SURVEY REPORT FOR IDENTIFYING FRAUD IN CREDIT-CARD USING ARTIFICIALNEURAL NETWORK

S Kavya (1RN20IS126)
Department of ISE, RNSIT
Bengaluru, India

Surabhi K C (1RN20IS167)
Department of ISE, RNSIT
Bengaluru, India

Sangeetha S (1RN20IS134)
Department of ISE, RNSIT
Bengaluru, India

Teena Ronihal (1RN20IS170)
Department of ISE, RNSIT
Bengaluru, India

Mrs. Vinutha G.K
GUIDE
Assistant Professor
Department of ISE, RNSIT
Bengaluru, India

ABSTRACT

In today's world, a lot of our money moves around through credit cards online. But, with more online transactions, there's also a rise in tricky people trying to commit credit-card theft. So, to tackle this problem, We recommend a sophisticated technique for identifying credit card theft that uses really advanced Artificial Intelligence (AI) methods. The main idea is to make the system better at catching fraud, making sure that both regular people and banks feel safe about their money. Our aim is to develop a solution that is user-friendly for anyone and protects your funds against unscrupulous credit card companies.

INTRODUCTION

In recent times, with the continuous evolution of technology credit-cards are currently often used for a range of transactions, leading to a gradual increase in associated frauds. Credit-cards are becoming the go-to method of payment for all types of businesses, big and small, in the modern world. Fraud involving credit cards is common in many industries. including appliances, automobiles, and banking. Despite attempts to identify credit-card fraud using methods like ML and data mining algorithms, the results are not as significant as desired. Therefore, There's pressing need for the growth of more effective and efficient algorithms. Our approach aims to prevent fraud related activities by utilizing artificial neural network algorithms, matching other machine learning algorithms' efficacy with theirs, ensuring a robust defense against potential theft in credit card before transactions are approved.

LITERATURE REVIEW

Numerous scholarly articles and investigations have examined the potential of Artificial-Neural-Networks in the identification of credit card fraud. Below are summaries of a few relatedworks that have employed ANNs in this context.

[1] Title: "A Deep-Neural-NetworkAlgorithm for Detecting Credit Card Fraud"

Authors: Xiaohan, Yu,Xianwei Li,Yiyang, Dong,Ruizhe Zheng

Published:2020

Summary: they suggest a deep network for fraud detection algorithms. To address the data skewness issue in the data set, logarithmic transformation is utilised. To acquaint the network with complex scenarios, add focus loss. Research indicates that our neurological-network-model outperforms other classical models like SVM and logistic regression

[2] Title: "Credit-Card-Fraud-Detection Using Neural Network"
Authors: S. Sudharsan, M. Nandhini, R. Aishwarya, R. Nandhini
Published:2019
Summary: This article introduces a credit card theft algorithm based on neural networks. The authors use feedforward neural networks to classify transactions as correct or incorrect. It specifies the significance of feature selection and optimization techniques to enhance the productivity of neural-network models is discussed.

[3] Title: " Detecting Credit-Card theft by ANN and Logistic Regression"
Authors Y. Sahin,E. Duman
Published:2020
Summary: In this study, To address the issue of credit-card theft, a classification model based on logistic regression (LR) and artificial neural networks (ANN) was created. One of the first studies to examine the effectiveness of LR and ANN approaches for real-world credit card analysis is this one.

[4] Title: "Credit-Card theft Detection using Artificial-Neural-Networks"
Authors: Harsha Sharma, Kamal Kant
Published: 2018
Summary: This project focuses on identifying credit card theft using artificial intelligence. The authors evaluate various neural network topologies and evaluate their performance on data from transactions with credit cards. This study highlights the importance of feature selection and neural networks' capacity to process heterogeneous data.

[5] Title: "A Dual Approach for Credit-Card theft Detection using Neural-Network and Data -Mining Techniques"
Authors:AanchalSahu,Harshvardhan GM,Mahendra Kumar Gourisaria
Published:2020
Summary: In this work, they developed a methodology for identifying theft on credit cards using five classifiers to identify the best classifier for the problem. They employed two distinct techniques to resolve data inconsistencies. The first method uses resampling to boost the quantity of samples in the subgroup, while the second method uses the error of each weighted group.

[6] Title: "Credit-Card Theft Detection Using Autoencoder-Based Deep-Neural Networks"
Authors: Jiatong Shen, Shanghai High School Shanghai
Published:2021
Summary: Here, they developed a credit card theft model using autoencoder-based deep-neural networks. To be accurate and robust, they put two models through training, one running normally and the other illegally.

[7] Title: "Credit-Card theft Prediction And Detection using Artificial-Neural-Network And Self Organizing Maps"
Authors: E. Saraswathi, Prateek Kulkarni, Momin Nawaf Khalil, Shishir Chandra Nigam.
Published:2019
Summary: The approach described using artificial-intelligence and the likelihood of Self organizing map correctly identifying credit card theft is great. Utilising SOM's integrated algorithm as the foundation of our strategy allows us to identify credit card ransomware activity.

PROBLEM STATEMENT

The frequency with which credit card theft occurs presents a substantial challenge to both financial institutions and cardholders. With the

increasing quantity of dealings made with credit-cards, there is a critical need for reliable fraud detection mechanisms. Traditional rule-based systems encounter difficulties in recognizing intricate patterns and adjusting to evolving fraud strategies. Hence, the objective of the undertaking is to create a credit-card theft detection on the basis of ANNs.

OBJECTIVE

Making artificial neural networks (ANNs) that can distinguish between authentic and fraudulent credit card transactions is our goal. The system needs to understand complicated patterns in transaction data and remain informed about new fraudulent tactics. We'll assess the performance of the model by employing measures such as accuracy, repeatability, and F1-score, emphasizing a balance between minimizing incorrect positives and incorrect negatives.

METHODOLOGY

Artificial Neural Networks (ANN)

```
Artificial Neural Network (ANN):
Pseudocode:
The ANN algorithm has two parts: Training part and testing part.
Training part: Def ANN:
Step 1: START
Step2:Loading and observing the dataset
          pd.read.csv(.csv) # reads the dataset
        resampling of data
     StandardScaler() #scaling and normalization of data
Step 3: Data pre-processing
        Train_test_split() #Splitting of data
Step 4: Training the model
        Dense() #Adding data to activation function
 Step 5: Analyzing the model
     Prediction of fraud is made, and this trained data is stored .it can used to test
    takes longer time so it is stored)
Step 6: STOP Testing part:  Def ANN
     It is carried out in a similar way. The only difference is that the stored traine
```

This study aims to educate policymakers to create an effective model for identifying credit-card theft by utilising Artificial Neural Networks (ANNs). The primary focus is on leveraging the power of deep learning to accurately identify fraudulent transactions. The system will be trained on a dataset containing 31 attributes, including information related to customer details, account information, and a binary outcome indicating whether a transaction is fraudulent (1) or not (0). In ANNs, nodes are interconnected, resembling the neural connections found in the brain. The basic structure of an ANN consists of input, hidden, and output layers

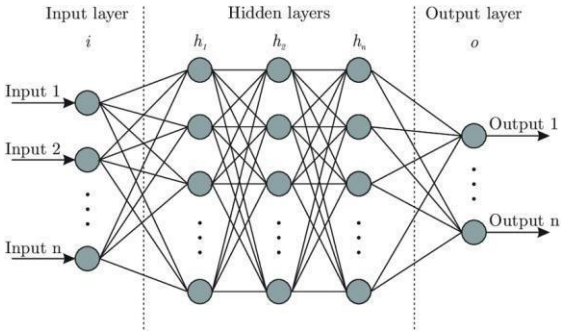

Fig. 1: Architecture of an ANN

1. **Input Layer:**

Number of neurons: Represents the features in dataset (e.g., transaction amount,location, time, etc.)

2. **Hidden Layers:**

Many hidden layers are present to capture complex patterns.

Activation functions: ReLU (Rectified-Linear-Unit) for intermediate layers to introduce non-linearity.

3. **Output Layer:**

Just one neuron to classify binary data (fraud or not fraud).

Activation function: Sigmoid for binary classification.

4. **Neuron Connectivity:**

Completely connected layers for the initial design.

Experiment with different connectivity patterns to optimize the model.

BACK PROPAGATION ALGORITHM

The term back-propagation (BP) is known to be one among the most widely used NN-algorithms After choosing the the network's random weights, the back-propagation algorithm is employed to calculate the necessary corrections.The algorithm can be decomposed in the

Following four steps:

- Feed-forward computation
- Back -propagation to output layer
- Back -propagation to hidden layer
- Weight updates

ADVANTAGES

1) Adaptability and Flexibility: ANNs can understand and adjust to complex patterns in data, making them highly flexible for varioustasks.
2) Non-linearity:Non-linear interactions may be modelled using ANNs, which is crucial for resolving complicated issues when it is difficult to grasp the relationship between input and output.
3) Parallel Processing: ANNs can process multiple inputs simultaneously, enabling parallel processing and speeding up training and prediction times.
4) Generalization: ANNs can generalize well to unseen data which qualifies them for tasks where the model needs to perform well on unseen examples.
5) Robustness: ANNs can handle noisy data and still produce reasonable outputs, making them robust in real-world scenarios.

DISADVANTAGE

1) Computational Intensity: Training ANNs is computationally intensive, requiring powerful hardware, especially for deep neural networks.
2) Data Requirements: ANNs often needs excess amount of labeled data for training, and their performance may suffer if the dataset is unrepresentative.
3) Black Box Nature: The inner workings of ANN s are often considered a "black box", making it difficult to interpret and understand what the decision model is
4) Overfitting: Overfitting is a common challenge in (ANNs), particularly when confronted with limited datasets or overly intricate models
5) Training Time: Training deep neural networkscan take a significant amount of time, especiallyfor large datasets and complex architectures.
6) Hyperparameter Tuning: ANNs typically involve tuning a large number of hyperparameters, such as learning rates, layer sizes, and regularization parameters, which could be time-consuming and require expertise
7) Sensitivity to Initial Conditions: ANNs can besensitive to initial weights and biases, and small changes in these values can lead to different outcomes, requiring careful initialization strategies.

CONCLUSION

In conclusion, the survey utilizing Artificial-Neural-Networks with Backpropagation reveals a landscape of significant advancements and insights. The reviewed studies collectively underscore the efficiency of ANN Backpropagation models in addressing the intricate challenges associated with detecting fraudulent transactions. The diverse datasets employed, sourced from credit card companies and financial entities, and public repositories, have facilitated a comprehensive evaluation of model performance. Assessment of performance metrics, includes accuracy, precision, recall, and AUC-ROC, provides a nuanced understanding of the models' capabilities in distinguishing between legitimateand fraudulent transactions. Despite the progress made, challenges such as imbalanced datasets and the need for robust generalization persist.

REFERENCES

[1] I. Sadgali, N. Sael, F. Benabbou, “Detection of credit-card theft: State of art”, l, Vol.18, No.11, pp.76-83, 2018.

[2] Y.Dai, J.Yan, X.Tang, H.Zhao and M.Guo, “Online Credit Card Theft: A Hybrid

Framework with Big Data Technologies", IEEE, Trustcom/BigDataSE/ISPA, 1644-1652, 2016.

[3] K. Modi, R. Dayma, "Review on theft Detection Methods in Credit-Card Transactions", IEEE, (I2C2'17), 2017.

[4] C. Jiang, J. Song, G. Liu, L. Zheng, W. Luan, Credit card fraud detection: a unique method utilising input and an aggregation strategy mechanism, IEEE Internet Things J.

[[5] K. Chaudhary, B. Mallick, "Credit Card Fraud: The study of its impact and detection techniques", (IJCSN), vol. 1, no. 4, pp. 31-35, 2012, ISSNISSN: 2277-5420

[6] A. A. Taha, S. J. Malebary, "Intelligent stratergy to Credit-Card Theft Identification Using an OLightGBM", IEEE Access (2020), pp. 25579-25587

[7] Hecht-Nielsen, R. (1992). Theory of the backpropagation neural network. In Neural-networks for perception (pp. 65-93). Academic Press.

[8] J. T. S. Quah, and M. Sriganesh, "Real-time credit-card theft identification using computational intelligence," Applications for Expert Systems, vol. 35, pp. 1721–1732, 2008. doi:10.1016/j.eswa.2007.08.093

[9] J. R. Dorronsoro, F. Ginel, C. Sgnchez and C. S. Cruz, "Neural theft identification in credit-card operations," in Networks and Neural Systems Journal, IEEE, vol.8, no.4, pp. 827-834, July 1997.