JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(1), MARCH, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

Credit Card Fraud Detection Using Deep Learning Based on Auto-LSTM Algorithms: A Comprehensive Review

[1]Usman Shehu Musa, [2]Kabiru Ibrahim Musa, [1]Badamasi Imam Ya'u, [1]Abuzairu Ahmad.
[1]*Department of Mathematical Sciences, ATBU, Bauchi*
[2]*Department of Management Information Technology, ATBU, Bauchi*

ABSTRACT
In recent years, credit card fraud has become one of the growing problems. A large financial loss has greatly affected individual person using credit card and also the merchants and banks. It became very rampant and easy mode of payment. People choose online payment and e-shopping; because of time convenience, transport convenience, as a result of huge amount of e-commerce use, there is a vast increment in credit card fraud also. Fraudsters try to misuse the card and transparency of online payments. Thus, to overcome with fraudster's activity become very essential. Charge card extortion can be done from multiple points of view. By lost or taken cards, by delivering phony or fake cards, by cloning the first site, by eradicating or adjusting the attractive strip present at the card which contains the client's data, by phishing, by skimming or by taking information from a dealer's side. With proceeded with headway in fake systems it is critical to create powerful models to battle these fakes in their underlying stage, just before they can take to fruition. Fraud detection involves monitoring the activities of populations of users in order to estimate, perceive or avoid objectionable behavior, which consist of fraud, intrusion, and defaulting. This is a very relevant problem that demands the attention of communities such as machine learning and data science where the solution to this problem can be automated. Our work is based on the basic idea of the deep learning technique to correctly determine whether a transaction pattern is fraudulent or non-fraudulent. The focus is on improving the classification performance in the existing work, using autoencoder-LSTM using credit card datasets obtained from ULB Machine Learning Group. The research scope will be limited to only decision support accuracy measure as an evaluation index while ignoring the computationally capacity of the algorithms as an index for evaluating the quality of the models.

ARTICLE INFO
Article History
Received: August, 2023
Received in revised form: December, 2023
Accepted: January, 2024
Published online: March, 2024

KEYWORDS
Deep learning, Credit card, Fraud detection, Auto-LSTM algorithms, K-Nearest Neighbors (KNN), multilayer perceptron (MLP), Logistic regression (LR).

INTRODUCTION

In recent years credit card fraud has become one of the growing problems. A large financial loss has greatly affected individual person using credit card and also the merchants and banks. It became very rampant and easy mode of payment. People choose online payment and e-shopping; because of time convenience, transport convenience, etc. As the result of huge amount of e-commerce use, there is a vast increment in credit card fraud also. Fraudsters try to misuse the card and transparency of online payments (Popat & Chaudhary, 2018). Thus, to overcome with fraudster's activity become very essential. Charge card extortion can be done from multiple points of view. By lost or taken cards, by delivering phony or fake cards, by cloning the first site, by eradicating or adjusting the attractive strip

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(1), MARCH, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

present at the card which contains the client's data, by phishing, by skimming or by taking information from a dealer's side. With proceeded with headway in fake systems it is critical to create powerful models to battle these fakes in their underlying stage just, before they can take to fruition (Vengatesan, Kumar, Yuvraj, Kumar, & Sabnis, 2020).

Statement of the problem

The existing system uses autoencoder to detect fraudulent transaction on credit card. However, the major problem of a regular autoencoder as used in the existing work of (Misra et al., 2020) is that, regular autoencoders are feed forward architecture and thus cannot generate and recall pass sample sequence for a given input distribution thereby suffer from long-term dependency problem (Vincent, 2011) . In addition, regular autoencoder can only take fixed size inputs (Vincent, 2011). Contrary to regular autoencoder, LSTM auto-encoders are explicitly designed to avoid the long-term dependency problem with variable inputs size (Zhao, Feng, Zhao, Yang, & Yan, 2017), remembering information for long periods of time is practically their default behavior and hence they have an advantage over normal auto-encoders. Therefore, credit card datasets are time series univariate data which is probably best modeled as a sequence where the data point at each time step is dependent on the previous data points. As found in the literature (Gensler, Henze, Sick, & Raabe, 2016; Nguyen, Tran, Thomassey, & Hamad, 2021; W. Wei, Wu, & Ma, 2019), to detect irregularities in time series data, LSTM autoencoder is one of the best candidates. Motivated by this advantage, this research will employ Autoencoder- LSTM algorithms to improve on the existing method used for credit card fraud detection.

Aim and Objectives of the Study

The aim of this study is to develop an efficient credit card fraud detection model by adopting and improving on the work of (Misra et al., 2020) by redesigning the regular autoencoder into an autoencoder-LSTM as supported by (Sailusha, Gnaneswar, Ramesh, & Rao, 2020). Following are the Objectives to;

1. Propose fraud pattern detection and classification using deep Autoencoder-LSTM model.
2. Evaluate the detection performance of the developed model against the existing detection approaches autoencoder (AE), K-Nearest Neighbors (KNN), multilayer perceptron (MLP) and logistic regression (LR) using accuracy, precision, recall and F-Measure.

LITERATURE REVIEW

Data Mining Approaches Used in Credit Card Fraud Detection

There are mainly six data mining approaches: classification, clustering, prediction, outlier detection, regression and visualization. These approaches of data mining are how useful in credit card fraud detection is given below in this section (Ngai, Hu, Wong, Chen, & Sun, 2011).

Classification in Data Mining

Classification is very common learning model comes under the data mining techniques. To differentiate various category of object, a model is use called as classification. Classification predicts the labels of object; labels are predefined, unordered and distinct. Classification and prediction both are the method of distinguishing the objects which having the similar features. The application like, detection of credit card fraud, healthcare fraud, automobile insurance, corporate fraud, etc. where classification become very useful to detect fraud (West & Bhattacharya, 2016).

Clustering in Data Mining

Clustering is variant of unsupervised classification. In clustering, objects are divided into conceptually meaningful groups called cluster. In same cluster, the objects are very similar to each other in terms of feature. While dissimilar objects are not become the part of that cluster; it transfers to another cluster (group of objects) (Yue, Wu, Wang, Li, & Chu, 2007). Cluster Analysis in Data Mining means that to find

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

out the group of objects which are similar to each other in the group but are different from the object in other groups (Carneiro, Dias, Da Cunha, & Mialaret, 2015). In the process of clustering in data analytics, the sets of data are divided into groups or classes based on data similarity. Then each of these classes is labeled according to their data types (Bansal, Sharma, & Goel, 2017). There are many uses of Data clustering analysis such as image processing, data analysis, pattern recognition, market research and many more (Ali & Kadhum, 2017). Using Data clustering, companies can discover new groups in the database of customers. They can also classify the existing customer base into distinct groups depending on the patterns of their purchases. Classification of data can also be done based on patterns of purchasing.

Prediction in Data Mining

Prediction is use to predict the continuous value. Based on the historic data, it makes patterns, estimates the numeric, and ordered value for future. As per the study author stated that, predicted values are continuous value rather than discrete value (Mining, 2006). "Prediction" refers to the output of an algorithm after it has been trained on a historical dataset and applied to new data when forecasting the likelihood of a particular outcome, such as whether or not a customer will churn in 30 days (C.-P. Wei & Chiu, 2002). The algorithm will generate probable values for an unknown variable for each record in the new data, allowing the model builder to identify what that value will most likely be (Saias, Rato, & Gonçalves, 2022).

The word "prediction" can be misleading. In some cases, it really does mean that you are predicting a future outcome, such as when you're using machine learning to determine the next best action in a marketing campaign. Other times, though, the "prediction" has to do with, for example, whether or not a transaction that already occurred was fraudulent (Voican, 2021). In that case, the transaction already happened, but you're making an educated guess about whether or not it was legitimate, allowing you to take the appropriate action. Machine learning model predictions allow businesses to make highly accurate guesses as to the likely outcomes of a question based on historical data, which can be about all kinds of things – customer churn likelihood, possible fraudulent activity, and more. These provide the business with insights that result in tangible business value (Dal Pozzolo, Caelen, Le Borgne, Waterschoot, & Bontempi, 2014). For example, if a model predicts a customer is likely to churn, the business can target them with specific communications and outreach that will prevent the loss of that customer.

Outlier Detection

Outlier means the data objects that is completely different from whole remaining dataset. Outlier detection means measure that "distance" between the data points and that outlier object. Data points that having different characteristics with compare to reminder of whole dataset are known as outlier (Mining, 2006). Hence, (Mining, 2006) mentioned that outlier detection is very crucial issue in the field of data mining. Outliers are extreme data points that are beyond the expected norms for their type (Singh & Upadhyaya, 2012). This can be a whole data set that is confounding, or extremities of a certain data set. Imagining a standard bell curve, the outliers are the data on the far right and left. These outliers can indicate fraud or some other anomaly you are trying to detect, but they can also be measurement errors, experimental problems, or a novel, one-off blip (Rousseeuw & Hubert, 2011). Basically, it refers to a data point or set of data points that diverge dramatically from expected samples and patterns. There are two types of outliers, multivariate and univariate. Univariate outliers are a data point that is extreme for one variable. A multivariate outlier is a combination of unusual data points, including at least two data points (Leys, Delacre, Mora, Lakens, & Ley, 2019).

Regression Method

Regression shows the relationship between more than one dependent and

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

independent variable. Regression is one of the best statistical methods. Hence, for several empirical studies regression is like a benchmark (Mining, 2006). Regression captures the correlation between variables observed in a data set and quantifies whether those correlations are statistically significant or not. The two basic types of regression are simple linear regression and multiple linear regressions, although there are non-linear regression methods for more complicated data and analysis (Nathans, Oswald, & Nimon, 2012). Simple linear regression uses one independent variable to explain or predict the outcome of the dependent variable Y, while multiple linear regression uses two or more independent variables to predict the outcome (while holding all others constant) (Hafemeister & Satija, 2019). Regression can help finance and investment professionals as well as professionals in other businesses. Regression can also help predict sales for a company based on weather, previous sales, GDP growth, or other types of conditions (Darlington & Hayes, 2016)

Review of Related Literature

Multiple Supervised and Semi-Supervised machine learning techniques are used for fraud detection. New methods for credit card fraud detection with a lot of research methods and several fraud detection techniques with a special interest in the neural networks, data mining, and distributed data mining. Many other techniques are used to detect such credit card fraud. When done the literature survey on various methods of credit card fraud detection, we can conclude that to detect credit card fraud there are many other approaches in Machine Learning itself. For example, (Awoyemi et al., 2017) compare the Performance of Naive bayes, K-nearest neighbor and logistic regression on highly skewed credit card fraud data. The results show that K-nearest neighbor performs better than naïve bayes and logistic regression. However, the study can be extended to achieve great results by examining meta-classifiers and Meta learning approaches in handling highly imbalanced credit card fraud data. A further comparative performance of ten different machine learning algorithms, done on a credit card fraud detection application was proposed by (Rajora et al., 2018). The investigations used datasets with “Time” and without “Time” attributes in addition to preparing the dataset suitable for feeding into the machine learning algorithms by using the method of under sampling. The Linear Regression has the better performances than that given by the others. However, this research fails to address the data imbalance. More so, the performance of Decision tree, Random Forest, SVM and logistic regression on highly skewed credit card fraud data was evaluated by (Campus, 2018) for credit card fraud detection to find the most suitable algorithm to solve the problem. It was observed that Random Forest performed better than Logistic Regression, SVM and Decision Tree. However, the research fails to address more preprocessing on data that will make SVM better.

Additionally, (Dighe, Patil, & Kokate, 2018) compare Four classifiers based on different machine learning techniques are trained and the corresponding results are obtained which are compared based on accuracy metrics. It was observed that the KNN perform better than other Algorithms. However, the paper fails to address hybrid approach for better result. Similarly, (Varmedja, Karanovic, Sladojevic, Arsenovic, & Anderla, 2019) analyze various machine learning algorithms, such as Logistic Regression (LR), Random Forest (RF), Naïve Bayes (NB) and Multilayer Perceptron (MLP) in order to determine which algorithm is most suitable for credit card fraud detection. SMOTE technique was used for oversampling. Further, feature selection was performed and dataset was split into two parts, training data and test data. Random Forest algorithm gives the best Results compare to other techniques. Further, it was observed that better result can be achieved by applying genetic algorithms, and different types of stacked classifiers, alongside with extensive feature selection. Similarly, (Shukur & Kurnaz, 2019) implement 3 different machine learning models in order to classify, to the highest possible degree of accuracy, credit card fraud from a dataset. Data

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

processing techniques were used to check the patterns and characteristics of suspicious and non-suspicious transactions supported normalized and anomalies knowledge. Results show that Isolation model is the best compare to other models.

Table 1: Summary of Related Work

Authors	Proposed solution	Findings	Weakness
(Awoyemi et al., 2017)	Performance of Naive bayes, K-nearest neighbor and logistic regression on highly skewed credit card fraud data.	Shows that K-nearest neighbor performs better than naïve bayes and logistic regression.	Fail to examining meta-classifiers and meta learning approaches in handling highly imbalanced credit card fraud data.
(Rajora et al., 2018)	The investigations used datasets with "Time" and without "Time" attributes in addition to preparing the dataset suitable for feeding into the machine learning algorithms by using the method of under sampling.	LR has the better performances than that given by the others.	This paper fails to address the data imbalance.
(Campus et al, 2018)	Survey was conducted to compare different credit card fraud detection algorithm to find the most suitable algorithm to solve the problem.	Random Forest performs better than Logistic Regression, SVM and Decision Tree.	This paper fails to address more preprocessing on data that will make SVM better.
(Dighe et al., 2018)	Four classifiers based on different machine learning techniques are trained and the corresponding results are obtained which are compared based on accuracy metrics.	KNN perform better than other Algorithms.	The paper fails to employ hybrid approach for better result.
(Dhankhad et al., 2018)	Many Machine Learning algorithms to implement a super classifier using ensemble learning methods and identify the most important variables that may lead to higher accuracy in credit card fraudulent transaction detection.	Stacking Classifier perform better than other compared algorithms.	The paper fails to use voting classifier and check the performance with other ML learning methods, increase the size of training and testing dataset.
(Shirgave et al., 2019)	Supervised learning technique Random Forest was selected to classify the alert as fraudulent or authorized and classifier will be trained using feedback and delayed supervised sample to aggregate each probability to detect alerts.	The result showed that Random Forest algorithm showed better accuracy and precision than other techniques.	The paper failed to apply semi-supervised learning methods for classification of alert in FDS.
(Maniraj et al., 2019)	Latest machine learning algorithms are used to detect anomalous activities, called outliers.	The result shows that the Isolation Forest algorithm is the best	Failed to reach out goal of 100% accuracy in fraud detection.

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

		compare to the other algorithms.	
(Puh & Brkić, 2019)	Performance evaluation of the tree machine learning algorithms in detecting fraud in real-life data containing credit card transaction	Programming code is written in python programming language and Scikit learn Implementation was used.	The paper fails to investigate incremental learning on more realistic dataset.
(Shukur & Kurnaz, 2019)	Data processing techniques were used to check the patterns and characteristics of suspicious and non-suspicious transactions supported normalized and anomalies knowledge	Isolation model is the best compare to other models.	The paper fails to apply random forest model as a best classifier.

Comparative Analysis of Related work by Performance Metric

This section enumerated a comparison of different machine learning algorithms for detecting credit card fraud and the respective results achieved in each study. The Table below presents the performance analysis of existing literature in chronological order, authors, proposed algorithm used, Datasets, Accuracy, Precision, Recall, F-Score, AUC, MAE and RMSE of each research paper that have been reviewed. Furthermore, an overview of the performance metric is presented in preceding section for better understanding and evaluation purposes.

Table 2: Performance Analysis of Existing Literature

Source	Proposed ML algorithms	Datasets	Precision (%)	Recall (%)	F1-score (%)	Accuracy (%)	Detection speed	Optimization
(Dornadula & Geetha, 2019)	logistic regression	European credit card fraud dataset.	90.7	99	78	99	Low	Nil
/(Awoyemi et al., 2017)	K-NN	European cardholders' dataset.	97.92	Nil	Nil	100	Low	Nil
(Rajora et al., 2018)	Logistic Regression	European cardholders	95	94	94	93.9	High	Nil
(Campus, 2018)	Random Forest	European cardholders	99.7	Nil	Nil	98.6	High	Nil
(Dighe et al., 2018)	K-NN	European cardholder	Nil	Nil	Nil	99.13	Nil	Nil
(Dhankhad et al., 2018)	Stacking Classifier	Real World Dataset	95	95	95	95.270	High	Nil

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

(Shirgave et al., 2019)	Random Forest		99.7	Nil	Nil	96.2	High	Nil
(Shukur & Kurnaz, 2019)	Isolation Forest	Dataset gathered in Europe in 2 days in September 2013	Nil	Nil	Nil	0.99.7	Nil	Nil
(Varmedja et al., 2019)	Random Forest	European card holders Dataset	96.38	81.63	Nil	99.96	Nil	Nil
(Vengatesan et al., 2020)	K-NN	Not reported	95	72	82	Nil	Nil	Nil
(Sadineni, 2020)	Decision Tree	Kaggle data repository	84.98	Nil	Nil	98.47	Nil	Nil
(Khatri et al., 2020)	Decision Tree	European Card Holders	85.11	Nil	Nil	Nil	Nil	Nil

Discussion and Research Gap

To analyze clearly the performance achieved by each algorithm proposed in the literature for credit card fraud detection, a comparative graph is plotted below to enable the reader clearly understand how the trend in performance continues. Based on the review, it is clear that machine learning has shown to achieve promising results. From Figure 4, it is quite obvious that the KNN classifier proposed in (Awoyemi et al., 2017) achieved the best performance in terms of accuracy with an accuracy of 100% so far. However, for precision and recall, the random forest Classifier and logistic regression achieved the best precision and recall when compare to all the other classifiers value with an average precision and recall of 98.7% and 99% respectively (see Table 2). Furthermore, for F-Score the Stacking Classifier algorithms were the better with an average F-score of 95% respectively (see Table 2).

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(1), MARCH, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

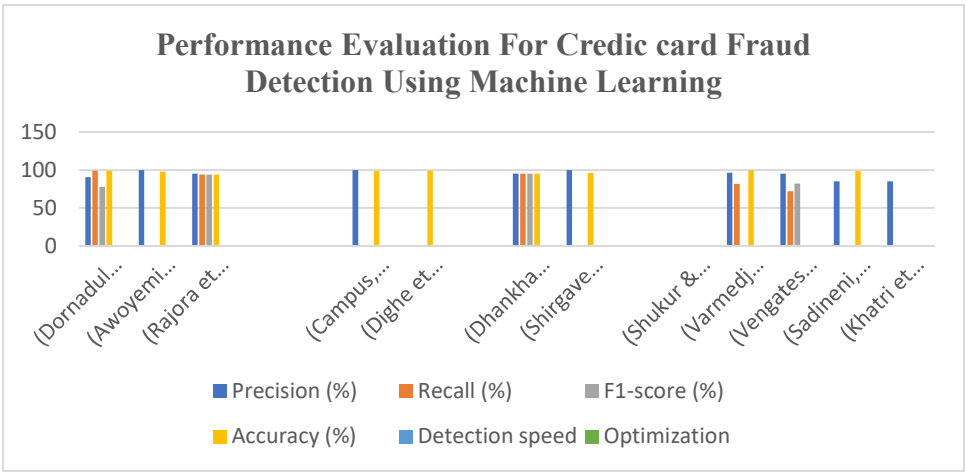

Figure 1: Performance Comparison of different Machine Learning Algorithms for Credit Card Fraud Detection
Source: (Awoyemi et al., 2017)

On average, the KNN algorithms have shown to performed better that all the other algorithms used in this context both in terms of accuracy (100%) and precision (97.92%), thereby making it state of the art machine learning algorithm applied in this context. This is because KNN has some potential benefits as follows: (I) Classification can be easily implemented (II) It is robust to noisy training data; (III) It is appropriate for the large training data. However, it also has a number of drawbacks such as: (I) The selection of K value, which influence on the performance of KNN. (II) The requirements of distance computation for those k neighbors making it computationally expensive. (III) Accuracy degradation in case of multidimensional datasets (Ayyad, Saleh, & Labib, 2019). Despite the promising results demonstrated by KNN, the high computational cost is one of the major drawbacks of this algorithms as stated earlier. This requires significant approach to bridge this gap. In general, enhancing a model performance can be challenging at times. Thus, the need for exploitation of more robust machine learning approaches to improve on the aforementioned performance of the existing approach. This can be achieved in the future studies via the following techniques. Firstly, more datasets can be included in the study to have a wider angle and more variety in the inputs which will be reflected to have a better estimation and more accurate results. Moreover, some other ML algorithms can be tested and involved in upcoming studies in order to cover all available machine learning methods (Jukic et al., 2020). This include considering the exploitation of other robust machine learning classifiers such as support vector machine, modified k-Nearest Neighbors and Multi layered perceptron and deep learning algorithms (Dornadula & Geetha, 2019) which are still yet to be explored in this context.

Feature engineering helps to extract more information from existing data. New information is extracted in terms of new features. These features may have a higher ability to explain the variance in the training data. Thus, giving improved model accuracy and reduces the computational cost of the existing algorithms (Zheng & Casari, 2018). Similarly, PCA helps to represent training data into lower dimensional spaces, but still characterize the inherent relationships in the data. It is a type of dimensionality reduction technique that can also be utilized in this context to improve the classification accuracy. Furthermore, there are various robust methods that can further be exploit to reduce the dimensions (features) of training data like factor analysis, low variance, higher

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

correlation, backward/ forward feature selection and others.

Finally, machine learning algorithms are driven by parameters. These parameters majorly influence the outcome of learning process. The objective of parameter tuning is to find the optimum value for each parameter to improve the accuracy of the model (Wang, Xu, & He, 2016). To tune these parameters, one must have a good understanding of these meaning and their individual impact on model. You can repeat this process with a number of well performing models. For example: In random forest, we have various parameters like max_features, number_trees, random_state, oob_score and others. Intuitive optimization of these parameter values will result in better and more accurate models.

METHODOLOGY

The Proposed System

The main aim of this research is to classify the transactions that have both the fraud and non-fraud transactions in the dataset using machine learning algorithms. Then these algorithms are compared to choose the algorithm that best detects the credit card fraud transactions more efficiently. The process flow for the credit fraud detection problem is depicted in the preceding section.

Analysis of the Existing System

The existing work (Misra et al., 2020) aims to build a methodology that learns the meaningful transaction attributes using an autoencoder which are subsequently utilized in classification., at the first stage of the proposed model an autoencoder is used to transform the transaction attributes to a feature vector of lower dimension. The feature vector thus obtained is used as the input to a classifier at the second stage. Experiment is done on a benchmarked dataset. It is observed that in terms of F1-measure, proposed two stage model performs better than the systems relying on only classifier and other autoencoder based systems. The methodology can also be tuned so that it can be used for stream data. The architecture of the autoencoder is depicted in Figure 5.

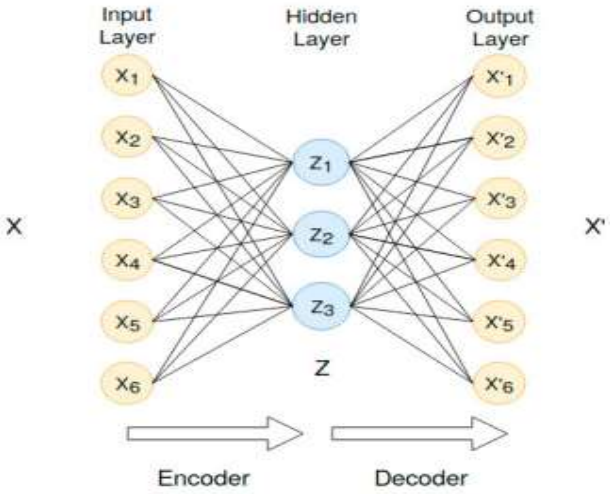

Figure 2: Architecture of Auto-encoder With a Single Encoding Layer and a Single Decoding Layer
Source: (Misra et al., 2020).

Weakness of the Existing System

With the rapid growth in credit card based financial transactions, it has become important to identify the fraudulent ones. However, understanding and learning the complex associations among the transaction attributes is a

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

major problem (Misra et al., 2020). The existing system uses autoencoder to detect fraudulent transaction on credit card as depicted in Figure 3.

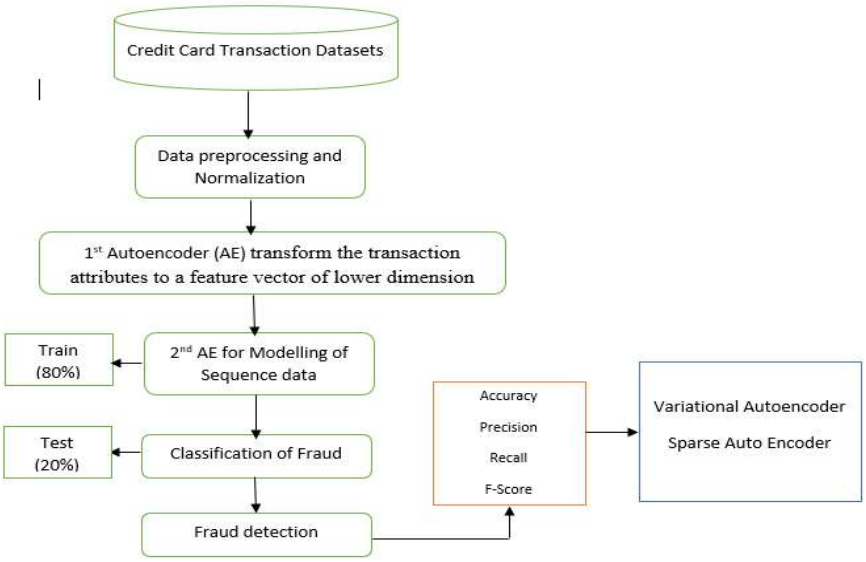

Figure 3: Architecture of the Existing System

At the first stage of the proposed model an autoencoder is used to transform the transaction attributes to a feature vector of lower dimension. The feature vector thus obtained is used as the input to a classifier at the second stage. Experiment is done on a benchmarked dataset. It is observed that in terms of F1-measure, proposed two stage model performs better than the systems relying on only classifier and other autoencoder based systems. However, the major problem of a regular autoencoder as used in the existing work of (Misra et al., 2020) is that, regular autoencoders are feed forward architecture and thus cannot generate and recall pass sample sequence for a given input distribution thereby suffer from long-term dependency problem. In addition, regular autoencoder can only take fixed size inputs (Vincent, 2011). However, LSTM auto-encoders are explicitly designed to avoid the long-term dependency problem with variable inputs size (Zhao et al., 2017), remembering information for long periods of time is practically their default behaviour and hence they have an advantage over normal auto-encoders.

Therefore, credit card datasets are time series univariate data which is probably best modeled as a sequence where the data point at each time step is dependent on the previous data points. As seen in the literature (Gensler et al., 2016; Nguyen et al., 2021; W. Wei et al., 2019), to detect irregularities in time series data, LSTM autoencoder is one of the best candidates. Motivated by this advantage, this research will employ Autoencoder- LSTM algorithms to improve on the existing method used for credit card fraud detection.

Architecture of the proposed method

Figure 8 illustrates the flowchart of the proposed framework. Primarily, the first step of the framework involves the data set and a preprocessing layer.

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(1), MARCH, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

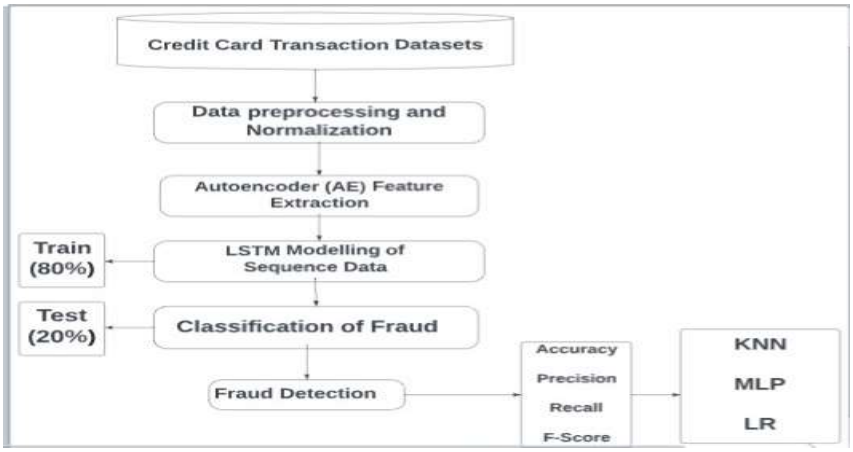

Figure 4: The Proposed Credit Card Fraud Detection Model

Data Preprocessing and Normalization

The first part of the entire strategy is the dataset stage, which reads all the defined dataset. Different operations are executed on the datasets including connecting to the database that includes dataset loading and reading files. The min max normalization strategy was employed to normalize the data. The proposed strategy has been examined on well-known credit card fraud benchmark datasets to ensure the reliability of our proposed strategy.

First Stage Auto Encoder for Feature Engineering

Autoencoders are a specific category of feed-forward neural networks that are used to learn efficient encodings of the training data. An autoencoder network has the same input and output dimensions; it transforms the input to a hidden representation, having a different dimension than the input (and output) dimension, and then reconstruct the input from this hidden representation. It tries to learn the function $f_\theta(X) = X$ for an input X, where θ denotes the function parameters to be learned. In other words, it tries to approximate the identity function, which can be done trivially, but by placing constraints on the network, such as by limiting the number of hidden units, the trivial solution can be eliminated.

An autoencoder has two parts - an Encoder and Decoder. For an under complete autoencoder dim (Z) ≤ dim(X) always holds, where dim(X) denotes the dimensional of X. Also, since X' is a reconstruction of X, dim(X') = dim(X) holds. The encoders and decoders are modelled by deep neural network.

•**Encoder:** The encoder maps the input data X into hidden form Z. Let W_φ and B_φ be the weights and biases for the encoder layer, then the hidden form Z can be represented as:

$$Z = f_E(W_\phi \times X + B_\phi)$$

f_E is the Encoder activation function

• **Decoder:** The decoder transforms Z to the reconstruction X' of the original data X. Let W_θ and B_θ be the weights and biases for the encoder layer, then the hidden form Z can be represented as:

$$X' = f_D(W_\theta \times Z + B_\theta)$$

f_D is the Decoder activation function

The activation functions $f_E(.)$ and $f_D(.)$ can be non-linear, and hence an autoencoder is able to detect non-linearly correlated features in the input, which are otherwise hard to detect. The goal of the autoencoder network is to provide a transformed feature vector Z such that reconstructed data X' is close to the original data X. The reconstruction error Δ measures the distance between the reconstructed input from the autoencoder and the original input. In this work, Euclidean distance

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

between X and X' was considered as the reconstruction error, i.e.

$$\Delta(X, X') = \|X - X'\|_2$$

The Long Short-Term Memory (LSTM)

LSTM is a modified network of RNN proposed to learn long-range dependencies across time-varying patterns. Generally, LSTM is a second order recurrent neural network that solves the vanishing and exploding gradients issue by replacing RNN simple units with the memory blocks in recurrent hidden layer. This network is one of the recurrent neural networks (RNN), which helps in classification and regression problems. A LSTM network's key elements are an input sequence layer and an LSTM layer. A sequence input layer enters information in the network in sequence or time series. Long-term dependence between time steps of sequence information is learned by an LSTM layer. The architecture of the LSTM layer adopted in this research work is presented in the Fig. 5.

Figure 5: Architecture of the LSTM Network

The network starts with an input layer of a sequence followed by a layer of LSTM. The network finishes with a fully linked layer, a SoftMax layer, and an output classification layer to predict class labels of the credit card fraud data.

Evaluation Metric

Accuracy: These performance metric deals with the correct prediction made by the model and this metric can be expressed as:

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN} \quad \ldots(4)$$

Precision: precisions provide information about how precise/accurate your model is out of those predicted positives, how many of them actual positives are. Precisions are a good measure to determine when cost of false positives is high. It is mathematically expressed as:

$$\text{Precision} = \frac{TP}{TP+FP} \quad \ldots(5)$$

Recall attempts to answer what proportion of actual positives was identified correctly. It is expressed mathematically as

$$\text{Recall} = \frac{TP}{TP+FN} \quad \ldots(6)$$

F-Measure is a function of precision and recall, it might be better to use when we seek to balance between precision and recall and there is an even class distribution (large number of actual negatives). It is mathematically express as:

$$F1 = 2^* \frac{Precision*Recall}{Precision+Re} \quad \ldots(7)$$

Where TP (True Positive) = Are the cases when the actual class of the data point was 1 (true) and the predicted is also 1 (true).
TN (True Negative) = Are the cases when the actual class of the data point was 0 (false) and the predicted is also 0 (false).
FP (False Positive) = Are the cases when the actual class of the data point was 0 (false) and the predicted is 1 (true).
FN (False Negative) = Are the cases when the actual class of the data point was 1 (true) and the predicted is 0 (false).

Implementation of the System

The developed deep LSTM classifier model will be implemented using MATLAB R2021a. The computer to be used is a Dell laptop running on Windows 10 Operating System with 8GB RAM and Pentium ® Core i7 processor.

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

Data Collection

In this research, credit card transaction dataset from ULB Machine Learning Group (Akande, Misra, Akande, Oluranti, & Damasevicius, 2021) is used, which was downloaded from Kaggle repository portal. It contains credit card transactions made by cardholders in Europe in 2013. The dataset has a total of 284, 807 transactions, and the fraudulent ones make up only a meagre 0.172% of the data with 492 such transactions. So, the data is highly imbalanced towards the fraudulent class.

CONCLUSIONS AND FUTURE RESEARCH DIRECTION

This research addresses a new framework based on credit card fraud detection using an auto encoder and LSTM deep recurrent neural network. The proposed credit card fraud detection approach uses AE for feature engineering and LSTM deep recurrent neural network for detecting the credit card fraud efficiently in other to achieved an improve performance. The credit card fraud detection methodology can be simply divided into the data processing stage, feature engineering, LSTM modeling, models training and classification stage.

REFERENCES

Akande, O. N., Misra, S., Akande, H. B., Oluranti, J., & Damasevicius, R. (2021). *A supervised approach to credit card fraud detection using an artificial neural network.* Paper presented at the Applied Informatics: Fourth International Conference, ICAI 2021, Buenos Aires, Argentina, October 28–30, 2021, Proceedings 4.

Ali, H. H., & Kadhum, L. E. (2017). K-means clustering algorithm applications in data mining and pattern recognition. *International Journal of Science and Research (IJSR), 6*(8), 1577-1584.

Alsamiri, J., & Alsubhi, K. (2019). Internet of Things cyber attacks detection using machine learning. *Int. J. Adv. Comput. Sci. Appl, 10*(12), 627-634.

Auger, S. D., Jacobs, B. M., Dobson, R., Marshall, C. R., & Noyce, A. J. (2021). Big data, machine learning and artificial intelligence: a neurologist's guide. *Practical Neurology, 21*(1), 4-11.

Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). *Credit card fraud detection using machine learning techniques: A comparative analysis.* Paper presented at the 2017 international conference on computing networking and informatics (ICCNI).

Ayyad, S. M., Saleh, A. I., & Labib, L. M. (2019). Gene expression cancer classification using modified K-Nearest Neighbors technique. *Biosystems, 176*, 41-51.

Bansal, A., Sharma, M., & Goel, S. (2017). Improved k-mean clustering algorithm for prediction analysis using classification technique in data mining. *International Journal of Computer Applications, 157*(6), 0975-8887.

Bre, F., Gimenez, J. M., & Fachinotti, V. D. (2018). Prediction of wind pressure coefficients on building surfaces using artificial neural networks. *Energy and Buildings, 158*, 1429-1441.

Campus, K. (2018). Credit card fraud detection using machine learning models and collating machine learning models. *International Journal of Pure and Applied Mathematics, 118*(20), 825-838.

Carneiro, E. M., Dias, L. A. V., Da Cunha, A. M., & Mialaret, L. F. S. (2015). *Cluster analysis and artificial neural networks: A case study in credit card fraud detection.* Paper presented at the 2015 12th International Conference on Information Technology-New Generations.

Cunningham, P., Cord, M., & Delany, S. J. (2008). Supervised learning *Machine learning techniques for multimedia* (pp. 21-49): Springer.

Dal Pozzolo, A., Caelen, O., Le Borgne, Y.-A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert systems with applications, 41*(10), 4915-4928.

Corresponding author: Usman Shehu Musa
usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

Darlington, R. B., & Hayes, A. F. (2016). *Regression analysis and linear models: Concepts, applications, and implementation*: Guilford Publications.

Dhankhad, S., Mohammed, E., & Far, B. (2018). *Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study.* Paper presented at the 2018 IEEE international conference on information reuse and integration (IRI).

Dighe, D., Patil, S., & Kokate, S. (2018). *Detection of credit card fraud transactions using machine learning algorithms and neural networks: A comparative study.* Paper presented at the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA).

Dike, H. U., Zhou, Y., Deveerasetty, K. K., & Wu, Q. (2018). *Unsupervised learning based on artificial neural network: A review.* Paper presented at the 2018 IEEE International Conference on Cyborg and Bionic Systems (CBS).

Dornadula, V. N., & Geetha, S. (2019). Credit card fraud detection using machine learning algorithms. *Procedia computer science, 165*, 631-641.

Gajjar, R., & Zaveri, T. (2017). *Defocus blur radius classification using random forest classifier.* Paper presented at the 2017 International Conference on Innovations in Electronics, Signal Processing and Communication (IESC).

Garcıa, J., & Fernández, F. (2015). A comprehensive survey on safe reinforcement learning. *Journal of Machine Learning Research, 16*(1), 1437-1480.

Gensler, A., Henze, J., Sick, B., & Raabe, N. (2016). *Deep Learning for solar power forecasting—An approach using AutoEncoder and LSTM Neural Networks.* Paper presented at the 2016 IEEE international conference on systems, man, and cybernetics (SMC).

Glielmo, A., Husic, B. E., Rodriguez, A., Clementi, C., Noé, F., & Laio, A. (2021). Unsupervised learning methods for molecular simulation data. *Chemical Reviews, 121*(16), 9722-9758.

Hafemeister, C., & Satija, R. (2019). Normalization and variance stabilization of single-cell RNA-seq data using regularized negative binomial regression. *Genome biology, 20*(1), 296.

Hastie, T., Tibshirani, R., & Friedman, J. (2009). Unsupervised learning *The elements of statistical learning* (pp. 485-585): Springer.

Hegde, M., Kepnang, G., Al Mazroei, M., Chavis, J. S., & Watkins, L. (2020). *Identification of Botnet Activity in IoT Network Traffic Using Machine Learning.* Paper presented at the 2020 International Conference on Intelligent Data Science Technologies and Applications (IDSTA).

Jukic, S., Saracevic, M., Subasi, A., & Kevric, J. (2020). Comparison of ensemble machine learning methods for automated classification of focal and non-focal epileptic EEG signals. *Mathematics, 8*(9), 1481.

Khatri, S., Arora, A., & Agrawal, A. P. (2020). *Supervised machine learning algorithms for credit card fraud detection: a comparison.* Paper presented at the 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

Leys, C., Delacre, M., Mora, Y. L., Lakens, D., & Ley, C. (2019). How to classify, detect, and manage univariate and multivariate outliers, with emphasis on pre-registration. *International Review of Social Psychology, 32*(1).

Maniraj, S., Saini, A., Ahmed, S., & Sarkar, S. (2019). Credit card fraud detection using machine learning and data science. *International Journal of Engineering Research and, 8*(09).

Mining, W. I. D. (2006). Data mining: Concepts and techniques. *Morgan Kaufinann, 10*, 559-569.

Misra, S., Thakur, S., Ghosh, M., & Saha, S. K. (2020). An autoencoder based model for detecting fraudulent credit card transaction. *Procedia computer science, 167*, 254-262.

Corresponding author: Usman Shehu Musa
✉ *usmanshehumusa@gmail.com*
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

Nasteski, V. (2017). An overview of the supervised machine learning methods. *Horizons. b, 4*, 51-62.

Nathans, L. L., Oswald, F. L., & Nimon, K. (2012). Interpreting multiple linear regression: a guidebook of variable importance. *Practical assessment, research & evaluation, 17*(9), n9.

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems, 50*(3), 559-569.

Nguyen, H., Tran, K. P., Thomassey, S., & Hamad, M. (2021). Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management. *International Journal of Information Management, 57*, 102282.

Popat, R. R., & Chaudhary, J. (2018). *A survey on credit card fraud detection using machine learning.* Paper presented at the 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI).

Puh, M., & Brkić, L. (2019). *Detecting credit card fraud using selected machine learning algorithms.* Paper presented at the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

Rajora, S., Li, D.-L., Jha, C., Bharill, N., Patel, O. P., Joshi, S., . . . Prasad, M. (2018). *A comparative study of machine learning techniques for credit card fraud detection based on time variance.* Paper presented at the 2018 IEEE Symposium Series on Computational Intelligence (SSCI).

Rousseeuw, P. J., & Hubert, M. (2011). Robust statistics for outlier detection. *Wiley interdisciplinary reviews: Data mining and knowledge discovery, 1*(1), 73-79.

Sadineni, P. K. (2020). *Detection of Fraudulent Transactions in Credit Card using Machine Learning Algorithms.* Paper presented at the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC).

Saias, J., Rato, L., & Gonçalves, T. (2022). An approach to churn prediction for cloud services recommendation and user retention. *Information, 13*(5), 227.

Sailusha, R., Gnaneswar, V., Ramesh, R., & Rao, G. R. (2020). *Credit card fraud detection using machine learning.* Paper presented at the 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS).

Shirgave, S., Awati, C., More, R., & Patil, S. (2019). A Review On Credit Card Fraud Detection Using Machine Learning. *Int. J. Sci. Technol. Res, 8*, 1217-1220.

Shukur, H. A., & Kurnaz, S. (2019). Credit card fraud detection using machine learning methodology. *International Journal of Computer Science and Mobile Computing, 8*(3), 257-260.

Singh, K., & Upadhyaya, S. (2012). Outlier detection: applications and techniques. *International Journal of Computer Science Issues (IJCSI), 9*(1), 307.

Sisodia, D. S., Vishwakarma, S., & Pujahari, A. (2017). *Evaluation of machine learning models for employee churn prediction.* Paper presented at the 2017 International Conference on Inventive Computing and Informatics (ICICI).

Srivastava, S., Sharma, D., & Sharma, P. (2020). Comparing various Machine Learning Techniques for Predicting the Salary Status: EasyChair.

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019). *Real-time credit card fraud detection using machine learning.* Paper presented at the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

Trivedi, N. K., Simaiya, S., Lilhore, U. K., & Sharma, S. K. (2020). An efficient credit card fraud detection model based on machine learning methods. *International Journal of Advanced Science and Technology, 29*(5), 3414-3424.

Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., & Anderla, A. (2019).

Corresponding author: Usman Shehu Musa
✉ usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.

Credit card fraud detection-machine learning methods. Paper presented at the 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH).

Vengatesan, K., Kumar, A., Yuvraj, S., Kumar, V., & Sabnis, S. (2020). Credit card fraud detection using data analytic techniques. *Advances in Mathematics: Scientific Journal, 9*(3), 1185-1196.

Vincent, P. (2011). A connection between score matching and denoising autoencoders. *Neural computation, 23*(7), 1661-1674.

Voican, O. (2021). Credit Card Fraud Detection using Deep Learning Techniques. *Informatica Economica, 25*(1).

Wang, G., Xu, J., & He, B. (2016). *A novel method for tuning configuration parameters of spark based on machine learning.* Paper presented at the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS).

Wei, C.-P., & Chiu, I.-T. (2002). Turning telecommunications call details to churn prediction: a data mining approach. *Expert systems with applications, 23*(2), 103-112.

Wei, W., Wu, H., & Ma, H. (2019). An autoencoder and LSTM-based traffic flow prediction method. *Sensors, 19*(13), 2946.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. *Computers & security, 57*, 47-66.

Whig, P., Gupta, K., Jiwani, N., Kouser, S., & Anand, M. (2022). Adaptive Clinical Treatments and Reinforcement Learning for Automatic Disease diagnosis *AI-Enabled Multiple-Criteria Decision-Making Approaches for Healthcare Management* (pp. 204-221): IGI Global.

Wiering, M. A., & Van Otterlo, M. (2012). Reinforcement learning. *Adaptation, learning, and optimization, 12*(3).

Yue, D., Wu, X., Wang, Y., Li, Y., & Chu, C.-H. (2007). *A review of data mining-based financial fraud detection research.* Paper presented at the 2007 International Conference on Wireless Communications, Networking and Mobile Computing.

Zhao, F., Feng, J., Zhao, J., Yang, W., & Yan, S. (2017). Robust LSTM-autoencoders for face de-occlusion in the wild. *IEEE Transactions on Image Processing, 27*(2), 778-790.

Zheng, A., & Casari, A. (2018). *Feature engineering for machine learning: principles and techniques for data scientists*: " O'Reilly Media, Inc.".

Corresponding author: Usman Shehu Musa
✉ usmanshehumusa@gmail.com
Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi.