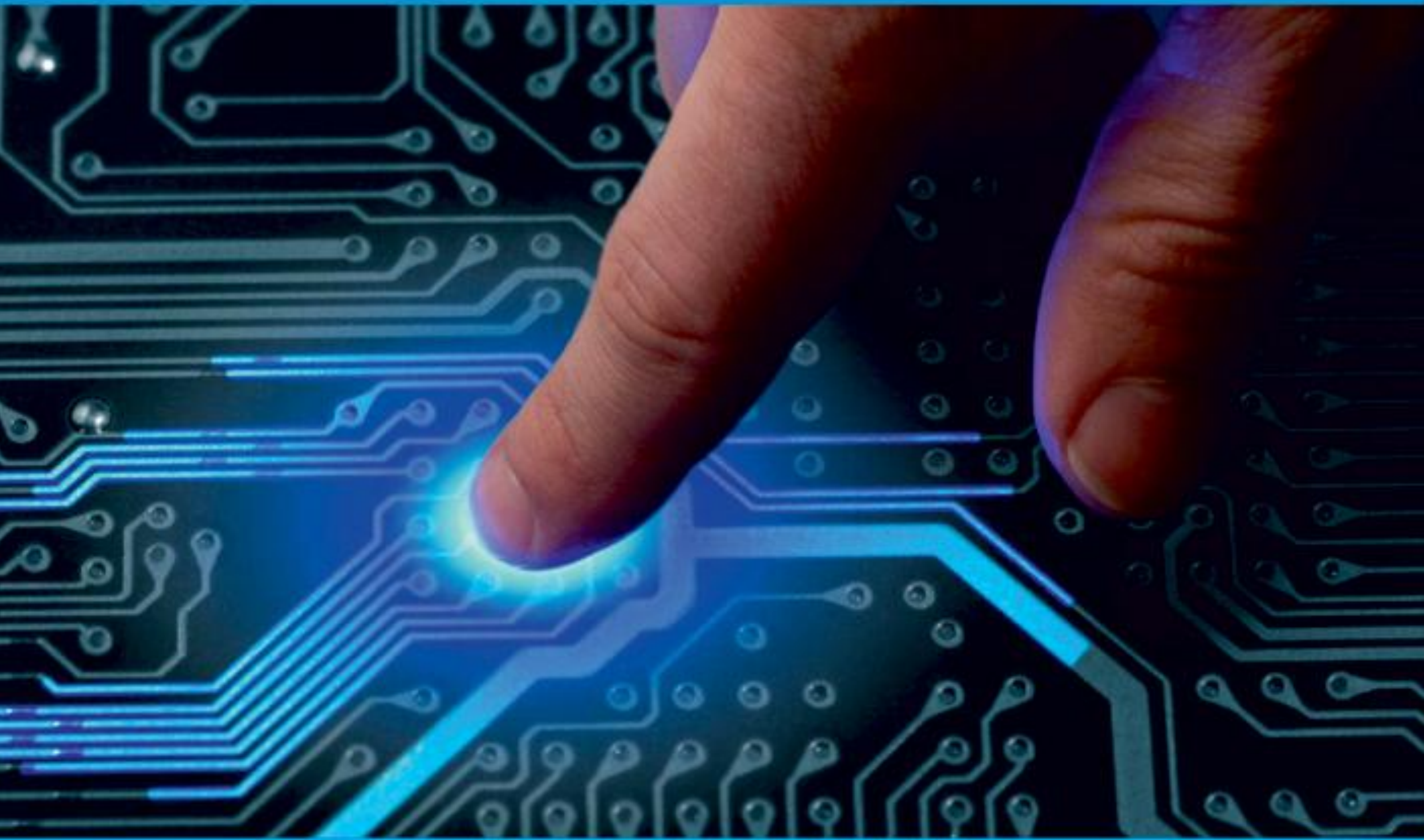
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907038 |

Implementation of Autoencoder for Detecting Credit Card Fradulent System in Neural Networks Using Deep Learning

Dr.P.L. Kishan Kumar Reddy[1], Devisetty Venkata Sai Kathyaeeni[2],Juturi Sirisha[3], Gunduboyina Venkata Naga Rupa[4], Battiprolu Bhavana[5]

[1]Professor, Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India[1]

U.G. Students, Department of Information Technology, Vasireddy Venkatadri Institute of Technology,Nambur, Guntur, Andhra Pradesh, India[2,3,4,5]

ABSTRACT: Credit card fraud occurs when an unauthorized person gains access to the information and uses it to make purchases. There are some ways fraudsters get the information are Lost or stolen credit cards, Skimmingthe credit card, such as at a gas station pump, Hackingthecomputer, calling about fake prizes or wire transfers, Phishing attempts, such as fake emails, looking over the shoulder at checkout, Stealing your mail. Unfortunately, there is no fool-proof way to stop hackers from making such attempts, and fraudsters seem to always find new ways to tap into the information. So, we believe that deep learning algorithms can help better to detect fraudulent transactions. Artificial Neural Networks plays a vital role in handling fraudulent systems. Our objective here is to detect the fraudulent transactions while minimizing the incorrect fraud classifications. Credit Card Fraud Detection is a typical sample of Auto Encoder Neural Network classification. In this process, we have focused on analyzing and pre-processing data sets. This work is implemented in python with autoencoders using keras. The neural networks help detecting fraud credit cards if there is an existence of a greater number of transactions in given dataset by using PCA.

KEYWORDS: credit card fraud detection, deep learning, neural networks, autoencoder, keras, PCA.

I.INTRODUCTION

The Association for Payment Clearing Services (APACS) has estimated that total losses through credit card fraud in the United Kingdom have been growing rapidly from $122 million in 1997 to $440.3 million in 2010. In order to dwindling the fraudulent transactions, we can use many algorithms in any domain, so in this we are implementing an autoencoders for detecting fraud credit cards by using neural networks in deep learning.Banking transactions, such as online transactions, credit card transactions and the mobile wallet, are gaining popularity in recent years. People are shopping more and more by using credit cards. Credit cards have become a necessity, to the virtual world, for digitalized and transactions without a paper copy. Millions of online transactions take place in day-to-day life and all of these transactions are subject to various types of fraud. Fraudulent credit card transaction is still one of problems that faced by companies and in banking sector; it causes them to lose billions of dollars every year. The design of efficient algorithm is one of the most important challenges in this area. This paper aims to propose an efficient approach that detects fraudulent credit card transactions given in the data set using deep learning algorithm called Autoencoders.

Deep learning is a branch of machine learning which is completely based on artificial neural networks, as neural network is going to mimic the human brain so deep learning is also a kind of mimic of human brain. So, we create an artificial structure called an artificial neural net where we have nodes or neurons. Artificial neural networks (ANNs) or connectionist systems are computing systems inspired by the biological neural networks that constitute animal brains. Such systems learn to do tasks by considering examples, generally without task-specific programming. As of 2017, neural networks typically have a few thousand to a few million units and millions of connections. Despite this number being several orders of magnitude less than the number of neurons on a human brain, these networks can perform many tasks at a level beyond that of humans.

An autoencoder is a neural network model that seeks to learn a compressed representation of an input. It is an Unsupervised Machine learning algorithm that applies backpropagation, setting the target values to be equal to the inputs. Autoencoders are used to reduce the size of our inputs into a smaller representation. Autoencoders are a specific type of feedforward neural networks where the input is the same as the output. They compress the input into a lower-dimensional code and then reconstruct the output from this representation. The code is a compact summary or compression of the input, also called the latent-space representation. To build an autoencoder we need 3 things: an encoding method, decoding method, and a loss function to compare the output with the target. The encoder maps from the input to hidden layer, the decoder maps from the hidden layers. to the output layer to reconstruct the inputs. Hidden layers of the autoencoder are low dimensional and nonlinear representation of the input data.

Unsupervised Learning uses machine learning algorithms to analyze and cluster unlabeled data sets. These algorithms discover hidden patterns in data without the need for human intervention. Unsupervised learning models are used for three main tasks: clustering, association and dimensionality reduction

II.LITERATURE REVIEW

Fraud is defined as the unlawful or criminal deception intended to gain financial or personal gain. It is a premeditated conduct against the law, rule, or policy with the intent of obtaining illicit pecuniary profit. Numerous literatures on anomaly or fraud detection in this domain have previously been published and are freely available to the public.

According to a detailed assessment conducted by Clifton Phua and his coworkers, approaches used in this arena include data mining applications, automated fraud detection, and adversarial detection. Unconventional techniques, such as a hybrid data mining/complex network classification algorithm, can detect illicit cases in a real-world card transaction data set, based on a network reconstruction method that allows for the creation of representations of the deviation of one instance from a reference group, these algorithms have proven to be efficient on medium-sized online transactions. Fraud detection is a difficult task, and no system can correctly anticipate any transaction as fraudulent. A good fraud detection system should have the following characteristics:

1. The scams must be correctly identified.
2. Frauds should be detected as soon as possible.
3. A genuine transaction should not be considered fraudulent. Outlier detection is a vital activity since outliers indicate aberrant running conditions that can lead to severe performance deterioration.

There are two types of fraud detection techniques:

1) Supervised procedures in which previous known legitimate/fraud cases are utilized to develop a model that generates a suspicion score for future transactions.
2) Unsupervised transactions are ones in which there are no prior sets and the condition of the transactions is unknown to be fraudulent or lawful.

III.PROPOSED METHOD

Our project's major goal is to make Credit Card Fraud Detection aware to people in order to protect them from credit card online frauds. The primary goal of a credit card fraud detection system is to protect our transactions and security. With this approach, criminals are unable to conduct repeated transactions on a stolen credit card before the cardholder becomes aware of the fraudulent behavior.This model is then utilized to determine whether or not a new transaction is fraudulent. Our goal is to detect 90% of fraudulent transactions while decreasing inaccurate fraud categories.

The following diagram shows the completeArchitecture:

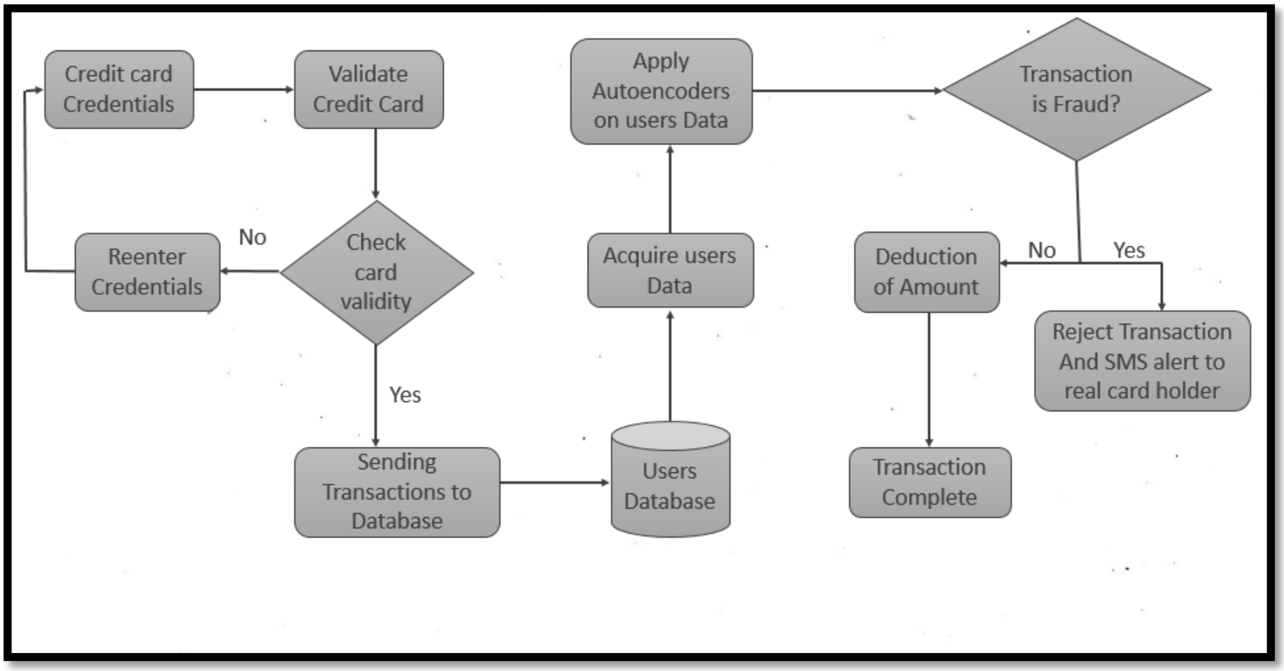


Fig. 1 Architecture Design

There are many methods to enhance accuracy like Adding more data, treating missing and outlier values, Algorithm Tuning, Using many Algorithms. In this, by using dimensionality reduction method called PCA which helps to represent training data into lower dimensional spaces, but still characterize the inherent relationships in the data. There are various methods to reduce the dimensions of training data like factor analysis, low variance, higher correlation, backward or forward feature selection and others.

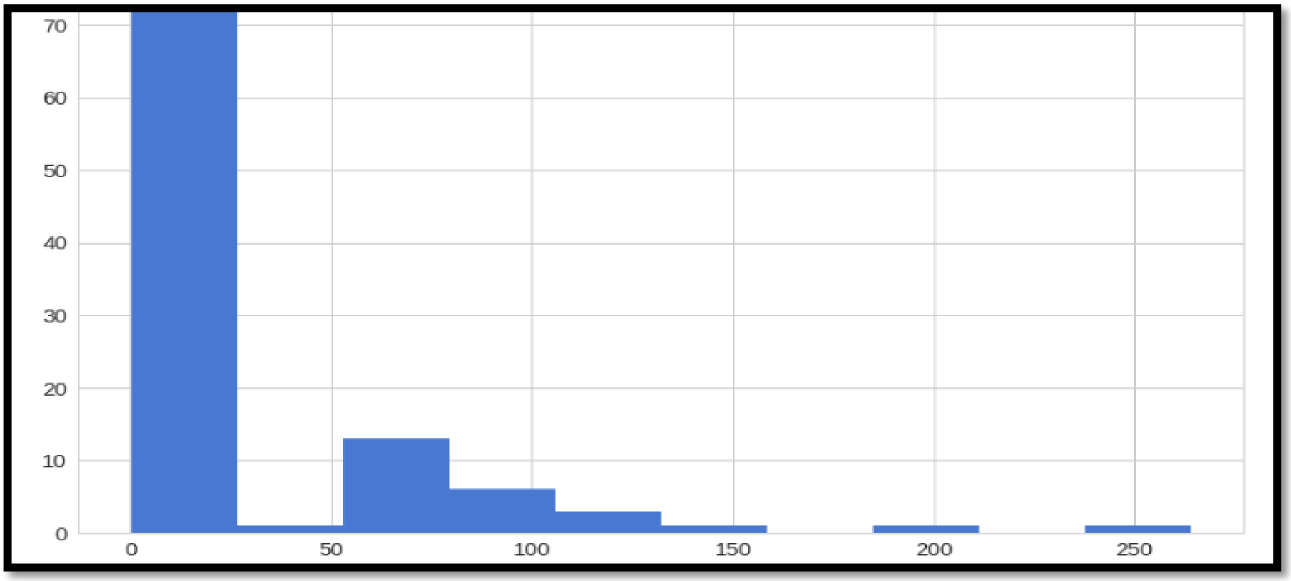


Fig. 2 Reconstruction error with fraud

Reconstruction error is the distance between the original input and its autoencoder reconstruction. Autoencoders compress the input into a lower-dimensional projection and then reconstruct the output from this representation.

IV.RESUTLS

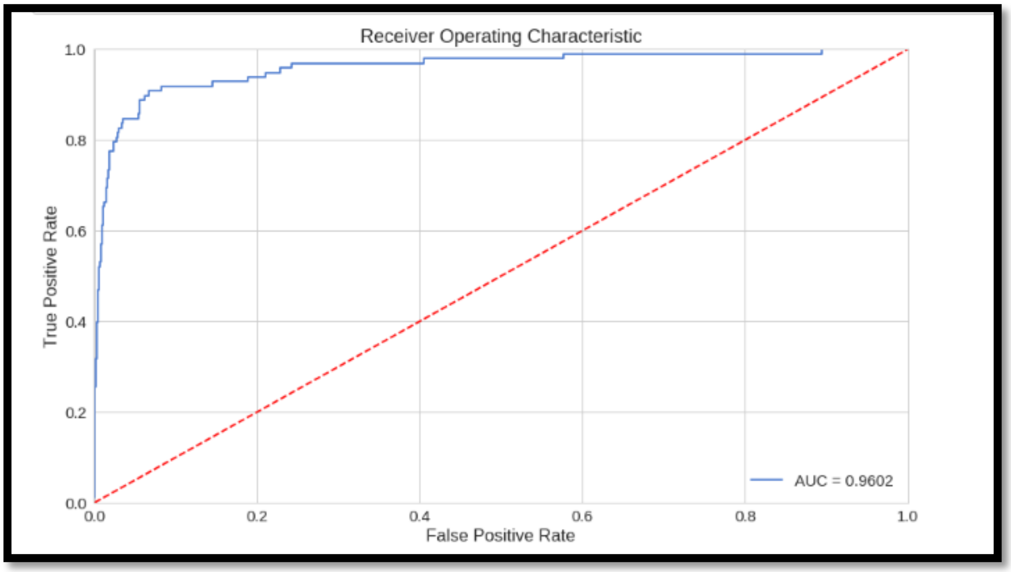


Fig.3 ROC Curve

The above figure depicts the ROC curve of implementation of autoencoder for detecting credit card fraudulent system in neural networks using deep learning.

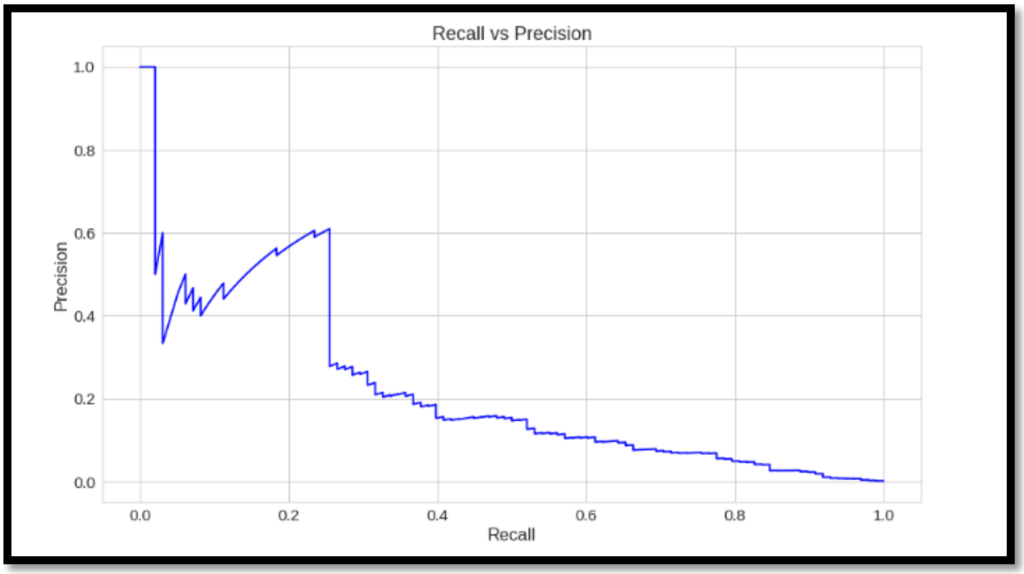


Fig.4 Recall vs Precision

A high area under the curve represents both high recall and high precision, where high precision relates to a low false positive rate, and high recall relates to a low false negative rate. High scores for both show that the classifier is returning accurate results, as well as returning a majority of all positive results.

REFERENCES

[1] Yeh IC, Lien C. The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients. Expert Systems with Applications. 2009;36(2):2473-2480.

[2] West J, Bhattacharya M, Islam R. Intelligent financial fraud detection practices: An investigation. In International Conference on Security and Privacy in Communication Systems. Cham: Springer. 2014; 186-203.

[3] Bhatla PT, Vikram P, Amit D. Understanding credit card frauds. Cards Business Review. 2003;1:6.

[4] Bose I, Wang J. Data mining for detection of financial statement fraud in Chinese Companies. In International joint Conference on e-Commerce, e-Administration, e-Society, and e-Education. International Business Academics Consortium (IBAC) and Knowledge Association of Taiwan (KAT). Taiwan; 2007.

[5] Kirkos E, Spathis C, Manolopoulos Y. Data mining techniques for the detection of fraudulent financial statements. Expert Systems with Applications. 2007;32(4):995-1003.

[6] Ravisankar P, Ravi V, Rao GR, Bose I. Detection of financial statement fraud and feature selection using data mining techniques. Decision Support Systems. 2011;50(2):491-500.

[7] Bhattacharyya S, Jha S, Tharakunnel K. Data mining for credit card fraud: A comparative study. Decision Support Systems. 2011;50(3):602-613.

[8] Pinquet J, Ayuso M, Guillen M. Selection bias and auditing policies for insurance claims. Journal of Risk and Insurance. 2007;74:425-40.

[9] Ngai EWT, Hu Y, Wong YH, Chen Y, Sun X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems. 2011;50(3):559-569.

[10] Chawla NV, Bowyer KW, Hall LO, Philip KPW. SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research. 2002;16:321-357.

[11] A Dal Pozzolo. Adaptive machine learning for credit card fraud detection; 2015.

[12] Zhao X, Zhang J, Qin X. LOMA: A local outlier mining algorithm based on attribute relevance analysis. Expert Systems with Applications. 2017;84:272-280.

[13] Bahnsen AC, Aouada D, Stojanovic A, Ottersten B. Feature engineering strategies for credit card fraud detection. Expert Systems with Applications. 2016;51:134-142.

[14] Van Vlasselaer V, Bravo C, Caelen O, Eliassi-Rad T, Akoglu L, Snoeck M, Baesens B. APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. Decision Support Systems. 2015;75:38-48.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details