International Journal for Modern Trends in Science and Technology, 8(02): 275-277, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0802045
Available online at: http://www.ijmtst.com/vol8issue02.html

Fuzzy Logic and Neural Network to Identify and analysis for Credit Card Fraud

Dr S.B.Thorat[1], Dr. P.R. Patil[2], Dr. Anagha K. Joshi[3]

[1]Director, Department of computer science, SSBES ITM College Nanded
suryakant_thorat@yahoo.com
[2]Assistant Professor, Department of computer science, SSBES ITM College Nanded
pritam.itm@gmail.com
[3]Assistant Professor, Department of computer science, SSBES ITM College Nanded
Anagha.k.joshi@gmail.com

To Cite this Article
Dr S.B.Thorat, Dr. P.R. Patil, Dr. Anagha K. Joshi. Fuzzy Logic and Neural Network to Identify and analysis for Credit Card Fraud. International Journal for Modern Trends in Science and Technology 2022, 8, pp. 275-277. https://doi.org/10.46501/IJMTST0802045

Article Info
Received: 20 January 2022; Accepted: 23 February 2022; Published: 26 February 2022

ABSTRACT

In this work, we present a two-phase neuro-fuzzy expert system to identify credit card fraud. In the first phase, a pattern-matching system analyzes incoming transactions. This section includes a fuzzy clustering module and an address matching module, both of which give the transaction a score depending on how much of a departure there is from the norm. A fuzzy inference algorithm then uses the combined values of these scores to determine if the transaction is legitimate, suspicious, or fraudulent. In the second phase, after a suspicious transaction has been identified, a neural network is used that has been trained using historical transactions to determine whether or not the action was fraudulent. Experiments and analysis involving comparisons to existing systems have confirmed the viability of the proposed technology.

Keywords: neuro-fuzzy,credit card fraud,ANN, LSTM

1. INTRODUCTION

Credit cards are now widely used for internet transactions. Simple pattern matching algorithms are insufficient for detecting fraudulent operations. Accurate and efficient fraud detection is essential to ensure minimal false positives. An example of fraudulent behavior is when someone uses another person's account without permission. To commit fraud is to purposefully engage in illegal activity for the purpose of gaining financial gain. Credit card fraud has expanded dramatically, making it crucial to learn how to recognize and report instances of this crime. Anomalies in data or unusual business processes alone are not enough to identify fraud effectively in practice. Recognizing anomalies is difficult and requires sophisticated tools. In most cases, the systems' foundations are the rules and parameters established by knowledgeable researchers. The confluence of millions of monthly purchases makes it hard to check each one individually, making fraud a major concern today. Computerized automation is the only practical answer. Using straightforward statistical methods, computers can determine whether or not a credit card transaction is "suspicious." However, the nature and scope of fraud are both broad and intricate. Therefore, cutting-edge methodologies such as machine learning

are required. In order to achieve more effective automatic systems, this work aims to refine and advance conventional approaches. In 1965, Lofti Zadeh [1] proposed the concept of fuzzy logic, which is the focus of this work. Zero or one can be the result in traditional set theory. However, fuzzy logic emerges from the need to express imprecise and unreliable facts via logical operators. Fuzzy logic's rules are easy to grasp even for someone unfamiliar with the method since they reflect the fuzziness with which most people think. Mallinson and Bentley [2] in 1999 proposed the use of fuzzy rules to achieve both precise and insightful classification. Matlab's fuzzy logic toolbox is used to put into practice the principles of fuzzy logic. There is a comparison between the outcomes of the dataset and those of neural networks trained on the same data.

2. RELATED WORK

Based on the information from the credit card transaction behavior pattern, Yongbin et al. [8] developed a behavior-based credit card fraud detection model. The data was initially processed using a membership function based on fuzzy logic. The data was fed into the SOM algorithm for further processing. The legitimacy of the transaction was determined based on the results generated by SOM. Pasadena, California, USA; April 3 - 6, 2016; SpringSim-CNS © 2016 The International Society for Modeling and Simulation (SCS) Before training the sets with multilayer perceptron (MLP), which mapped the output into fraud or valid transactions, Carneiro et al. [3] performed cluster analysis on an artificial neural network to handle the data (normalize it). The credit card processing sequence was analyzed by Guo et al. [4], who employed a neural network trained on confidence data and validated their results with a receiver operating characteristic (ROC) curve. Using a combination of ANN and a Bayesian Belief Network (BBN), Maes et al. [5] developed an automated approach to detect credit card fraud. The ROC was used to evaluate the efficiency of the fraud detection system. Our method differs from others in that we preprocess the data with a credit card model that learns user habits from past purchases. Next, a membership function is developed in Matlab utilizing fuzzy logic to further categorize the data. We feed the data into our system and check the findings for accuracy. Now there is a third possible outcome in addition to the previously existing legal and fraudulent ones: suspicious. We'll put ANN through its paces, too, and use mean square error (MSE) to compare the two approaches' precision.

3. METHODOLOGY

In order to accurately identify fraudulent, suspect, or authorized credit card transactions, the author of this paper applies fuzzy logic member ship functions. In this study, we present the neuro-fuzzy expert system for credit card fraud detection (NFES_CCFD), which integrates evidences from two separate sources based on several transaction parameters to assess if a user's behavior deviates from his typical spending pattern. Additionally, a NN-based learning process is employed to confirm the suspicious. The following values are extracted from the dataset by the author of the proposed research utilizing fuzzy member ship functions

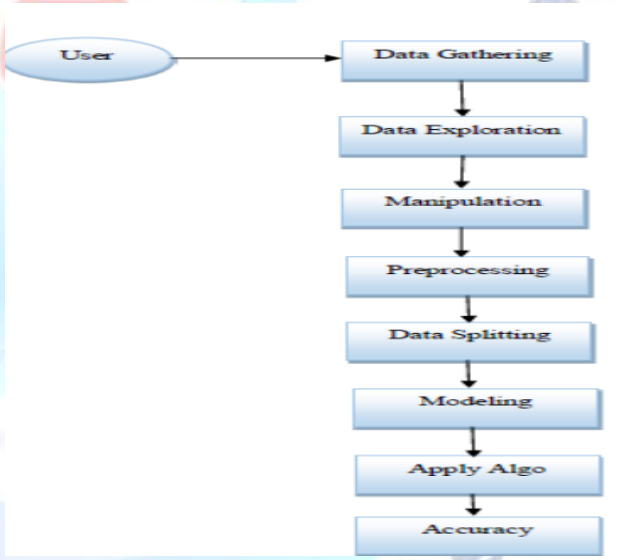

Figure 1: system architecture

1) Time Difference: Using this, we can compare the length of the current transaction to the mean of all transactions from a single user, which is the average transaction time. Transactions days difference under 4 are considered low, and those between 4 and 7 are considered medium, otherwise high.

2) Amount Difference: By using this, we can determine the difference between the amount of the current transaction and the typical transaction. The Base Paper contains the amount range for the fuzzy member.

3) Location: determining if the transaction takes place in Toronto, outside of Toronto, or outside of Canada. If

you're inside Toronto, use LOW or 0; if you're outside, use MEDIMU or 1; otherwise, use HIGH or 2.

Using this, we can determine how many days there are between the current transaction date and the LAST transaction date.

5) Frequency: Using this, we can determine how many transactions occur each day.

After extracting all of the values, we will discover a class that is labeled as fraud if the low values are higher, suspicious if the medium values are higher, and fraud if the high values are higher.

We have code to extract all member values in the screen below. Because LSTM and FUZZY only accept numeric values and not character values, we are using 0 for LOW, 1 for MEDIUM, and 2 for HIGH in this case.

Read the red-colored code comments in the aforementioned screen to learn how to calculate fuzzy member functions. The dataset details utilized in this research are displayed in the screen below.

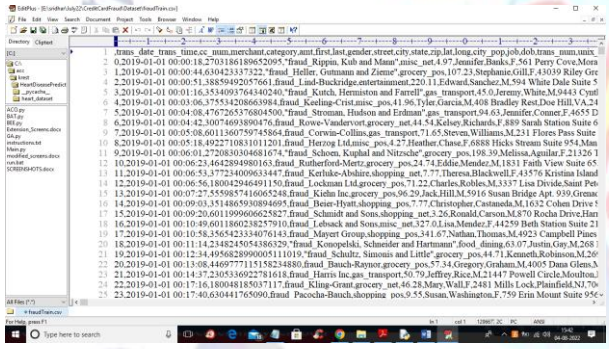

Figure 2: Dataset

4. RESULTS

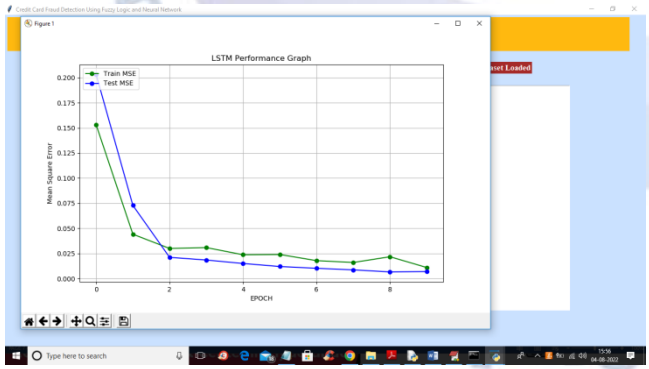

Figure3: Performance of the model

5. CONCLUSION

To reduce computational time and false alarms in credit card fraud detection, accurate and quick computing approaches are needed. Our study tracked credit card usage patterns using a behavior credit card model. The data were preprocessed into relevant attributes, then fuzzy logic membership functions were built for each attribute. Based on input weight, rules were established and prioritized. Our results were verified using ANN. ANN outperformed fuzzy logic by 33%. The mean square error of 0.476 makes fuzzy logic results acceptable. Our system makes decisions using transaction statement data, hence no data preprocessing is needed. We want to implement our solution utilizing real credit card transactions from many users and expand our research area to include big data analysis of everyday transactions.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Zadeh, L.A, B. "Fuzzy sets" in Information and Control, Vol. 8, 1965, pp.338- 353

[2] Mallinson, H. and Bentley, P.J. "Evolving Fuzzy Rules for Pattern Classification" in International Conference on Computational Intelligence for Modelling, Control and Automation - CIMCA'99.Vol. 1, IOS Press,1999, pp. 17- 19

[3] Mineda Carneiro, E.; Vieira Dias, L.A.; Da Cunha, A.M.; Stege Mialaret, L.F., "Cluster Analysis and Artificial Neural Networks: A Case Study in Credit Card Fraud Detection," in Information Technology - New Generations (ITNG), 2015 12th International Conference on , April 2015, pp.122-126, 13-15

[4] Tao Guo; Gui-Yang Li, "Neural data mining for credit card fraud detection," in Machine Learning and Cybernetics, 2008 International Conference on , vol.7, July 2008, pp.3630-3634, 12-15

[5] S. Maes, K. Tuyls, B. Vanschoenwinkel and B. Manderick, "Credit card fraud detection using Bayesian and neural networks," in Proceedings of the First International NAISO Congress on Neuro Fuzzy Technologies, 2002

[6] Tripathi K.K. and Pavaskar M.A. "Survey on Credit Card Fraud Detection Methods" in International Journal of Emerging Technology and Advanced Engineering, 2(11), November 2012

[7] Tej Paul Bhatla, Vikram Prabhu & Amit Dua "Understanding Credit Card Frauds" 2003.

[8] 8.Zhang Yongbin; You Fucheng; Liu HuaQun, "BehaviorBased Credit Card Fraud Detecting Model," in INC, IMS and IDC, 2009. NCM '

[9] Fifth International Joint Conference on, August 2009, pp.855-858, 25-27 9.Hetvi Modi, Shivangi Lakhani, Nimesh Patel and Vaishali Patel, "Fraud Detection in Credit Card System Using Web Mining" in International Journal of Innovative Research in Computer and Communication Engineering, November 2013, pp. 175-179

[10] Nutan Suman, "Review Paper on Credit Card Fraud Detection" in International Journal of Computer Trends and Technology (IJCTT),V4(7), July 2014, pp. 2207-2215