Research Article / Review Article FUPRE JOURNAL 9(3):206-226(2025)

FUPRE Journal

of

Scientific and Industrial Research

ISSN: 2579-1184(Print) ISSN: 2578-1129 (Online)

http://fupre.edu.ng/journal

Development of a Credıt Card Fraud Detectıon System Usıng Artıfıcıal Neutral Network and Support Vector Machıne

DIDIGWU, H. T.[1,*], *AKO, R. E.*[1], *NIEMOGHA, S.*[1], *ASUOBITE, M.*[1]

[1]*Department of Computer Science, Federal University of Petroleum Resources, Effurun, Nigeria*

ARTICLE INFO

Received: 15/08/2025

Accepted: 10/09/2025

Keywords

Artificial Intelligence, Algorithm, Fraud, Machine learning, Detection

ABSTRACT

Credit card fraud has without hesitation an expression of criminal intent and deception. Fraud identification seems to be a complicated problem that requires a significant amount of skill until the emergence of machine learning algorithms were deployed for their classification and detection. However, it is an implementation for both the better of machine learning as well as artificial intelligence, ensuring that perhaps the funds of both the customer seems to be secure and therefore not manipulated. This project therefore proposed the development of an improved credit card fraud detection system using machine learning algorithms. The proposed model deployed a fusion of support vector machine and artificial neural network algorithms for the classification and detection of credit card fraud was developed using feature driven development methodology which deploys a feature centric approach to program development combining different requirement components to meet user needs. The system was trained and tested with credit card fraud datasets from Kaggle machine learning repository split into 70:30 ratio for training and testing purposes respectively. After 20 epochs the model performance outperformed the existing system with an accuracy of 99.83%, precision 100%, recall 100% and F1-score 100% respectively.

1. INTRODUCTION

The adoption of IT tools in the financial sector has improved service delivery, decision-making, and competitiveness (Luka and Frank, 2012). Environmental, organizational, and technical factors have shaped a highly competitive landscape centred on customers (Turban. 2005). Digital technologies, especially online banking, have shifted consumer expectations towards convenience. Financial institutions now offer tools that meet these demands, such as credit cards, which simplify digital payments but also increase fraud risks. Business growth today depends on retaining customers and responding quickly to market changes (Ako. 2024). With the 2014 cashless policy in Nigeria, non-cash payments rose significantly (Abubakar, 2017). Credit cards, issued by banks with revolving credit lines, support cashless payments online and offline.

*Corresponding author, e-mail:ako.rita@fupre.edu.ng, Didigwu.hillary@fepo.edu.ng

DIO

2 LITERATURE REVIEW

The theoretical foundation of this study is the Fraud Triangle Theory, developed which identifies three elements that drive individuals to commit fraud: perceived opportunity, perceived pressure, and perceived rationalization, pressures include financial stress (e.g., debt or medical bills), personal vices (e.g., gambling, alcohol), and workplace demands (e.g., unrealistic performance expectations or pressure to outperform competitors). This pressure, combined with opportunity and rationalization, can lead to fraud.

Fraudsters often believe they can act without consequence or detection. The rise of internet-based systems has also expanded access for adversaries, enabling large-scale attacks for personal gain. Global financial crime has led to losses exceeding $1.3 trillion, much of it through credit card fraud (Arnold et al., 2023). Institutions must now prioritize stronger safeguards to protect data and finances.

Opportunities arise when employees access assets and information that enable fraud, often in environments with weak internal controls, poor enforcement, or apathy. Restricting access to only essential systems and resources is vital.

Rationalization involves justifying dishonest acts. Employees may believe they deserve more for their contributions or feel unrecognized (Aduda. 2013). The "absence of guardians" refers to insufficient oversight, when no systems are in place to verify financial accuracy or test controls, fraud risks increase. Together, these three elements pressure, opportunity, and rationalization form the conditions under which fraud typically occurs.

Cybersecurity

Computers have transformed modern life, but this progress also brings the need for digital protection. Technology itself is not harmful rather, its misuse by individuals for personal gain or harm creates security risks. Businesses now operate in a hyper-connected environment made possible by the internet. This interconnectivity blurs national and industry boundaries, increasing exposure to external and internal cyber threats (Jiang. 2021). As cyber-attacks grow more complex, especially under the threat of global terrorism and organized crime, the digital space becomes a battlefield with real-world consequences. Critical infrastructure is increasingly at risk, requiring continuous monitoring and a strong cybersecurity commitment.

A major challenge in securing cyberspace is the absence of international regulatory frameworks and enforceable boundaries. Cybersecurity refers to practices and tools used to protect digital systems hardware, software, and data against unauthorized access. It includes maintaining data confidentiality, integrity, and availability (Seemma. 2018). Cyber threats can be categorized by vulnerability, response, and legal redress, involving both offensive and defensive strategies. Threat actors range from lone hackers to state-sponsored attackers, each with varying resources and tactics. For example, Vietnam-based actors targeted the World Health Organization in 2020.

The financial sector remains a prime target due to the ease of digital transactions. Financial customers face 66% more cyber-attacks than any other sector (World Bank, 2018). In Nigeria, fraud cases rose from ₦2.40 billion in 2016 to ₦15.15 billion in 2018, driven by cybercrime, illegal credits, and IT-based fraud. This trend threatens the stability and liquidity of financial institutions (Ikechi and Anthony, 2020).

2.1 *An overview of electronic banking in Nigeria and its associated threats*

The cybersecurity challenge in the banking and financial service sector remain unparalleled in comparison to others, not just in terms of the quantity of breaches but also in terms of the financial cost of incidents. The reason for this is that financial products and services like payments and transactions, savings, and borrowing are popular targets for cyber thieves. Furthermore, the increasing number of processes, usage of robotics for automated trading, and outsourcing to third parties all contribute. Cross-border transactions and interactions with clients over many channels and devices may worsen cybersecurity concerns. As a result, financially motivated hackers, worldwide intrusions and manipulation, internet fraud and phishing activities have the potential to cost financial institutions millions of dollars in assets (Jiang and Broby, 2021). Aside from that, a single system meltdown. Even a minor hiccup caused by ignorance can jeopardize a company's reputation, resulting in significant revenue loss and brand damage. The average annualized cost of cyber-crime for financial services organizations is USD 18.28 million, ranking among the highest of the 15 industries

Nigeria has made significant investments in the development of information technologies, as at December 2017, it was estimated that more than half of its population currently utilizes the internet. This equates to about 100 million people ranking it eight in the world in terms of Internet users. This advancement in information technology has also increased Nigeria's economic growth. For example, between 2010 and 2016, its GDP expanded from 369 billion USD to 405 billion USD (World Bank, n.d.), while Internet penetration increased from 11.5% to 25.7%.

Internet banking was first introduced to Nigeria in 2003. The event was marked by the introduction of Guidelines on Electronic Banking in Nigeria (CBN, 2003) by the Central Bank of Nigeria. Soon after, the Nigerian banking industry was recapitalized, with only 25 of the previous 89 Nigerian banks surviving. Those who lived were known to have used internet technologies to provide effective and efficient financial services. Internet adoption rate is 83% while Internet banking is 32%. The major inhibitors to Internet banking by non-adopters are risk, the ease-of-use perceived usefulness of the technology, the convenience of using ATM, phone banking, and branch banking. In addition, security of the innovation continues to be a main concern for adopters and non-adopters. The Nigerian banking sector in 2004 underwent a major banking reform, due to persistent cases of distress and failure, in addition to poor capital base, poor asset quality, fraud, corruption, erosion in public confidence among others. The Nigerian banking institution has realized the importance of technological adoption, and has therefore embraced the electronic and telecommunication networks for delivery products and services. The terms 'internet banking' and 'online banking' are frequently used interchangeably. They refer to a variety of financial services delivered via various technological platforms and electronic devices such as the internet, computers, mobile phones, and bank cards. According to Wang et al (2020) the various range of banking services available by the application of internet technology to improve service delivery and customer satisfaction in the sector include;

i. Automated Teller Machines (ATMs);
ii. Point of Sale terminals (POS terminals) that handle cheque verification, credit authorization, cash deposit and withdrawal, and cash payment;
iii. Personal Computer (PC) and mobile phone banking that primarily uses

personal computers and mobile phones as banking devices;

iv. card systems that use plastic smart cards with embedded integrated circuits to settle financial transactions.

2.2 Cybercrime Threats in Nigerian Banking Industry

Cybercrime is a global phenomenon that occurs in cyberspace, or the realm of computers and the internet. Cybercrime is the use of specialized apps in computers connected to the internet to conduct crime by technically skilled individuals. The consequences of such crimes may jeopardize a country's security architecture and financial health. So, cybercrime is simply defined as a crime committed with the assistance of a computer system. It refers to criminal conduct made easier by the usage of the internet (Ibrahim, 2019).

The expansion of the information and communication technology environment brings with it new and serious threats. Cyber-attacks now have the potential to cause significant harm to society in novel and critical ways. Online fraud and cyber-attacks are only a few instances of computer-related crimes that occur on a daily basis (Ojeka et al., 2017). Cybercrime has long harmed Nigeria's reputation globally and discouraged foreign direct investment (FDI) and other businesses. The amazing increase of mobile connectivity, as well as the Central Bank of Nigeria's push toward a cashless economy, also triggered the rise in cybercrime especially against the Nigerian banking industry and her teeming customers. Opines that the financial damages incurred by cyber-attacks are reported to be very high and rapidly increasing. According to report by Nigeria inter-banks settlement systems, Nigerian banks have lost N159 billion between 2000 and 2013 to cyber-crime and according to Nigeria-based information and communications technology company New Horizons Limited, N413 billion (USD 2.5 billion) is being lost annually to cybercrime. Although this financial cost can be measured, cost in human misery and tragedy is incalculable and now it is costing more than physical crime (Ali et al., 2014). The need to improve cyber security and protect critical and delicate information is extremely necessary for every nation's security and economic well-being. The Nigerian financial industry has a flaw. The extended arms of fraud appear to be inflicting a catastrophic blow on banks beneath the polished appearance and gentlemanly temperament of the nation's money managers. This occurrence has become a frequent nominee in the industry. Unfortunately, greed is the plague of our society today, and the idea of "getting rich quick" is unfortunately the order of the day. Banks have been a popular target for criminal elements using the cyberspace to carry out their illicit trade. It is not an exaggeration to say that only well-managed and secured banks will survive in the coming years in terms of fraud prevention. Every time provisions are made for losses caused by fraud; the banks' books lose their luster.

2.3 Types of Cybersecurity Attacks in the Banking Sector

In the last two decades banking and financial services have become more accessible to the general public as a result of advancements in information and communication technology (ICT) and the widespread use of mobile networks. However, technological advancement has made banking services more accessible and affordable, but it has also increased the risk of being a target of cybercriminals. The implementation of the cashless policy in the Nigerian financial service sector by the central bank of Nigeria (CBN) did not only come with is the ease in doing business and the reduction of the volume of physical cash carried by individuals and groups for one form of

transaction or the other it also came with the challenges of cyber-attacks of unsuspected bank customers and the financial institutions as they loss huge sum of money annually to these criminals.

a. Phishing

Phishing refers to the sending of unsolicited emails to the customers of monetary institutions, with the intention to encourage them to enter their information, such as username and password to access their account, usually into electronic forms in fake copy-cat websites (Hassan et al., 2012). These fake copy-cat websites take advantage of consumers who are not familiar with the exact web addresses and interfaces of their banks. The perpetrators are then asked to access online bank accounts of customers without their knowledge. The phishing scam is now perceived as a very common type of cyber security threat and is becoming one of the fastest growing threats affecting the financial sector in Nigeria.

b. Cyber Terrorism

Cyber terrorism refers to the launching of attacks on organizations or governments to access or distort information stored in their computer systems. Cyber extortion through Distributed Denial of Services attacks (DDOS) could be a possible method. It involves putting computer systems under DDOS attacks and demanding ransoms to restore services. Cybercriminals are more sophisticated than ever before, making it even more difficult to protect sensitive data. Failure to protect this data can result in serious financial losses, reputational damage, and legal obligations. While a complete hack may not be necessary to do considerable damage, the failure of a major bank might open the door to further dangers such as phishing schemes, malware assaults, and other types of misconduct. Cybercriminals' methods are growing more sophisticated across the board, and firms must prioritise cybersecurity measures to avoid cyber risks before they occur.

The nation's banking system is under constant threat, with bank runs, panic, and defaults lurking on the horizon. While there are systemic factors at work, emotion drives most of the reaction. The failure of Silicon Valley Bank (SVB) has raised concerns about the financial sector's overall vulnerability, particularly in the case of a cyberattack.Although the banking industry has always been cognizant of the threat posed by cyberattacks, it may today be more vulnerable than ever. Cybersecurity risks are fast developing, with nation-states attacking specialised industries such as banking (Sayegh, 2023).

c. Bank Verification Number (BVN) Scam

Bank Verification Number (BVN) scam is another form of cyber security threat, particularly in Nigeria that affects the banking industry. A BVN is a biometric identification system that uses an 11-digit number as a universal identifier across all banks in the country. The primary reason for the introduction of this system, by the central bank of Nigeria, has been to link all the bank accounts of an individual in order to minimize fraudulent activities. Its implementation, however, also provided fraudsters with an opportunity through which to carry out fraudulent activities on a much larger scale.

d. Password Sniffing

Password sniffing has also emerged as a foremost cyber secuirty threat affecting the banking sector. The threat involves the use of programs that are specifically designed to monitor all traffic in an organisation’s network. When a user types in his/her username and password as requested by the system, the sniffing program collects all that

information. Additional programs are then used to filter the information gathered, pulling out some important details, while covering up the existence of password sniffers. Evidence suggests that a significant number of financial institutions across the globe are now affected by attacks linked to password sniffing.

2.4 Electronic Banking Applications and Credit Card Fraud

The Internet is a shared network of computers that allows for the free movement of data or information. As previously stated, it is a crucial part of our everyday lives, and the number of individuals who expect to be able to direct their bank financial statements anywhere, at any time is steadily increasing (Vyshali-Rao 2014). Banks that use this medium must have the necessary systems to ensure secure transactions. Unlawful access to essential systems, tampering, or theft of customer data creates a safety concern.

Credit card fraud is the illegal use of another person's credentials or credit standing. It is a major form of identity theft. According to Kropelnytsky and Vidjikant (2023), the FTC reported over $2.6 billion lost in imposter scams in 2022. The purpose is to make unpaid purchases or steal money. The rise in ICT has led to more credit card-based transactions, increasing risks. Hackers now target banks for the customer data they hold. Consequently, banks lead in cybersecurity. Credit card fraud costs billions annually. New techniques are being used to track and detect it, but evolving threats require advanced tools (Btoush et al., 2021).

The surge in credit card usage has led to more fraud. Theft of the card or its information, and unauthorized use online, are common. The pandemic sped up digital payments. According to the BBB Foundation (2022), credit cards were the most reported scam payment method. The US Census Bureau (2023) reported $1.034 trillion in e-commerce sales in 2022. Birnstengel et al. (2021) found 127 million Americans were victims of credit card fraud, totalling $8 billion in attempted charges.

2.5 Types of Credit Card Frauds

There are various sorts of credit card fraud, ranging from counterfeit card fraud to lost or stolen card fraud. 'Lost and stolen card fraud is opportunistic and can be controlled by cardholders taking precautionary measures, whereas counterfeit card fraud involves a variety of technological fraud types such as cloned cards, changing information on the magnetic stripe, and re-embossing details onto. Credit card fraud does not occur in isolation. Credit card fraud is frequently associated with other crimes such as burglary, mail theft, and organized crime.

i. Fraud with stolen and lost credit cards

Lost and stolen card fraud encompasses all frauds committed on cards that have been declared lost or stolen by the cardholder. It may occur at stores that do not have chip and PIN equipment before the cardholder reports the theft or loss. This can be used for phone, online, or mail-order purchases. The most common sort of credit card fraud is the "theft of genuine card details that are used to make a purchase through a remote channel such as the phone, fax, mail order, or the Internet, and/or by presenting the card at a till point (Trenca and Bojan, 2009).

ii. Counterfeit fraud

When a credit card is used remotely, only the credit card details are required. This is known as counterfeit fraud. At some time, someone will steal your card number and codes and use them on websites that do not require a signature or real cards. In a 2005 research, Pago, one of the largest international acquiring and payment service providers, stated that credit card theft is an increasing

concern to firms providing goods or services over the internet. Online merchants are at risk since they must accept credit card payments from their customers (Pago-Report, 2005). When fraudsters utilise stolen or modified credit card data, the merchant loses money due to charge-backs which are automatically generated when card hoders object to items on their monthly statement due to the fact that they were not responsible for suh purchases.

iii. Skimming

Credit card skimming is the illegal copying of a credit card or a bank card by thieves using a device that reads and duplicates the information from the original card. Dishonest business employees use small machines known as "skimmers" to read credit card numbers and other information, capturing and reselling it to criminals who build counterfeit cards or charge products over the phone or the Internet. Pundkar and Zubei (2023), opined that card skimming can also occur offline, where these cybercriminals place devices known as skimmers on physical card readers such as ATMs or point-of-sale (POS) terminals. When a cardholder swipes or inserts their card, these skimmers record the information. The stolen information is then used to build counterfeit cards or make fraudulent purchases.

2.6 Credit Card Fraud Detection Systems

The range of fraud types makes detecting credit card fraud a complex task. Most banks conduct standard checks on new applications to spot potentially fraudulent ones. In some cases, investigators have identified fake applications by analyzing handwriting styles, including some tied to organized Nigerian fraud rings. However, once a card is issued, banks typically rely on monitoring account activity to detect suspicious behaviour. Many use rule-based systems to evaluate account actions, such as setting limits on the number of daily transactions or flagging high-value purchases (Ghosh and Reilly, 1994). These rules are generally derived from past fraud patterns, but many banks apply only basic statistical methods, resulting in simple threshold-based conditions. While these systems can catch some anomalies, more advanced technologies tend to perform better. Fraud detection, when viewed as a pattern recognition task, fits well with artificial intelligence (AI) methods—especially machine learning.

Machine learning can identify subtle patterns in large volumes of data that rule-based systems may miss. As a result, AI tools such as artificial neural networks, support vector machines, and K-Nearest Neighbour algorithms are increasingly used in fraud detection. These methods are already being applied to various problems in financial services and are proving to be effective in enhancing fraud prevention strategies.

2.7 Application of Machine Learning Algorithms for Credit Card Fraud Detection

Machine Learning is the most popular and widely utilized technology due to its numerous applications, low time consumption, and higher accuracy in results. Machine learning is a technology that deals with algorithms, which give computers the ability to learn and progress via experience without being explicitly programmed. Machine learning can be used in a variety of fields. Medical terms, for example, diagnostic, regression, and so on. Machine learning is a combination of algorithms and statistical models that enable computers to accomplish tasks without hard coding. A model is built using training data and then evaluated on the trained model (Asha and Suresh, 2021). Over time, different machine learning algorithmic approaches have been used to detect fraud in credit card transactions, but with little success. As a result, effective and efficient algorithms that work effectively must be devised. Here we

shall consider different machine learning algorithms and their efficiency in credit card fraud detection.

2.8 Random Forest (RF)

Random Forest (RF) is a machine learning algorithm based on decision trees (DT), commonly used for regression and classification. It combines multiple decision trees to improve prediction accuracy and reduce overfitting (Darwish, 2019). While effective with large, unbalanced datasets, RF struggles with training speed and scalability in real-time regression tasks.

Traditional methods like logistic regression (LR), C4.5, and RF have been used in credit card fraud detection (CCFD). LR models binary relationships but may fail with nonlinear real-time datasets, making it less suitable for CCFD. C4.5 is often used for decision-based classification in data mining.

Vynokurova et al. (2020) proposed a hybrid approach combining RF and Isolation Forest to detect anomalies. Their model includes both unsupervised anomaly detection and a supervised explanation subsystem. While effective, it lacks measures for data privacy and does not address geolocation spoofing risks.

Our contribution will focus on integrating geolocation and time-based features, using Artificial Neural Networks (ANN) and Federated Learning to improve fraud detection while preserving user data confidentiality.

Although RF is effective on controlled datasets, it performs poorly on real-time data due to slow training and prediction, making it less ideal for practical CCFD scenarios.

2.9 Artificial Neural Network (ANN) Algorithms

Artificial neural network (ANN) is a machine learning algorithm which functions similarly to the human brain. Artificial neural network models are highly fault tolerant, for example, the generation of output is sustained even with the corruption in single or multiple cells. Due to its high speed and effective processing capabilities, ANN can be considered an effective solution for the credit card fraud detection. Typically, ANN is based on supervised method and unsupervised learning methods. The Unsupervised Neural Network is widely used in detecting fraud cases since it has an accuracy rate of 95%. The unsupervised neural network attempts to find similar patterns between the credit cardholders present and those found in earlier transactions. Suppose the details found in the current transactions are correlated with the previous transactions. Then, a fraud case is likely to be detected.

According to Ehsan (2023), artificial neural networks (ANN) are computational networks consisting of an input layer, hidden layer(s) and an output layer. Each layer consist of neurons as depicted in Figure 2.1 and in turn each neuron has a weight value (*w)* and bias value (*b)*. The output vector of each layer is computed as;

$$S^{(i)} = W_i x^{(i-1)} + b_i \quad (2.1)$$

$$x_i = f\left(s^{(i)}\right) \quad (2.2)$$

where $f : \mathbb{R} \longrightarrow \mathbb{R}$ is an activation function and x_i are the input values. Typically, the hyperparameters w and b are initialized with random values and changed during the training process. The network's output is calculated in a process known as forward pass, in which the input vector x is fed into the network, which calculates the output of the

layers from the first to the last output layer using Equations 2.1 and 2.2.

The values of the weights and biases are modified during the iterative training phase of the model. The algorithm is trained using samples of training data with known input and output values. The forward pass is used to calculate the output for each training sample. In binary classification, the output layer can be built with two neurons, one for each class. Each neuron's level of activity (high or low output value) indicates which class the input belongs to. During the training process, the loss function is minimized by adjusting the network's weights and biases using gradient descent or other optimization procedures. (Ng, 2011).

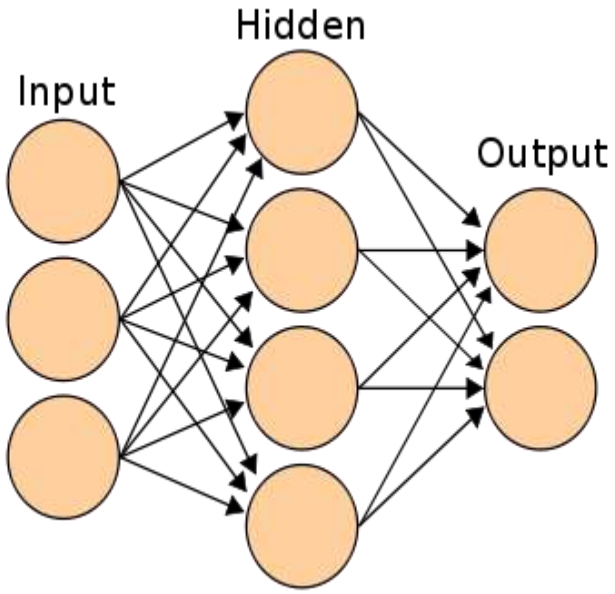

Figure 1: ANN Architecture (Source: Ng, 2011)

There are various loss functions that can be utilized to solve various problems. In general, the binary cross entropy loss function, which is utilized in binary classification issues can be defined as:

$$L = -\frac{1}{n}\sum_{j=1}^{n} y_j \,.\, log\hat{y}_j + (1 - y).\log(1 - \hat{y}_j) \quad (2.3)$$

where n is the output size, $\hat{y}_j$ is the output from the j:th neuron with the corresponding target value y_j. Using back-propagation, the loss is minimized by modifying the network's weights and biases by first calculating the derivative of the loss function with respect to the biases and weights, $\frac{\partial L}{\partial W_i}$ and , $\frac{\partial L}{\partial b_i}$. These derivative are solved by applying the chain rule. After calculating the derivatives, the update in the weights and biases are calculated by;

$$\Delta W_i = -\eta \frac{\partial L}{\partial W_i} \quad (2.4)$$

$$W_i + 1 = W_i + \Delta W_i$$

An artificial neural network that is trained using a simulated annealing algorithm is effective in identifying various fraudulent credit card transactions. The stimulation annealing algorithm optimizes the performance by finding out the best suitable configuration weight in the neural network (Li et al., 2021). According to the literature, ANN is an excellent algorithm that can be utilised in credit card fraud detection (CCFD); it has achieved good performance when employed in conjunction with other functions and algorithms. Individuals are missing from such functions. The application of ANN in CCFD, on the other hand, has proven to be promising due to its ability to accommodate a bigger volume of data and dispersed memory structure.

2.10 Support Vector Machine (SVM)

Support vector machine (SVM) is a supervised machine learning method capable of classification and regression. SVM algorithm seeks to locate a hyperplane in the data space that creates the greatest minimum distance (called margin) between objects (samples) belonging to different classes using a training set of objects (samples) split into classes. As a result, the hyperplane is referred to as the largest margin hyperplane. Rather than employing differences in class means, SVM simply uses objects (samples) on the margin's edges (called support vectors) to divide objects (samples). The algorithm is termed SVM because the separating hyperplane is supported (defined) by the vectors (data points) closest to the margin.

SVM has been proved to perform effectively in a wide range of real-world learning tasks and is often regarded as one of the best "out-of-the-box" classifiers. SVM has the benefits of enhancing class separation and decreasing predicted prediction error. Furthermore, SVM is adaptable for both linear and nonlinear discriminatory analyses, and it is appropriate for high-dimensionality datasets with limited sample sizes when combined with feature selection algorithms. It is considered for classification and carry out regression analysis for various problem (Xia, 2020). For the use of SVM in the identification of credit card fraud through the analysis of client usage patterns. The databases were used to collect client payment habits. The support vector machine technology is used to categorise consumer patterns as fraudulent or non-fraudulent. The SVM approach is efficient and produces reliable results when fewer features from the dataset are employed (Sriram et al., 2019). However, the issue arises when a larger number of datasets (at least 100,000) are used. When it comes to the application of SVM in credit card detection fraud (CCFD) analysis, it is unsuccessful when utilized in real-time due to the vast size of datasets.

2.11 K-Nearest Neighbour (KNN)

KNN is a type of supervised ML method that aids in problem classification and regression analysis. It is an effective method in supervised learning that aids in improving detection and decreasing false-alarm rates. It employs a supervised technique in determining the presence of fraudulent activity in credit card transactions. The KNN fraud detection technique requires two estimates: transaction correlation and distance between transaction occurrences in data. The KNN approach is appropriate for detecting fraudulent activities throughout the transaction process. It is possible to discover abnormalities in the targets by doing over-sampling and isolating data. As a result, it can be evaluated for credit card fraud detection in memory constraints. It can help with credit card fraud detection while requiring less memory and processing resources. It is a more efficient method for any number of datasets. KNN outperforms other anomaly-based approaches in terms of accuracy and efficiency.

It is extensively used to recognize a similar pattern in the cardholder's prior transactions. Machine learning algorithms that are often employed include LR, Nave Bayes, and KNN. When it comes to detecting fraudulent credit card transactions, the KNN has an accuracy rate of 97.69%. It has resulted in peak performance. KNN has been shown to be efficient in performance in terms of all metrics tested, since it did not record any false-positives while classifying. Another investigation was conducted using KNN, and 72% accuracy for CCFD was reached (Itoo and Meenakshi, 2021).

2.12 Related works

Sharma and Bohra (2017) proposed a five-phase authentication mechanism in "Enhancing online banking authentication using hybrid cryptographic method" that employs several authentication processes. First, a user ID and password are formed, followed by a user unique ID (UID). The important step in the paper is to match the UID with the user's QR code, and then the transaction is completed with a one-time password. This work uses the RSA method and the MD5 algorithm to secure the data communicated between the server and the merchant carrying out the transaction. The use of these algorithms assures privacy and secrecy authentication, non-repudation, and integrity.

An Online Fraud-Resistant Technology for Credit Card E-Transactions" employs the fraud resistant method. Normally, a 16-digit card number is displayed on cards that can be used unethically, however the author has developed a modal that replaces the last 8 digits of cards with alphanumeric characters. The eight-digit number identifies the issuer and card type, while the eight alphanumeric characters validate the cardholder's identity. In general, many users save their passwords in their browser, which can lead to unauthorised access because any other person can quickly get into the computer and conduct the transaction.

Ileberi et al.(2022) proposes a credit card fraud detection engine based on machine learning (ML) that uses the genetic algorithm (GA) for feature selection in "A machine learning based credit card fraud detection using the GA algorithm for feature selection". Following the selection of optimum features, the proposed detection engine employs the ML classifiers Decision Tree (DT), Random Forest (RF), Logistic Regression (LR), Artificial Neural Network (ANN), and Naive Bayes (NB). The suggested credit card fraud detection engine is assessed using a dataset produced from European cardholders to validate its performance. The results showed that our proposed method outperforms existing systems.

The Whale Swarm Optimization Algorithm (WOA) to solve the problem of slow convergence rate in their research "Credit card fraud detection based on Whale algorithm optimized BP neural network." They employed WOA to get an initial optimal value, then used the BP network method to correct the incorrect value to get the best value.

According to Dighe et al. (2018), data mining techniques such as the DT, MLP, and CFLANN are commonly used to discover patterns from previous transactions. When comparing performance, these models frequently employ two types of datasets. The accuracy of the Multiple-layer perception (MLP) model in the Australian-credit card dataset is 88.95% [Class Distribution: CLASS 2: +: 307 (44.5%), CLASS 1 383 (55.5%)] and 78.50% in the German-credit card dataset, indicating that the MLP performs differently in different datasets. The usage of MLP may not be very useful in credit card fraud detection (CCFD) because to the increased number of factors, which leads in a highly dense structure, resulting in duplication and performance inefficiency. The author did not address this issue, which is critical for using the MLP process in real-time.

Randhawa et al. (2018) tested both traditional models and hybrid techniques that used AdaBoost and majority voting. They added noise to the dataset again to test the resilience of their model. They came to the conclusion that majority voting has a high accuracy in detecting credit card fraud.

Pumsirirat and Yan (2018) used deep learning to detect credit card fraud using an auto-

encoder and a constrained Boltzmann machine. The authors argued for their method based on the fact that most supervised learning algorithms detect abnormalities as fraud by using behavioural patterns of "legitimate" user's spending behaviour, while keeping in mind that the "legitimate" user's behaviour can change, causing the algorithm to incorrectly classify legitimate transactions as illegitimate. As a result, they advocated for the adoption of unsupervised machine learning technique, which is how they came up with their methodology.

Seera et al. (2021) used the GA for feature selection and aggregation to create an intelligent payment card fraud detection system. The authors used multiple machine learning techniques to validate the efficacy of their proposed method. The results showed that the GA-RF had an accuracy of 77.95%, the GA-ANN had an accuracy of 81.82%, and the GA-DT had an accuracy of 81.97%.

Sailusha et al.(2020) in "Credit Card Fraud Detection Using Machine Learning" implemented machine learning methods for credit card fraud detection. The algorithms employed are the random forest method and the AdaBoost algorithm. The findings of the two algorithms are based on accuracy, precision, recall, and F1-score. The ROC curve is plotted using the confusion matrix. The Random Forest and AdaBoost methods are compared, and the approach with the highest accuracy, precision, recall, and F1-score is regarded the best one for detecting fraud.

3. MATERIALS AND METHODOLOGY

The software development methodology deployed for the study is the agile development methodology consists of various software engineering methods with high level sensitivity to the user and the ever-evolving business environment requirement. Agile development methodologies incorporate variables that can change requirements, resources, time frames and technologies. Leveraging on discrete event simulation of complex interactions and algorithms that can predict the impact of various random events which may influence the output generate. Agile software development methodology has over the years made software development more customer collaborative and responsively address efficiency and effectiveness. From the agile the group, the feature driven development methodology would be used for the development of the proposed system.

further affirms that FDD groups all the features, design and build iteratively to create milestones that can be tracked to keep the customers up to date with the status of the development process. FDD is a lightweight process oriented, client centric methodology that is adaptive and incremetally implements functional requirements in short iterations with the aim of developing functional and qaulity software. It also focuses on the design and building phases of the software development process which is implemented in five distince phases. These phases include to develop an overall model, build a feature list, plan by feature, design by feature and build by feature respectively. Figure 3.1 shows the schematic of the feature driven development process as earlier stated from the design phase to the final phase where the system is built by features.

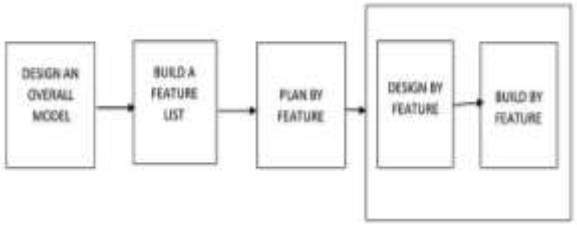

Figure 2: Feature driven development model (Source: Nawaz et al., 2017)

3.1 Analysis of the Existing System

The current system, developed by Kumar et al. (2022), uses support vector machines (SVMs) to identify fraudulent credit card transactions. The fraud detection problem is handled by the model as a binary classification problem. The dataset was imported from a Kaggle source that is open to the public. The dataset is in CSV (Comma Separated Values) file format. The dataset has been prepared by eliminating duplicates and ensuring that no values are missing. Every categorical feature in the dataset will be handled using label encoding and one-hot encoding. The attributes in the data have varying scales, and rescaling the attributes to the same size for every attribute in the data could benefit several machine models.

3.2 Architecture of the Existing System

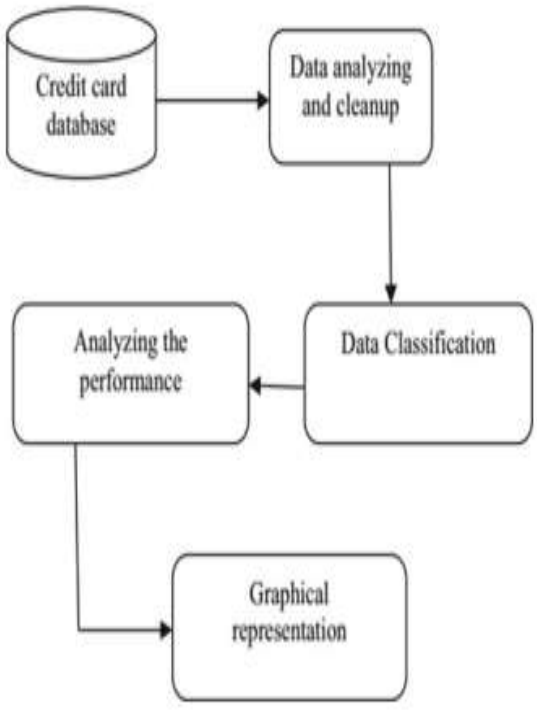

Figure 3 Architecture of the Existing System (Source: Kumar et al, 2022)

The existing system which is a support vector machine (SVM) algorithm used for classification and pattern analysis of credit card classifies and predict patterns into two classes; fraud or legitimate using binary classifications approach. In the existing system the process involved include the uploading of credit card dataset into the SVM model where the dataset is analyzed and preprocessed for data cleansing and features extracted. The dataset is further split into training and test data in the ratio of 70/30% for training and test activities respectively. The dataset for training is then used for training the model and test for testing the model before the classification process is done where legitimate transaction and fraud are classified and detected accordingly. Furthermore, the performance of the system is analyzed using standard machine learning model evaluation metrics. The existing system above others yielded an accuracy of 94.99% accuracy, precision of 95.98, recall 95.12, and an F1 score of 95.11 respectively

3.3 Limitations of the Existing System

The following limitations were identified from the existing system;

i. The model underfits due to large dataset,
ii. Unable to manage uncertainty in dataset due to noise
iii. Unable to manage and handle time series data,
iv. High false alert and false positive prediction
v. It takes a longer time to train the SVM model

3.4 Algorithm of the Existing System

Step 1: Start
Step 2: Import libraries (Numpy, Pandas, sklearn etc).
Step 3: Load the dataset (credit card fraud dataset in CSV format)

Step 4: Summarize the data
Step 5: Pre-processing data
Step 6: Checking for categorical data (using one-hot encoding to convert categorical into numerical data)
Step 7: Splitting the data (Split 70% training and 39% test)
Step 8: Move to SVM
Step 9: Verify transaction dataset
Step 10: Classify dataset using Use the SVM model
St3p 11: Detect incoming transactions as fraud or legitimate
Step 12: Evaluate algorithms
Step 13: Prediction of results
Step 14: Stop

3.5 Analysis of the Proposed System

The proposed system is a fusion of the existing support vector machine (SVM) and the artificial neural network (ANN) model aimed at leveraging on the advantages inherent in both models to deliver improved performance in credit card fraud detection. The reason for the combination of both machine learning models is that because ANN model has the robustness, which can effectively solve the non-linear and complex problem while the SVM model has the ability to solve the non-linear problems even with relatively less historical samples datasets. Though the ANN requires large dataset to optimize it performance. The process of the identification of credit card fraud must be sufficiently flexible to keep up with the continuous evolution of fraud over time and the occurrence of unknown anomalies. This therefore makes the proposed system relevant as it can handle real time credit card transaction fraud detection with high prediction accuracy.

a. Architecture of the Proposed System

Figure 3.3 show the architecture of the proposed system indicating the input component which is the incoming transaction which has to do with the input of card information into the system for the identification and classification process. The SVM model the data cleaning component where the process of data preprocessing and feature extraction is carried out and relevant feature extracted for the prediction process. The dataset containing the training and test datasets, the ANN component where the final classification of extracted feature earlier classified by the SVM component would be carried out to ensure for more succinct scrutiny of the datasets to enhance the classification accuracy of the improved SVM-ANN model.

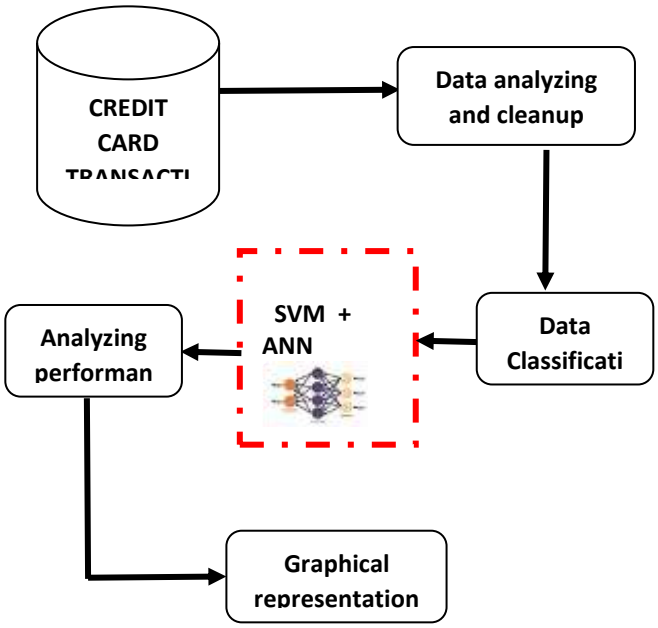

Figure 4: *Architecture of the Proposed System*

3.6 Advantages of the Proposed System

The proposed system implements a hybrid machine learning model that is improved and outperforms the existing system due to the combination of the SVM and the ANN models which enables it overcome the observed limitations and shortfalls of the existing system. The proposed system has the

following advantages as against the existing SVM model;

i. It overcomes the perceived limitation either of the machine learning algorithms,
ii. Overcomes the problem of class imbalance in data,
iii. It is more efficient for credit card fraud classification and prediction process,
iv. It is efficient in identification of anomaly and trends in the transaction process,
v. It is faster with minimal response time,
vi. High prediction accuracy with reduced false alert.

3.7 *Algorithm of the Proposed System*

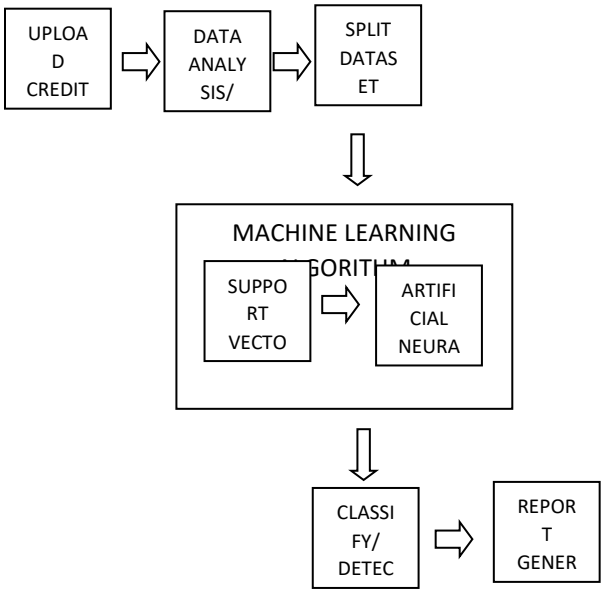

Figure 5: Process Flow Diagram of the Proposed System

Step 1: Start
Step 2: Import libraries (Numpy, Pandas, sklearn etc).
Step 3: Load the dataset (credit card fraud dataset in CSV format)
Step 4: Summarize the data
Step 5: Pre-processing data
Step 6: Checking for categorical data (using one-hot encoding to convert categorical into numerical data)
Step 7: Splitting the data (Split 70% training and 39% test)
Step 8: Move to SVM
Step 9: Verify transaction dataset
Step 10: Classify dataset using Use the SVM model
Step 11: ANN Model receives dataset
Step 12: Optimize ANN Model for classification
Step 13: Detect and classify incoming transactions as fraud or legitimate
Step 14: Evaluate algorithms

4 RESULTS AND DISCUSSION

The new system combines the efficiency, robustness and predictive accuracy of the support vector machine (SVM) and artificial neural network (ANN) to classify the credit card transaction data into fraud and non-fraud classes respectively. The new system was implemented in python using the Google Colab machine learning online platform designed for training and testing machine learning models giving developer the opportunity to leverage on the online GPU and inherent python libraries and other dependable file to ensure easy coding, debugging and collaboration with other third-party machine learning platforms like GitHub and Kaggle respectively.

The new system was implemented by;

i. Loading the dataset and preprocess it.
ii. Splitting the data into training and testing sets.
iii. Implement a hybrid SVM-ANN model.
iv. Train the model, evaluate it, and visualize the results.

From the above process, after loading the dataset, the dataset which is csv file will be available in the working directory and loaded to check for imbalanced class, processed and spilt into training and test data respectively. The training dataset is takes 70% and the test data 30% respectively. . Furthermore, the

SVM model component of the new system performs the feature transformation process where features are extracted and transformed into valued output that is fed as input to the ANN component for the predictive process where the dataset is evaluated as fraud and non-fraud cases respectively. The SVM is trained to reduce the dimensionality and then feed the output into a neural network. Figure 4.1 Show the process of uploading the dataset into the model from where the model now performs the preprocessing.

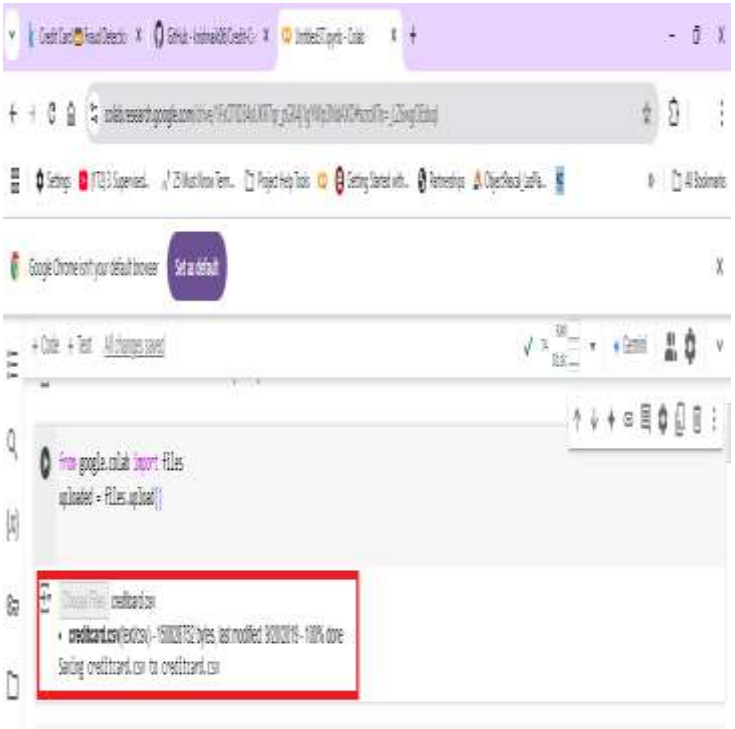

Figure 6: Uploading Dataset

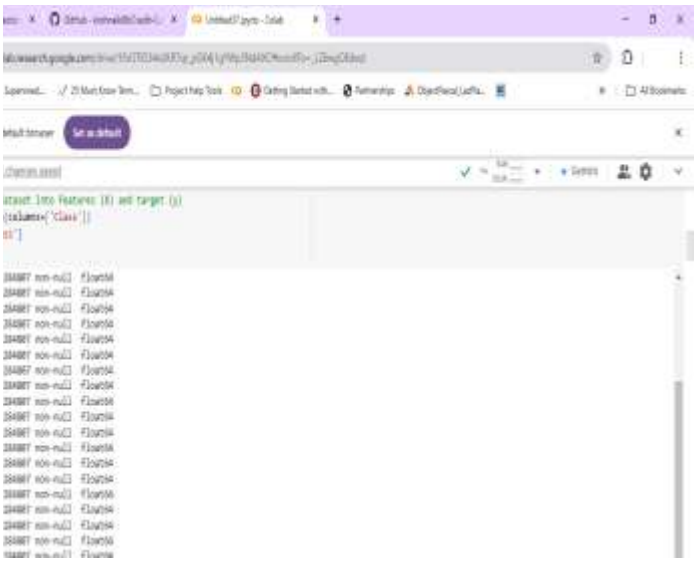

Figure 7: Displaying Basic information on Dataset

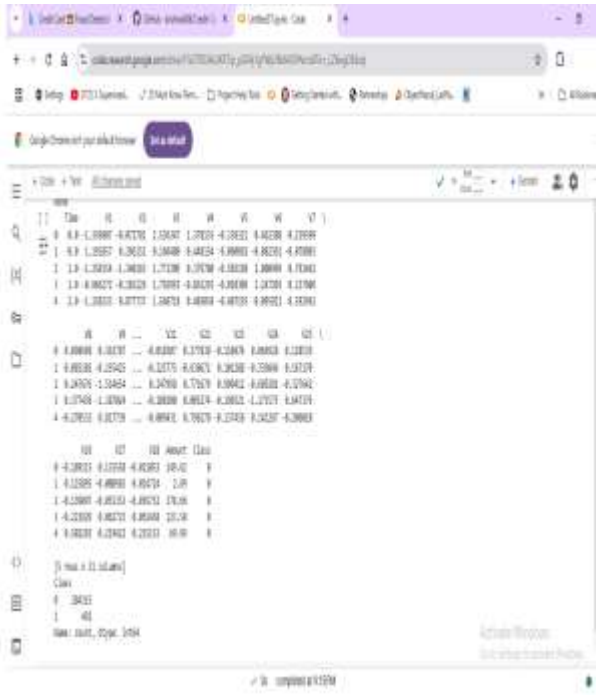

Figure 8: Basic information of the Datasets

Figure 9 Model Training

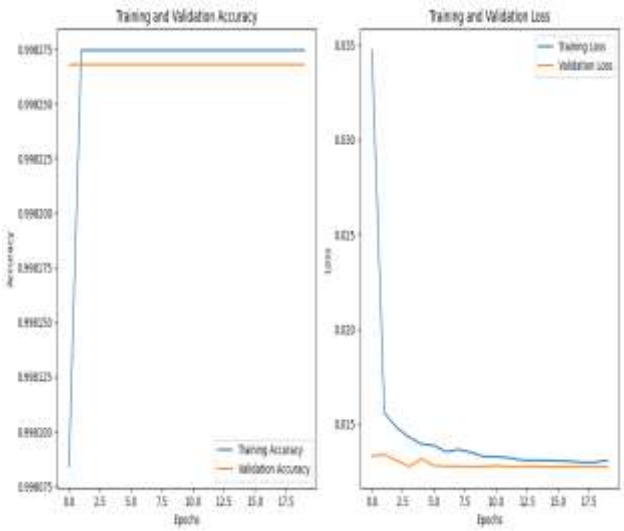

Figure 10 Training and Validation Accuracy and Loss Graph

Figure 11: Model Output and Confusion Matrix

The model after the upload of the dataset reveals the basic information of the dataset such as the head () which indicates the first few rows of the entire dataset. From the figure 4.3 model indicates that the dataset comprises of 5 rows and 31 columns with 284, 315 as non-fraud and 492 as fraud incidents. Though the dataset is unbalanced the model during the preprocessing phase balances does data augmentation and balances the dataset.

After 20 epochs model yielded a training and validation accuracy of 0.9982 and 0.9983 with a training and validation loss of 0.0134 and 0.0127 respectively as indicated figure 4.4 and 4.5 respectively. It important to note that the more training the model undergoes the more the accuracy it will attain the detection of credit card fraud. The epoch indicates the number of training time or iterations the model undergoes. This model attained the accuracy stated above after 20 iteration which implies that if subjected to more training time the efficiency of the model will be improved.

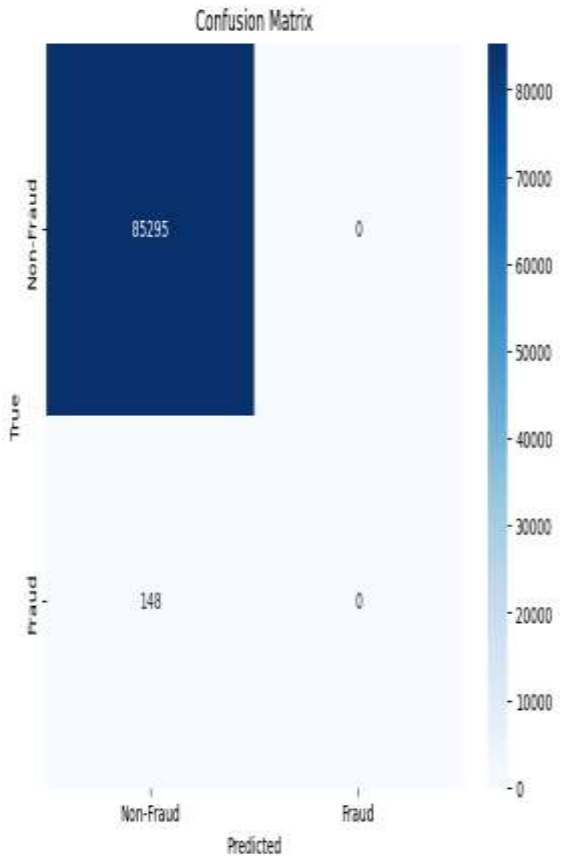

Figure 12: Confusion Matrix

The performance of the model as indicated in figure 10 shows that model yielded an accuracy of 99.83%, the model had a 100% precision, recall and F1-score respectively outperforming the existing system in all categories of the evaluation metrics. The confusion matrix in figure 11 also indicate that the model had a true positive (TP) prediction of 85, 295 for non-fraud cases, a false positive prediction of 0 while it yielded a true positive prediction (TP) of 0 for fraud cases with a false positive (FP)prediction of 148 respectively.

Model Evaluation

The new model here developed and implemented for the detection of credit card fraud using credit card fraud comer separated value files after 20 epoch yielded the values in table 1 and figure 12 with respect to the model accuracy, precision, recall and F1-score respectively.

Table 1 Model Performance Table

SN	Evaluation Metrics	Performance
1	Accuracy	99.83
2	Precision	100.00
3	Recall	100.00
4	F1-Score	100.00

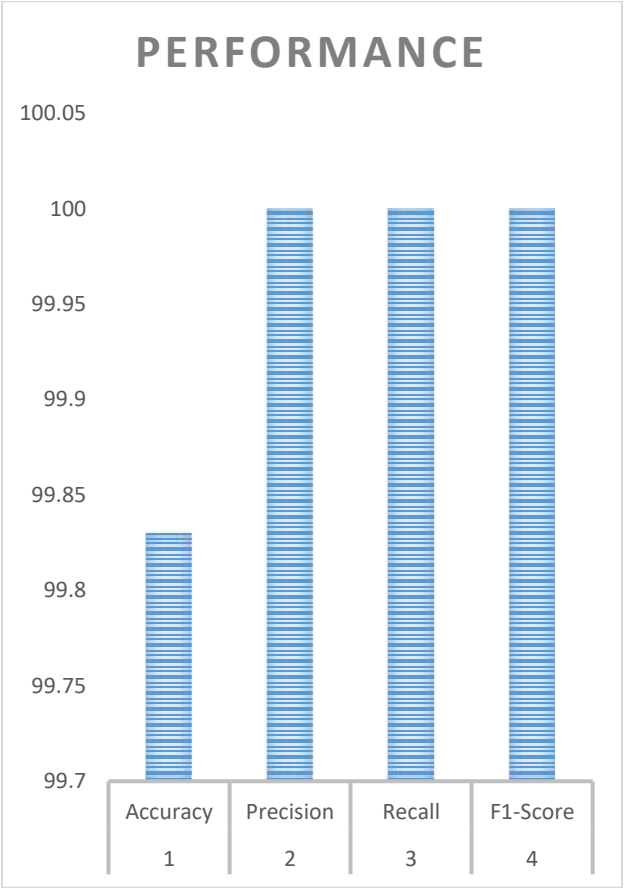

Figure 13: Model Performance Chart

Comparative Analysis of the New and the Existing Systems

The new system was predicated on the model developed by Kumar et al (2022) which

implemented a model for the detection of credit card fraud from online transaction using support vector machine to classify the transactions as fraud and non-fraud transactions respectively. The existing SVM model achieved a predictive accuracy of 94.99%, precision of 95.98% and recall of 95.12% and an F1-Score of 95.11% respectively. From the foregoing, it is evident that the new system outperformed the existing system significantly with a predictive accuracy of 99.83%, precision, recall and F1-Score of 100% respectively as indicated in the comparative analysis table and graph in table 4.2 and figure 4.9 respectively.

Table 2 Comparative Analysis Table

SN	**EVALUATION METRICS**	**PERFORMANCE**	
	Models	**Kumar et al (2022)**	**New System**
1	Accuracy	94.99	99.83
2	Precision	95.98	100.00
3	Recall	95.12	100.00
4	F1-Score	95.11	100.00

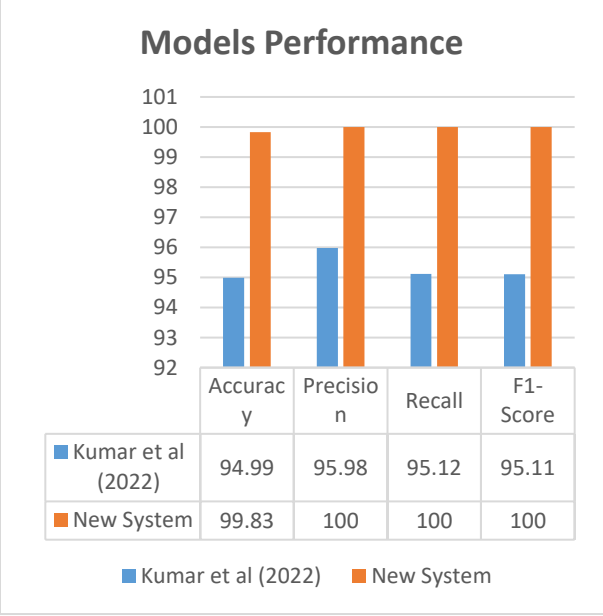

Figure 14 Comparative Analysis Chart

5 CONCLUSIONS

The application of machine learning models for predictive analytics have improved information security and reduced the level of intrusion into individual and organizational transactions especially with credit card fraud transaction which has taken and astronomical rise in the past 10 years. The study after an exhaustive review of recent related work leveraged on and improved the work by Kumar et al (2022) by infusing an artificial neural network model to their SVM model and the system yielded an impressive performance accuracy outperforming and surpassing the existing model by 0.64% with a 99.83 as against the 94.99% accuracy achieved by the existing system. The performance of the model is an indication that limitations and the inherent pitfalls of deploying a single machine learning model for solving prediction and classification problems can be improved and upscale by the introduction of hybrid and ensemble models irrespective of the domain.

REFERENCES

Abubakar, Y. (2017). An Historical Overview of the New Cashless Policy in Nigeria. *International journal of innovative research and development (IJIRD), 6*(7), 241-250.

Aduda, J. (2013). Relationship between Agency Banking and Financial Performance of Commercial Banks in Kenya. *Journal of Finance and Investment Analysis, 2*(4), 1-6.

Advanced Computer Science and Applications, 3(9), 146-149

Ako, R.E. (2024). Improving Customer Trust through Fraud Prevention E- Commerce Model (pp. 1-7). IEEE *Journal of Computing, Science and Technology* (JCST). Volume 1(2): 76-85

Arnold Et Al (2023). Forging A User-Trust Hybrid Memetic Modular Neural Network Card Fraud Detection

EnsembleJournal of Computing Theories and Applications ISSN, 2023

Asha, R.B and Suresh, K.K.R. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings*, *2*(1), 35-41.

BBB Foundation. (2022). *2022 BBB Online Scams Report: Start With Trust® Online.* Retrieved from BBB Foundation: https://bbbfoundation.images.worldnow.com/library/d2727fa5-c843-48f2-95aa-5e018bd7b39c.pdf

Birnstengel, et al., (2021). *Credit Card Fraud 2021 Annual Report: Prevalence, Awareness, and Prevention.* Retrieved from Security: https://www.security.org/digital-safety/credit-card-fraud-report/2021

Btoush, et al., (2021). A survey on credit card fraud detection techniques in banking industry for cyber security. *8th International Conference on Behavioral and Social Computing (BESC)* (pp. 1-7). IEEE

Central Bank of Nigeria [CBN]. (2003). *Guidelines on Electronic Banking in Nigeria.* Central Bank of Nigeria (CBN). Retrieved from https://www.arca.network/lib/E-BANKING-Regulation-document.pdf

cyber security. *8th International Conference on Behavioral and Social Computing (BESC)*

Darwish, S. (2019). An intelligent credit card fraud detection approach based on semantic fusion of two classifiers. *Soft Computing*, *24*(1), 1243–1253.

Dighe, et al., (2018). *Detection of credit card fraud transactions using machine learning algorithms and neural networks: a comparative study.* IEEE.

Ehsan, N. (2023). *Credit Card Transaction Fraud Detection Using Neural Network Classifiers.* KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science. Retrieved from https://kth.diva-portal.org/smash/get/diva2:1750971/FULLTEXT01.pdf

Ghosh, S and Reilly, G.L. (1994). Credit card fraud detection with a neural-network. *Twenty-Seventh Hawaii International Conference on System Sciences*, *3*, pp. 621-630.

Ibrahim, U. (2019). The impact of Cybercrime on the Nigerian Economy and Banking System. *NDIC-Quarterly, 34*(12).

Ikechi. and Anthony, N. (2020). Fraud Theories and White Collar Crimes: Lessons for the Nigerian Banking Industry. *International Journal of Management Science and Business Administration*, *6*(6), 25-40.

Ileberi, E., Sun, Y. and Wang. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal Big Data*, *9*(24), 45-59.

Intelligence. University of trathclyde, Centre for Financial Regulation and Innovation.

International Journal of Scientific and Research Publications, *4*(5), 2250-3153

Itoo, F and Meenakshi, SS. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *International Journal of Information Technology , 13*(1), 1503–1511.

Jiang and Broby. (2021). *Mitigating cybersecurity challenges in the financial sector with Artificial*

Kropelnytsky, Y and Vidjikant, S. (2023). *An Overview of Detecting and Preventing Credit Card Fraud by Using New Technology*. Retrieved from Soft Journ: https://softjourn.com/insights/detecting-and-preventing-credit-card-fraud

Kumar, et al., (2022). Credit Card Fraud Detection Using Support Vector Machine. *2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications* (pp. 27-37). ICRTM.

Li, et al., (2021). Application of credit card fraud detection based on CS-SVM. *International Journal of Machine Learning and Computing*, *11*(1), 34-39.

Luka, M.K and Frank, I.A. (2012). The Impacts of ICTs on Banks. *International Journal of Advanced Computer Science and Applications, 3*(9), 146-149

Ojeka, et al., (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing, 7*(2), 340-346.

Pago-Report. (2005). *The development of E-commerce sectors.* Pago eTransaction Services.

Pumsirirat, A and Yan, L. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. *International Journal of Advanced Computer Science and Applications(IJACSA), 9*(1), 18-25.

Pundkar, S.N and Zubei, M. (2023). Credit Card Fraud Detection Methods: A Review . *International Conference on Sustainable Development Goals (ICSDG 2023)*, (pp. 1-11).

Randhawa, et al., (2018). Credit card fraud detection using AdaBoost and majority voting. *IEEE Access, 6*, 14277–14284.

Sayegh, E. (2023). *Potential For Devastation: The Impact Of A Cyberattack On The Banking System*. Retrieved from Forbes: https://www.forbes.com/sites/emilsayegh/2023/06/06/potential-for-devastation-the-impact-of-a-cyberattack-on-the-banking-system/?sh=2dcdf2811b45 -sector-regulation-and-supervision

Seemma, P.S. (2018). Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125-128.

Seera, et al., (2021). An intelligent payment card fraud detection system. *Annals of Operations Research, 23*(7), 1–23.

Sriram, et al.,(2019). Credit card fraud detection using various classification and sampling techniques: a comparative study. *International Conference on Communication and Electronics Systems (ICCES)* (pp. 1713–1718). IEEE.

Trenca, L and Bojan, D. (2009). *Operational Risk in Banking – Card Fraud.* Babeş-Bolyai" University, Cluj-Napoca. Babeş-Bolyai" University, Cluj-Napoca.

Turban. (2005). *Information Technology for Management:Transforming Organizations in the Digital Economy* (5th ed.). John Wiley and Sons, Inc.

US Census Bureau. (2023). *QUARTERLY RETAIL E-COMMERCE SALES.* Retrieved from US Census Bureau News:

Vynokurova, et al., (2020). Hybrid machine learning system for solving fraud detection tasks. *2020 IEEE third international conference on data stream mining and processing (DSMP)* (pp. 1–5). IEEE.

Vyshali-Rao. (2014). ClientAuthorization and Secure Communication in Online Bank Transactions. *International Journal of Scientific and Research Publications, 4*(5), 2250-3153

Wang et al., (2020). Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability. *International Journal of Law Crime and Justice, 64*(1), 1-39.

World Bank. (2018). *Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision.* RetrievedfromWorld Bank: https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial