Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.3, May : 2024

CREDIT CARD FRAUD DETECTION USING FUZZY LOGIC AND NEURAL NETWORK

Mrs. Mohana deepti (Facility Guide) Associate professor Dept .of CSE Andhra Loyola Institute of Engineering and Technology Vijayawada, Andhra Pradesh ,India mdeepthi2012@gmail.com
Venu Bandi Computer Science and engineering Andhra Loyola Institute of Engineering and Technology Vijayawada, Andhra Pradesh India Venubandi3060@gmail.com
Vishnuvardhan Reddy Gongati Computer Science and Engineering Andhra Loyola Institute of Engineering and Technology Vijayawada, Andhra Pradesh India
Vishnuvardhanreddyv873@gmail.com

ABSTRACT
The surge in credit card fraud is closely tied to the exponential growth of E-commerce. The sheer volume of transactions poses a significant challenge for banks seeking to minimize losses and for customers yearning for secure transactions. This study employs a fuzzy database to identify instances of credit card fraud. Fraud detection revolves around monitoring user behavior to predict, detect, or prevent undesirable activities. The accurate classification of transactions as lawful or deceptive is treated as a data mining problem. This paper delves into the application of fuzzy logic, exploring fuzzy rules, membership functions, fuzzification, and defuzzification. The proposed method is implemented on a dataset using the fuzzy logic toolbox in Matlab, and the outcomes are compared with those obtained through the artificial neural network (ANN) approach. The results indicate that the ANN method is 33% more accurate than fuzzy logic.

Keywords:
Credit card, Fraud, ANN

I. INTRODUCTION
The popularity of credit card usage for online transactions has soared, necessitating more sophisticated approaches than simple pattern-matching algorithms for detecting fraudulent activities. Effective fraud detection is crucial to ensuring accuracy and minimizing false positives. Fraud is defined as unauthorized activity resulting in financial gain without the account holder's intention.
Given the substantial increase in credit card fraud, understanding the methods for identifying and uncovering such activities is paramount. In real-world scenarios, anomalies in data or operations alone are insufficient for efficient fraud detection. Anomaly detection, a complex task, requires technological assistance, often relying on systems grounded in rules and parameters established by experienced experts in the field.
The enormity of the fraud problem, coupled with millions of transactions monthly, renders manual checking impractical. The only viable solution is automation through computers, enabling the assessment of credit card transactions for potential suspicion using statistical techniques. However, the diversity and complexity of fraudulent activities necessitate advanced approaches like machine learning. This paper aims to enhance and optimize traditional methods, striving for automated systems with increased efficiency.
Focusing on fuzzy logic, introduced by Lofti Zadeh in 1965, this paper explores an alternative to conventional set theory, allowing for output other than just zero or one. The representation of vague and uncertain data through logical operators gave rise to fuzzy logic. Because humans often think in vague terms, fuzzy logic rules are comprehensible even to those unfamiliar with the technique. By employing fuzzy rules, this approach aims to achieve both accurate and intelligent classification, as demonstrated by Mallinson and Bentley in 1999.
The implementation of the fuzzy logic technique utilizes the fuzzy logic toolbox in Matlab. The obtained results from the dataset are then compared with outcomes from the same data using neural networks.

II. LITERARURE SURVY

Yongbin et al. [8] proposed a credit card fraud detection model centered on user behavior patterns in credit card transactions. They employed a fuzzy logic membership function for data preprocessing, with the subsequent results fed into the Self-Organized Map (SOM) algorithm. The SOM output was then used to determine the legitimacy or fraudulence of a transaction.

Carneiro et al. [3] utilized cluster analysis on an artificial neural network for data processing (normalization) before training sets using a multilayer perceptron (MLP), which map the output to identify fraud or legitimate transactions.

Guoet al. [4] focused on processing the sequence of transaction operations using a confidence-based NN. They then employed the receiver operating curve (ROC) for precision and efficacy assessment.

Maes et al. [5] introduced an computerized credit card deception detection using artificial neural network (ANN) and Bayesian Belief Network (BBN). The accuracy of fraud detection was measured using the ROC.

What distinguishes our loom is the preprocessing of data using a behavior-based credit card model that analyzes user behavior based on previous transactions. The data is further clustered by creating membership functions using fuzzy logic in Matlab. To authenticate the results, the data is input into our system, and the output is observed. In contrast to the conventional binary outputs of legal and fraud, our model includes a third output: suspicious. We will assess our results using ANN and compare the accuracy of the two methods using the mean square error (MSE).

III. PROBLEM STATEMENT

EXISTING SYSTEM:

Credit card fraud detection utilizes various techniques, with neural networks (NN), genetic algorithms, data mining, game-theoretic approaches, support vector machines, and meta-learning. The initial method employed in credit card deception detection (CCFD) was the artificial neural network (ANN). Ghosh and Reilly conducted a feasibility study for Mellon Bank, testing the efficacy of ANN in CCFD and achieving a reduction of 20–40% in losses due to fraud [4]. Aleskerov et al. introduced CARDWATCH, an NN-based data mining technique [5]. Dorronsoro et al. presented an online CCFDS using a neural classifier, incorporating Fisher's discriminant analysis to differentiate between fraudulent and normal activities.

PROPOSED SYSTEM:

In this paper, employed Fuzzy Logic membership functions to accurately identify fraud, suspicious, or legal card transactions. The proposed approach involves extracting specific values from the dataset using Fuzzy membership functions. After obtaining all the values, the classification of class labels is determined based on the prevalence of LOW, MEDIUM, or HIGH values. Specifically, the label is assigned as FRAUD if LOW values predominate, as Suspicious if MEDIUM values are more prominent, and as LEGAL if HIGH values are more prevalent.

Below is the code snippet illustrating the extraction of all membership values. Numeric values (0 for LOW, 1 for MEDIUM, and 2 for HIGH) are used, as both LSTM and FUZZY processes only accept numeric inputs, not character values.

In this study, a neuro-fuzzy expert system for credit card fraud detection (NFES_CCFD) is proposed. This system integrates evidence from two different sources, considering various transaction attribute to analyze deviations in a user's behavior from their standard spend profile. Additionally, a learning method on neural networks (NN) is employed to validate suspicious cases.

ADVANTAGES:

Integration of Evidences: NFES_CCFD integrates evidence from two divergent source, leveraging different transaction attributes. This comprehensive approach enhances the system's ability to analyze and detect deviations in a user's behavior, providing a more robust fraud detection mechanism.

Behavioral Analysis: The system focuses on analyze the deviation of a user's deeds from their

standard spending profile. This behavioral analysis allows for a more nuanced and context-aware assessment, improving the accuracy of fraud detection.

Learning Mechanism: Incorporating a learning mechanism based on neural networks (NN) enhances the system's adaptability and effectiveness over time. The NN-based learning allows the system to continuously evolve and improve its ability to identify suspicious cases.

Multi-Level Classification: The proposed system employs a multi-level classification approach, categorizing transactions into FRAUD, Suspicious, or LEGAL based on the prevalence of LOW, MEDIUM, or HIGH values. This adds granularity to the fraud detection process, enabling a more detailed and insightful classification.

Fuzzy Logic Membership Functions: The utilization of Fuzzy Logic membership functions provides a flexible and interpretable framework for handling uncertainty and imprecision in credit card transaction data. This enhances the system's ability to deal with real-world complexities.

Numeric Representation: The use of numeric values (0 for LOW, 1 for MEDIUM, and 2 for HIGH) facilitates compatibility with both LSTM and FUZZY processes. This ensures a seamless integration of different components, promoting efficient data processing and analysis.

Reduction in False Positives: By considering multiple transaction attributes and employing a sophisticated classification approach, the proposed system aims to minimize false positives. This reduction in false alarms contributes to a more reliable and trustworthy credit card fraud detection system.

Adaptability: The system's adaptability to changing patterns and emerging fraud techniques is enhanced through the combination of neuro-fuzzy techniques and NN-based learning. This adaptability is crucial for staying ahead of evolving fraud scenarios in the dynamic landscape of credit card transactions.

IV. RESULTS & DISCUSSION

The credit card operation account obtain from the bank encompasses crucial details concerning the transaction and user. To determine the legitimacy, suspicion, or fraudulent nature of a transaction, it is imperative for banks to track the history of transactions for a specific user in conjunction with the new transaction. The acquisition of this information is fundamental to the detection process. This section delineates the pre-processing and preparation of data, elucidates the detection algorithms employed, and subsequently verifies the results.

Data Preprocess Algorithm:

The unusual credit card transaction data from the bank includes transaction date, amount, and location (set a). These data are represented as xi={date, amount, location}, where xi∈a. To craft an helpful credit card fraud revealing system, the usage prototype of the credit card must be monitored [6]. The observation of historical data aids in detecting fraudulent transactions, considering any deviation from the average historical pattern as suspicious.

To achieve this, the historical data of past transactions is incorporated into the data feed into the planned system. The subsequent parameters are calculated: I. Average transaction time in hours II. Date of the last transaction in days III. Frequency of transactions per day IV. Average transaction amount V. Average transaction location

The resultant dataset (set B) is then represented as xi={time, interval, frequency, amount, location}, where xi∈B. Subsequently, membership functions are created using the fuzzy logic toolbox in Matlab.

Fuzzy Logic Algorithm:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.3, May : 2024

i. Five inputs: time, amount, location, interval, and frequency of credit card transactions.

ii. Output: Credit card classification presented in linguistic terms.

iii. Each input possesses fuzzy variables.

iv. Each fuzzy variable is associated with a membership function.

v. The membership function is calculated for each fuzzy variable.

vi. The strength of rules is calculated based on the membership function of the fuzzy variable.

vii. Credit card classification is determined by selecting the maximum output set as the final result.

V. RESULT FOR PROPOSED SYSTEM

After execute both planned algorithms, the outcome were assessed by evaluating the point to which they line up with the predicted output. Figure 1 illustrates the optimal performance achieved by the Artificial Neural Network (ANN) algorithm after 12 iterations.

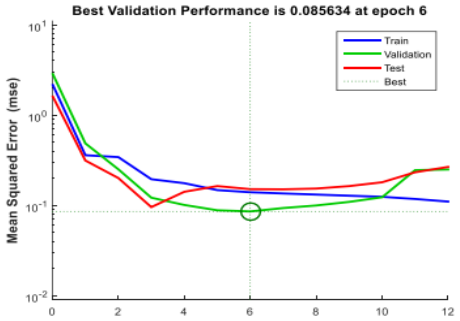

Fig.1.Validation of ANN

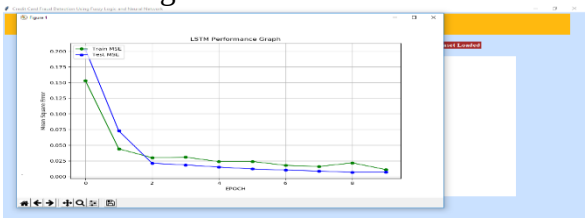

Fig.2.Trainging and Validation loss

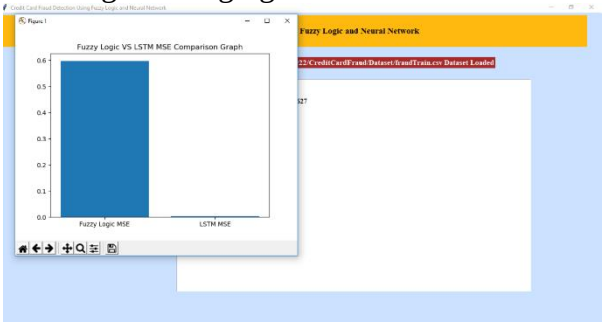

Fig.3.Algorithms Comparision

x-axis denotes algorithm names, while the y-axis represents Mean Squared Error (MSE) values. The

graph clearly illustrates that the MSE for the Long Short-Term Memory (LSTM) algorithm is significantly lower compared to the Fuzzy algorithm. Consequently, the data suggests that LSTM outperforms the Fuzzy algorithm in terms of accuracy and predictive capability.

VI. CONCLUSION

In this paper, we introduced an innovative approach to Credit Card Fraud Detection (CCFD) by integrating a rule-based fuzzy inference system with a erudition factor employing back-propagation neural network. Our proposed system underwent rigorous testing through experiments utilizing stochastic models. The obtained results suggest that the amalgamation of a neural network with fuzzy inference proves effective in tackling real-world challenges associated with credit card fraud detection.

VII. REFERENCE

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 20121. Inscoe, S. W.: Global Consumers: Losing Confidence in the Battle against Fraud. ACI Universal Payments, June, 2014,
7. Credit Card Fraud Statistics-2013, <http://www.cardhub.com/edu/creditfraud-Statistics>, 5 Feb, 2015.
3. Online Fraud is twelve times higher than offline fraud, <http://sellitontheweb.com/ezine/news034.shtml>, 20, June, 2007.
8. Ghosh, S., Reilly, D.L.: Credit card fraud detection with a neural-network. In: Proceedings of the Annual International Conference on System Science, pp. 621–630 (1994).
9. Aleskerov, E., Freisleben, B., Rao, B.: CARDWATCH: a neural-network based database mining system for credit card fraud detection. In: Proceedings of the Computational Intelligence for Financial Engineering, pp. 220–226 (1997).
10. Dorronsoro, J.R., Ginel, F., Sanchez, C., Cruz, C.S.: Neural fraud detection in credit card operations. IEEE Transactions on Neural Networks, pp. 827–834 (1997).
11. Liu, P., Li, L.: A Game-Theoretic Approach for Attack Prediction. Technical Report, PSU-S2-2002-01, Penn State University (2002).
12. Vatsa, V., Sural, S., Majumdar, A.K.: A game-theoretic approach to credit card fraud detection. In: Proceedings of the International Conference on Information Systems Security, Lecture Notes in Computer Science, vol. 3803. pp. 263–276 (2005).
13. Quah, J. T. S., Srinagesh, M.: Real-time credit fraud detection using computational intelligence. Expert Systems with Applications, 35, pp. 1721–1732 (2008).
14. Panigrahi, S., Kundu, A., Sural, S., Majumdar, A.: Credit card fraud detection a fusion approach using Dempster–Shafer theory and bayesian learning