approach "(Journal of Financial Crime).

Muhammad Wasim Akhtar, Muhammad Asif, and Muhammad Ali. (2022) "A Systematic Review of Fraud Detection in Online Marketplaces" (Decision Support Systems).

Mukhanov Lev (2008). Using Bayesian Belief Networks for credit card fraud detection. Conference: Proceedings of the 26th IASTED International Conference on Artificial Intelligence and Applications.

Mytnyk, B.; Tkachyk, O.; Shakhovska, N.; Fedushko, S.; Syerov, Y (2023). Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. Big Data Cogn. Comput. 7, 93. https:// doi.org/10.3390/bdcc7020093.

Olubusoye, O. E., and Akanbi. O. B. (2015). On g-Prior Elicitation in Bayesian Model Averaging Approach to Normal Linear Regression Model. Conference Proceedings on Perspectives and Developments in Mathematics,in honour of Prof. S. A. Ilori's 70th Birthday. 147 – 170.

Russell, S., Norvig, P., Canny, J., Malik, J., Edwards, D.: Artificial intelligence: a modern approach. Prentice Hall (2003).

Sajjad Hussain, Muhammad Tariq, Khalid Mehmood, and Muhammad Asif. (2023), "Anti-money laundering and financial fraud detection: A systematic literature review"

Sánchez-Aguayo, M.; Urquiza-Aguiar, L.; Estrada-Jiménez, J. (2021). Fraud Detection Using the Fraud Triangle Theory and Data Mining Techniques. https:// doi.org/10.3390/computers10100121.

Singh, S., Singh, R., & Singh, A. P. (2020). A review on bank fraud detection techniques using data mining and machine learning approaches. International Journal of Engineering and Technology, 8(6), 439-443.

Taneja, H. (2019). A comprehensive study on bank fraud detection techniques. International Journal of Information Management, 48, 1-12.

Voinov, A., & Bousquet, F. (2010). Modelling with stakeholders. Environmental Modelling & Software, 25(12), 1268-1281.

UNDER PEER REVIEW

Weiqing Wan, Qingyan Zeng and Zhicheng Wen (2020) Detecting Bank False Account Based on Naive Bayesian Network. 768 072074.

Yablon, A. (2020). The US Law Banks Use To Invoke Panic About Bank Fraud, Explained. Retrieved from https://www.chegg.com/homework-help/questions-and-answers/case-46-fraud-recipe-ceo-s-banks-hate-free-markets-love-crony-capitalism-william-f-black-t-q30538593

Yaya, O. S., Saka, L., and Akanbi, O. B. (2019). Assessing Market Efficiency And Volatility Of Exchange Rates In South Africa And United Kingdom: Analysis Using Hurst Exponent. *TheJournal of Developing Areas*, 127. https://doi.org/26501891

Zhang, D.F., Bhandari, B. and Black, D. (2020) Credit Card Fraud Detection Using Weighted Support Vector Machine Applied Mathematics, 11, 1275-1291. https://doi.org/10.4236/am.2020.1112087.

UNDER PEER REVIEW