Journal of Statistics & Management Systems
ISSN 0972-0510 (Print), ISSN 2169-0014 (Online)
Vol. 28 (2025), No. 1, pp. 139–149
DOI : 10.47974/JSMS-1320

An intelligent framework for credit card fraud detection through data analytics

Y. Ravi Kumar Chakrabarti *
Vemu Institute of Technology
Autonomous Institute
Chittor 517112
Andhra Pradesh
India

Bhuvan Unhelkar †
Muma College of Business
University of South Florida
8350 N. Tamiami Trail Sarasota
Florida, FL 34243
U.S.A.

S. Siva Shankar §
Department of Computer Science and Engineering
KG Reddy College of Engineering and Technology
Moinabad 500075
Telangana
India

Tulika Chakrabarti ‡
Department of Chemistry
Sir Padampat Singhania University
Udaipur 313601
Rajasthan
India

* *E-mail:* ravikumar.yeetha@gmail.com (Corresponding Author)
† *E-mail:* bunhelkar@usf.edu
§ *E-mail:* drsivashankars@gmail.com
‡ *E-mail:* tulika.chakrabarti@spsu.ac.in

Prasun Chakrabarti [@]
Department of Computer Science and Engineering
Sir Padampat Singhania University
Udaipur 313601
Rajasthan
India

B. Sivaneasan [#]
Specialist Adult Educator Engineering
Electrical Power Engineering Programme
Singapore Institute of Technology
1 Punggol Coast Road
Singapore 828608

Martin Margala [$]
School of Computing and Informatics
University of Louisiana at Lafayette
LA 70503
U.S.A.

Abstract

An intelligent framework combining Autoencoder Neural Networks and the Dragonfly optimization algorithm, which would be put forth to this research to combat effective credit card fraud by detecting fraudulent transactions quickly through extracting important features and patterns in transactional data with the help of Autoencoder Neural Networks. The Dragonfly optimization algorithm enhances the recital of the archetypal in question by refining the hyperparameters of the autoencoder archetypal. In doing so, the algorithm improves adaptability to emerging fraud patterns and always gives strong generalizations. Critical experiments are conducted that show that the framework has enormous precision, accuracy, F1 score, specificity, as well as recall while trying to detect credit card fraud as accurately as possible, reaching a maximum accuracy of 98%. This framework, therefore, will prove to be a good defence against credit card fraud by finally protecting financial interests, based on drawing the benefits of Autoencoder Neural Networks and Dragonfly optimization.

Subject Classification: *68T07, 68T10.*

Keywords: *Credit card fraud, Autoencoder, Dragonfly algorithm, Data analytics, Data-centric methodology.*

[@] *E-mail:* **drprasun.cse@gmail.com**
[#] *E-mail:* **sivaneasan@singaporetech.edu.sg**
[$] *E-mail:* **martin.margala@louisiana.edu**

I. Introduction

Credit card fraud, prevalent globally, stances a substantial hazard to financial security, with various deceptive tactics employed by fraudsters. Techniques such as skimming and online manipulation exploit vulnerabilities in transaction systems, demanding robust fraud detection measures [1-4]. Given the complexity and volume of data involved, analytical frameworks like Hadoop are essential for effective fraud prediction. Detecting fraud in real time involves swift analysis of payment requests and continual improvement through user feedback [5-7]. The proposed approach integrates autoencoder neural networks and Dragonfly algorithms, ornamental the efficiency and optimization of fraud detection systems. Evaluation metrics such as exactness, F1 score, remembrance, exactness, and specificity offer an inclusive assessment of the system's recital, ensuring a proactive response to fraudulent activities [8][9].

II. Problem statement

The persistence and evolution of credit card fraud pose significant challenges to financial societies, businesses, and cardholders globally [10-12]. The escalating sophistication of fraudulent activities jeopardizes the security and consistency of electronic payment systems [13-15]. Credit card fraud endures to be costly and unruly, impacting financial foundations, merchants, and consumers. Fraudsters employ various techniques to carry out unauthorized transactions, including whipped card information, card-not-present fraud, and identity theft. Current fraud detection approaches, though somewhat effective, frequently face challenges in adapting to evolving fraud tactics and may produce false positives, causing inconvenience for legitimate cardholders [16-18].

III. Proposed methodology

The proposed method generally refers to a suggested approach or a plan for carrying out a task conducting research or solving a problem.

1. *Data collection*

The preliminary phase includes determining the data source, which can be obtained from various channels such as financial institutions, payment processors, or entities managing credit card transactions.

Table 1

Information collection of credit card transaction

Sr. No	Data
1	Credit Card Number
2	Operation Amount
3	Transaction Date and Time
4	Merchant Information
5	Transaction Type
6	Cardholder Information
7	Transaction Status
8	Authorization Code
9	Payment Method
10	Gender
11	Transaction ID
12	Card Verification Value
13	Age group

Alternatively, publicly available datasets may be utilized for research purposes.

Table 1 provides an overview of the technical aspects of the information collection process for identifying credit card fraud.

2. *Pre-processing*

Effective pre-processing is required to ensure that the data is clean, unswerving and well-suited for drill machine learning models. Begin by examining the dataset for missing data and devise a strategy to address these gaps. Common approaches include imputation, where missing values are replaced with reasonable estimates.

3. *Autoencoder*

Specialising in the acquisition of informative data representations. Comprising two primary components, an encoder transmutes input data into a compact depiction, while a decoder restructures the novel input from this condensed form as demonstrated in Figure 1.

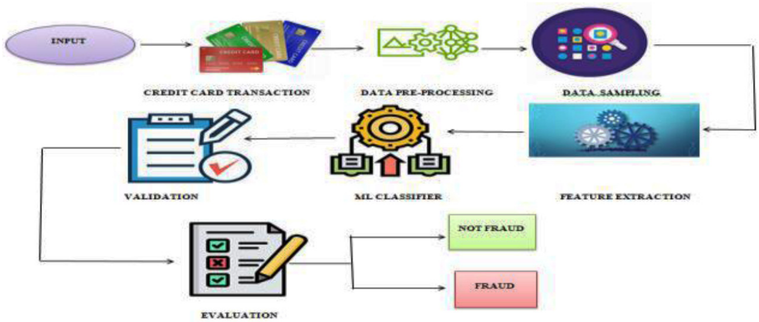

Figure 1

Proposed model for identifying credit card fraud

Figure 2 depicts the proposed tactic for sensing fraud.

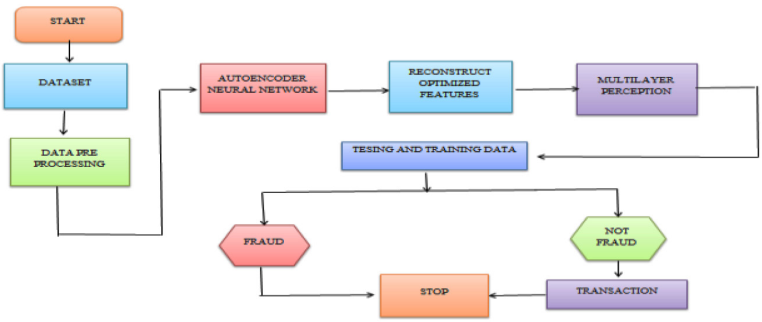

Figure 2

Flow diagram

Figure 3 illustrates the bid of neural networks in the framework of fraud recognition.

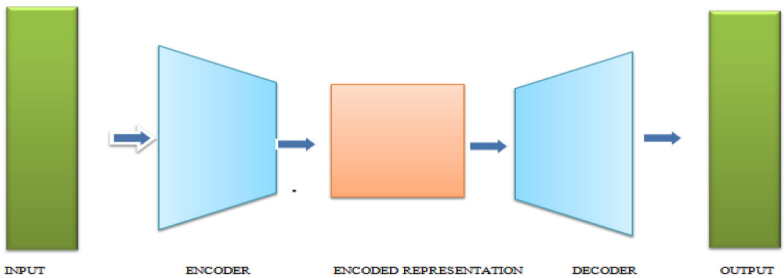

Figure 3

Neural network-based fraud detection

4. *Optimization*

In this proposed study, Dragonfly Optimization Algorithm (DOA) was employed to optimize the performance of credit card fraud identification by tuning its hyperparameters. The DOA draws inspiration from both dynamic and static swarming characteristics observed in dragonflies, reflecting the dual phases of meta-heuristic optimization: exploration and exploitation. In practical terms, dragonflies organize into sub-swarms, exploring diverse regions within a static swarm. The key characteristic during the exploration stage is the major objective of the dragonfly.

IV. Results

They evaluated the proposed technique using such as accurateness, precision, reminiscence, specificity, and F1-score. This allowed us to compare various algorithms comprehensively. Although accuracy is a commonly used metric, it may not be suitable when the dataset is imbalanced.

V. Performance testing

Performance testing is a systematic methodology for assessing the haste, reaction, and firmness of computer systems, networks, software applications, or devices under predefined workloads. Figure 4 and Figure 5 demonstrate the training and testing accuracy and loss of the projected technique.

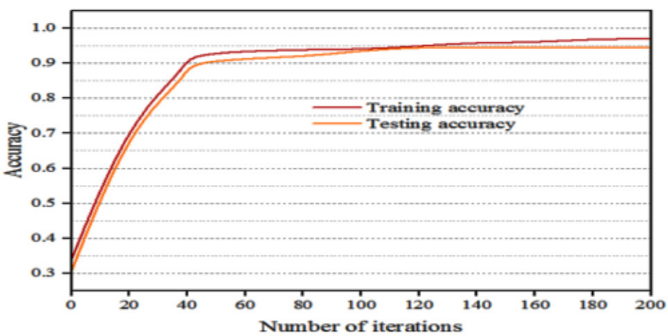

Figure 4

Accuracy in training and testing

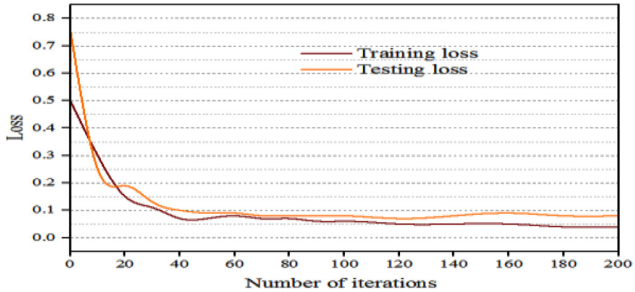

Figure 5

Loss in training and testing

Dataset

Detecting credit card fraud is vital in protecting cardholders and financial foundations from being wounded due to fraudulent activities. Figures 6 and 7 show the transaction status result. Figures 8, 9 and 10 show the fraudulent transaction and age distribution results.

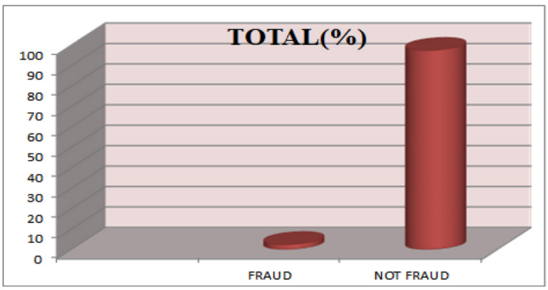

Figure 6

Transaction Status

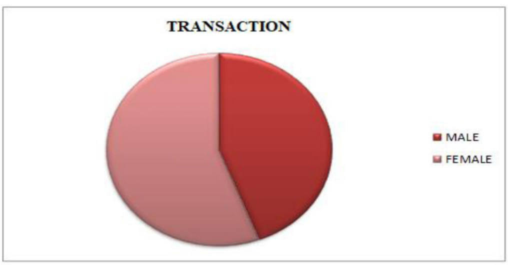

Figure 7

Transaction status by gender

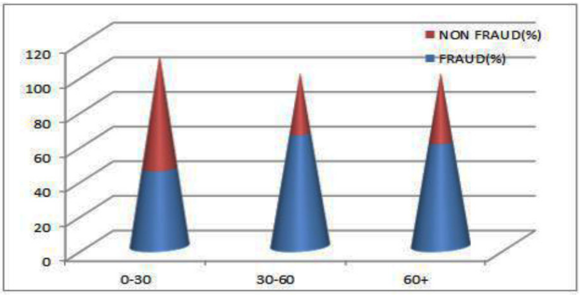

Figure 8

Age group distribution and fraud status

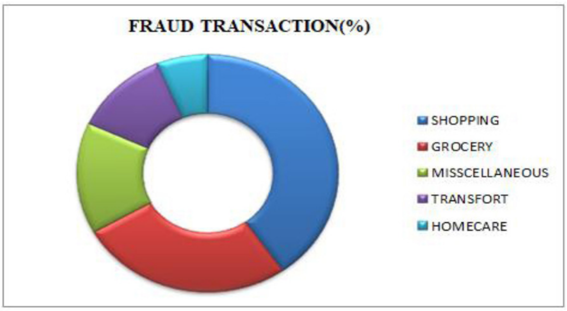

Figure 9

Fraudulent activity involving multiple merchant categories

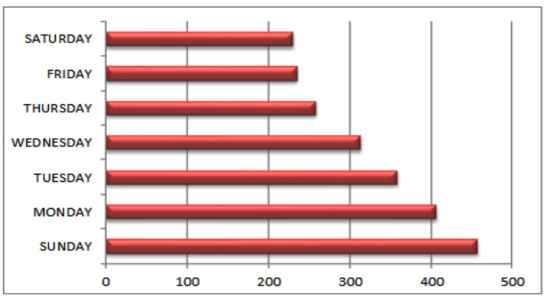

Figure 10

Fraudulent transactions on weekdays.

VI. Discussion

The optimization of the system for real-time transaction processing enables swift finding and timely retort to potential deceitful events.

Table 2

Overall performance with existing techniques

Models	Accuracy	F1-score	Recall	Precision	Specificity
Random forest	95	94	93	95	96
Decision tree	89	88	89	96	95
Logistic regression	94	95	87	93	89
Svm	93	94	92	89	94
Ann	90	92	90	92	96
Proposed	98	98	94	99	97

Leveraging advanced machine learning and deep neural networks, the approach exhibits high adaptability, effectively evolving to address emerging fraud patterns. Table 2 provides an overview of the overall performance in comparison with existing techniques.

VII. Conclusion

The integration of an autoencoder neural network with the Dragonfly algorithm has significantly improved credit card fraud recognition. By recognizing subtle patterns and anomalies, the system achieves enhanced accuracy, minimizing false positives and ensuring customer satisfaction. Its real-time processing capability empowers swift responses to potential fraud, reducing financial losses for organizations. Comparative analysis against established approaches demonstrates superior performance, with a 3% higher accuracy, 3% higher F1 score, 1% higher recall, 4% higher precision, and 1% higher specificity. This approach is highly effective in adapting to evolving fraud strategies, making it a valuable asset for financial security.

References

[1] O. Adepoju, J. Wosowei, and H. Jaiman, “Comparative evaluation of credit card fraud detection using machine learning techniques,” 2019 *Global Conference for Advancement in Technology* (GCAT), pp. 1–6, Oct. (2019).

[2] S. H. Z. Al-Thalabi, A. A. Heydari, and M. Tavakoli, “Modeling and prediction using an artificial neural network to study the impact of foreign direct investment on the growth rate/a case study of the State

of Qatar," *Journal of Statistics and Management Systems*, vol. 25, no. 8, pp. 1991–2003 (2022).

[3] O. Adepoju, J. Wosowei, and H. Jaiman, "Comparative evaluation of credit card fraud detection using machine learning techniques," 2019 *Global Conference for Advancement in Technology* (GCAT), pp. 1–6, Oct. (2019).

[4] A. A. Taha and S. J. Malebary, "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine," *IEEE Access*, vol. 8, pp. 25579–25587 (2020).

[5] N. Rtayli and N. Enneya, "Selection features and support vector machine for credit card risk identification," *Procedia Manufacturing*, vol. 46, pp. 941–948 (2020).

[6] N. H. Shah, N. Sheoran, and E. N. Jayswal, "Optimum controls to avert co-infection of Malaria-COVID-19," *Journal of Statistics and Management Systems*, vol. 25, no. 8, pp. 2043–2059 (2022).

[7] H. J. Mahanta and G. N. Sastry, "COVID-19 impact on Socio-economic and Health Interventions: A Gaps and Peaks analysis using Clustering Approach," *Journal of Statistics and Management Systems*, vol. 25, no. 8, pp. 2123–2153 (2022).

[8] R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," *Human-Centric Intelligent Systems*, vol. 2, no. 1, pp. 55–68 (2022).

[9] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. S. Hacid, and H. Zeineddine, "An experimental study with imbalanced classification approaches for credit card fraud detection," *IEEE Access*, vol. 7, pp. 93010–93022 (2019).

[10] M. I. Khan, "Dual generalized order statistics with moments properties using powered inverse Rayleigh distribution," *Journal of Statistics and Management Systems*, vol. 25, no. 8, pp. 2087–2099 (2022).

[11] S. Gore, G. S. P. S. Dhindsa, S. Gore, N. S. Jagtap, and U. Nanavare, "Recommendation of Contemporary Fashion Trends via AI-Enhanced Multimodal Search Engine and Blockchain Integration," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 1676–1682, Jul. (2023).

[12] S. Misra, S. Thakur, M. Ghosh, and S. K. Saha, "An autoencoder-based model for detecting fraudulent credit card transaction," *Procedia Computer Science*, vol. 167, pp. 254–262 (2020).

[13] M. R. Dileep, A. V. Navaneeth, and M. Abhishek, "A novel approach for credit card fraud detection using decision tree and random forest algorithms," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 1025–1028, Feb. (2021).

[14] T. T. Nguyen, H. Tahir, M. Abdelrazek, and A. Babar, "Deep learning methods for credit card fraud detection," arXiv preprint arXiv:2012.03754 (2020).

[15] A. Fallah, R. Kazemi, and S. Alipour, "Accuracy of L-moments approximation for spectral risk measures in heavy tail distributions," *Journal of Statistics and Management Systems*, vol. 25, no. 8, pp. 2073–2085 (2022).

[16] K. V. Metre, A. B. Smith, C. D. Johnson, and E. F. Williams, "An Introduction to Power BI for Data Analysis," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 1s, pp. 142–147 (2024).

[17] F. Itoo, Meenakshi, and S. Singh, "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection," *International Journal of Information Technology,* vol. 13, no. 4, pp. 1503–1511 (2021).

[18] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, "Credit card fraud detection using machine learning," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1264–1270 , May (2020).

Received February, 2024