

International Journal of Engineering Research and Science & Technology



www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(1) (2026)



ijerst.editor@gmail.com
editor@ijerst.com

Research Paper

MACHINE LEARNING APPROACHES FOR FRAUD DETECTION IN FINANCIAL NETWORKS

¹T. SAI SRAVANI, ²D. PAVAN KUMAR

¹PG Scholar, Dept. of CSE, PBR Visvodaya Institute of Technology and Science, Kavali, AP, India

²Assistant professor, Dept. of CSE, PBR Visvodaya Institute of Technology and Science, Kavali, AP, India

ABSTRACT — Globalization and rapid advances in digital innovation have greatly increased the complexity of financial networks, increasing their susceptibility to fraud. An estimated \$5 trillion in financial losses occur worldwide as a result of traditional fraud detection techniques' inability to keep up with changing fraudulent tactics. In response, this review article examines how artificial intelligence (AI) might be used to detect financial fraud, emphasizing machine learning (ML), deep learning (DL), and hybrid models as revolutionary approaches. AI may identify hidden fraud trends and flexibly adjust to new threats by examining large datasets. Supervised and unsupervised learning, as well as more sophisticated methods like Graph Neural Networks (GNNs), have been very successful in identifying several forms of financial fraud, such as money laundering, identity theft, and payment fraud. This work synthesizes information from a large number of research papers to give a thorough taxonomy of AI-driven fraud detection approaches. It offers an organized framework for comprehending the efficacy of fraud detection methods by methodically classifying them according to how they are used in various forms of fraud. It also looks at how distributed systems, cloud computing, and edge AI enable real-time transaction monitoring and fraud detection. Even while AI greatly increases detection accuracy, lowers operating costs, and improves regulatory compliance, issues including model explainability, data privacy concerns, algorithmic bias, and the dynamic nature of fraud continue to be major obstacles to its wider use. In order to address these issues, our assessment emphasizes the necessity of cooperative efforts between financial institutions, regulators, and technology vendors. Future studies should concentrate on enhancing the AI model's transparency, utilizing federated learning to improve fraud detection skills, and combining AI with blockchain for safe data exchange.

Index Terms— Financial Fraud Detection, Graph Neural Networks (GNNs), Fraud Analytics, Payment Fraud, Identity Theft, Money Laundering, Anomaly Detection, Edge AI, Distributed Systems, Real-Time Monitoring, Explainable AI (XAI), Data Privacy, Algorithmic Bias, Federated Learning, Blockchain, Regulatory Compliance.

I. INTRODUCTION

With the expansion of e-commerce and the widespread adoption of online payment

methods, fraudulent activities have seen a noticeable surge. Credible reports indicate a stark and rapid increase in financial losses

attributed to credit and debit card fraud between 2020 and 2022. What's particularly striking is that while unauthorized purchases and the use of counterfeit credit cards make up a relatively small portion, approximately 12-17%, of the total reported fraud cases, they account for a disproportionately large share, ranging from 75% to 80%, of the overall financial losses. In light of these critical issues, private businesses and government organizations have substantially increased their funding for research and development projects. Their primary objective is to create more resilient and effective systems for detecting fraudulent activities. Implementing automated fraud detection systems has become essential for financial institutions that oversee credit card issuance and online transaction management. These systems not only help reduce financial losses but also play a crucial role in enhancing customer faith and assurance. Innovative bigdata and artificial intelligence possibilities have opened up, giving intriguing potentials, particularly in utilizing powerful machine learning algorithms to combat financial crime. Modern fraud detection systems, aided by cutting-edge data analysis and advanced machine/deep learning algorithms, have demonstrated extraordinary efficacy. Typically, these algorithms are trained on large datasets of labeled transactions, allowing them to differentiate between regular and fraudulent activity. The ultimate result is the development of binary classification models capable of distinguishing between valid and fraudulent transactions. Detecting fraudulent transactions using classification algorithms is a difficult task that requires constant

innovation and flexibility. In the same way, innovation assures security, data availability, dependability, and resilience against cyber warfare assaults in the fight against wireless communication interference, the financial industry must continually innovate to stay ahead in the struggle against financial crime. Firstly, there's the issue of an imbalanced dataset, where the number of fraudulent transactions is significantly lower compared to legitimate ones. Secondly, there is the issue of cost sensitivity, where misclassifying fraudulent and normal transactions carries dissimilar costs, potentially having severe consequences. Additionally, transactions exhibit temporal dependence, necessitating consideration of their temporal relationships. Moreover, concept drift exists over time, which means that class conditional distributions can evolve, mandating periodic updates to the classifier. Lastly, managing the dimensionality of the feature space is a significant challenge, demanding sophisticated preprocessing techniques. A thorough examination of existing research found that when it comes to artificial neural networks, supervised learning techniques, logistic regression, and decision trees are the most commonly employed methods. Researchers have been drawn to the remarkable achievements of deep learning in various domains like computer vision, translation, speech recognition, and complex time series forecasting. As a result, several studies have started to utilize recurrent neural network variants, such as GRU, to develop credit card transaction fraud detection systems, taking inspiration from the success witnessed in those areas. LSTM and GRU

represent recurrent neural networks(RNNs) aimed at mitigating the issues of gradient vanishing and exploding gradients in RNNs. These architectures are designed explicitly for capturing temporal patterns within sequential data. Deep learning models are attractive because of the valuable information from unprocessed data. In many research areas, neural networks and deep learning methods have consistently shown better results than conventional algorithms. However, it's important to note that these models haven't been widely used in fraud detection of credit card fraud.

II. LITERATURE SURVEY

A) Artificial intelligence: Building blocks and an innovation typology

The range of topics and the opinions expressed on artificial intelligence (AI) are so broad that clarity is needed on the the field's central tenets, the opportunities AI presents, and the challenges it poses. To that end, we provide an overview of the six building blocks of artificial intelligence: structured data, unstructured data, preprocesses, main processes, a knowledge base, and value-added information outputs. We then develop a typology to serve as an analytic tool for managers grappling with AI's influence on their industries. The typology considers the effects of AI-enabled innovations on two dimensions: the innovations' boundaries and their effects on organizational competencies. The typology's first dimension distinguishes between product-facing innovations, which influence a firm's offerings, and process-facing innovations, which influence a firm's operations. The typology's second dimension describes innovations as either competence-

enhancing or competence-destroying; the former enhances current knowledge and skills, whereas the latter renders existing skills and knowledge obsolete. This framework lets managers evaluate their markets, the opportunities within them, and the threats arising from them, providing valuable background and structure to important strategic decisions.

B) No-reference stereoscopic image quality assessment based on global and local content characteristics

Existing no-reference image quality assessment (NR-IQA) methods mainly focus on designing the low-level features related to image degradation. However, the evaluation of image quality is the human visual perception of image content, involving the integrated analysis of global high-level semantics and local low-level characteristics. From this perspective, we propose a NR-IQA framework based on global and local content perception. We adopt the deep convolutional neural network (DCNN) to extract the semantic feature implied in global image content. The perception of visual quality associated with local content utilizes the visual attention and filtering mechanisms of human visual system. The overall image quality is estimated by combining the semantic and local characteristic features generated from the perceptions. Experimental results on the LIVE IQA database demonstrate that our method is superior to the state-of-the-art NR-IQA algorithms and competitive to the popular full-reference IQA methods. Further experiments on the TID2008 dataset show that the proposed approach is robust for various kinds of distortion types.

C) Banking is essential, banks are not. The future of financial intermediation in the age of the Internet

This paper examines the question how the future of financial intermediaries and banks as special financial intermediaries may look like in the age of the Internet. The reduction of transaction costs caused by the Internet will reduce the barriers to enter the market for financial products, because there may be no longer a need to run a large system of cost-intensive branches. But as closer examination of the functions of financial intermediaries shows, not everybody can sell and distribute financial products. This is true because of asymmetric information problems in financial business which require an intermediary with a good reputation and because of the need to keep large funds of capital to transform the risk of assets. Both requirements represent an important barrier to enter the market for financial intermediation. Not every financial product will be exposed to more competition due to the rise of the Internet but only products which are standardized and have a low risk. Moreover, large firms with high amounts of capital and a good reputation can be considered as new competitors for banks.

D) Credit card behavior, financial styles and heuristics

The paper makes four contributions. First, it provides new data and findings about credit card usage segmentation in respect to spending and borrowing behavior. Second, it sets the new findings against the backdrop of the newly emerging literature on financial literacy. There is great variability in financial literacy across American consumers. Third, it describes fast and frugal heuristics aimed

to help consumers make effective, and in some cases better, budgeting decisions when they use credit cards.

Fourth, it describes the introduction of a new set of online financial tools, offered by a large credit card company, which consumers are now using to make decisions about their spending and borrowing, and links these tools to the heuristics under discussion. Fast and frugal heuristics are likely to be especially valuable to consumers with low confidence in their online skills.

III. PROPOSED SYSTEM

The image below depicts an overview of our suggested system.

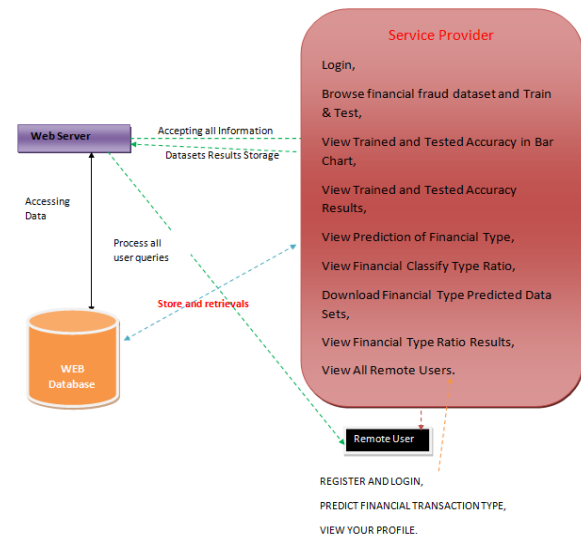


Fig. 1: System Overview

Implementation Modules

Service Provider

- In this module, the service provider has to login by using valid user name and password. After login successful he can do some operations such as
- Login, browse tweets data sets and train & test, view trained and tested accuracy in bar chart, view trained and tested accuracy results, view prediction

of financial type, view financial classify type ratio,

- Download financial type predicted data sets, view financial type ratio results, view all remote users.

Preprocessing

- In this module, service provider preprocess the data using minmax scalar function in python. This step includes data normalization, data cleaning and data transforming. This step useful to find relevant features to detect financial fraud.

Train and Test

- In this module, after preprocessing step service provider split the dataset as a train and test data. Train data is useful to train the models and test data is used for test the models. After splitting, service provider train the different machine learning models use training data and test the models using test data. Finally evaluate the models performances by constructing confusion matrix.

Remote User

- In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Register and login, predict financial transaction type, view your profile.

Prediction

- In this module, the remote user try to verify the financial data whether the

data is fraud or not. In this step the remote user provide the financial transaction data to the system and the pre trained model finds whether the transaction is fraud or not.

Methodology

Support Vector Machine Algorithm

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning.

The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane.

SVM chooses the extreme points/vectors that help in creating the hyperplane. These extreme cases are called as support vectors, and hence algorithm is termed as Support Vector Machine.

Decision Tree

Decision Tree is the most powerful and popular tool for classification and prediction. A Decision tree is a flowchart-like tree structure, where each internal node denotes a test on an attribute, each branch represents an outcome of the test, and each leaf node (terminal node) holds a class label.

A tree can be “learned” by splitting the source set into subsets based on an attribute value test. This process is repeated on each derived subset in a recursive manner called recursive partitioning. The recursion is completed when the subset at a node all has the same value of the target variable, or when splitting no longer adds value to the

predictions. The construction of a decision tree classifier does not require any domain knowledge or parameter setting, and therefore is appropriate for exploratory knowledge discovery. Decision trees can handle high-dimensional data. In general decision tree classifier has good accuracy. Decision tree induction is a typical inductive approach to learn knowledge on classification.

Logistic Regression

- Logistic regression is one of the most popular Machine Learning algorithms, which comes under the Supervised Learning technique. It is used for predicting the categorical dependent variable using a given set of independent variables.
- Logistic regression predicts the output of a categorical dependent variable. Therefore the outcome must be a categorical or discrete value. It can be either Yes or No, 0 or 1, true or False, etc. but instead of giving the exact value as 0 and 1, it gives the probabilistic values which lie between 0 and 1.
- Logistic Regression is much similar to the Linear Regression except that how they are used. Linear Regression is used for solving Regression problems, whereas Logistic regression is used for solving the classification problems.

Navy Base

- Naïve Bayes algorithm is a supervised learning algorithm, which is based on Bayes theorem and used for solving classification problems.
- It is mainly used in text classification that includes a high-dimensional training dataset.

- Naïve Bayes Classifier is one of the simple and most effective Classification algorithms which helps in building the fast machine learning models that can make quick predictions.

IV. RESULTS

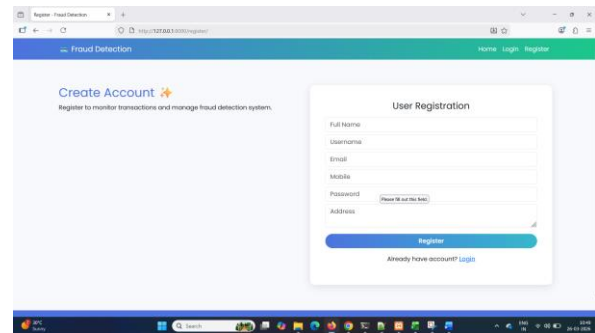


Fig.2: User Registration

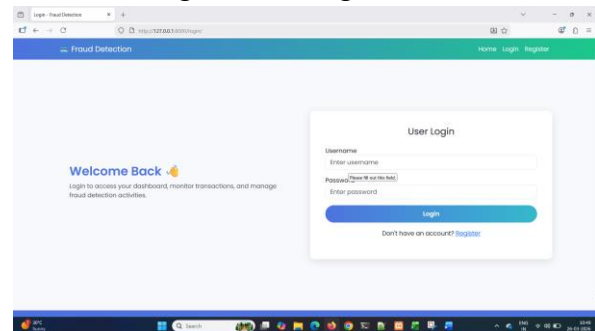


Fig.3: User Login

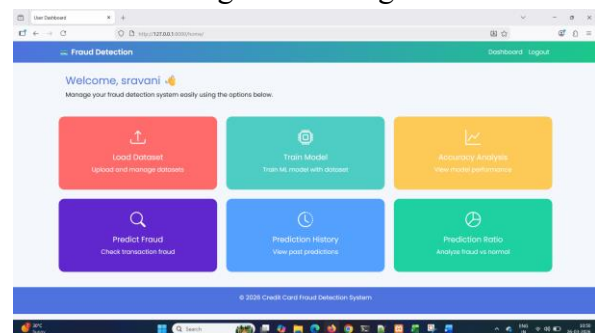


Fig.4: Dashboard

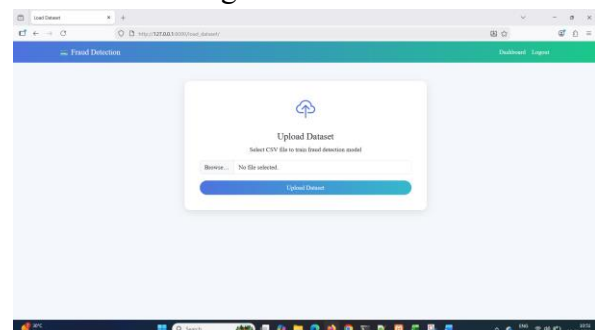


Fig.5: Upload Dataset

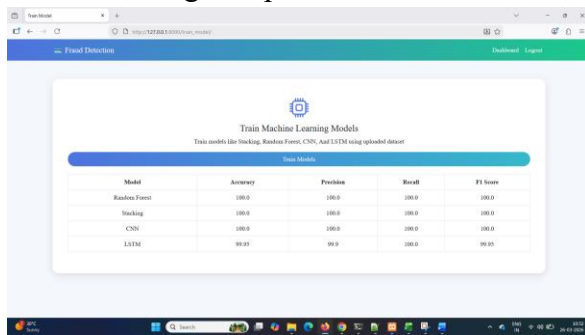


Fig.6: Train Models

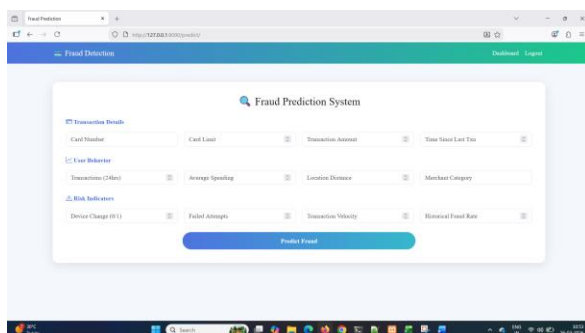


Fig.7: Prediction

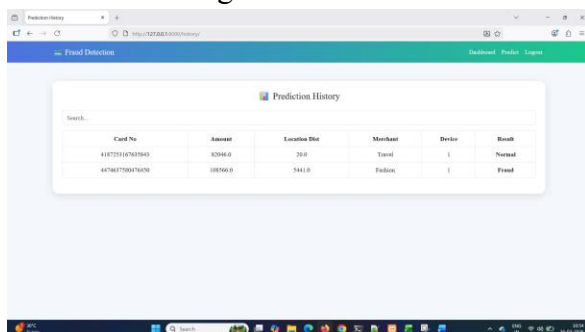


Fig.8: Prediction History

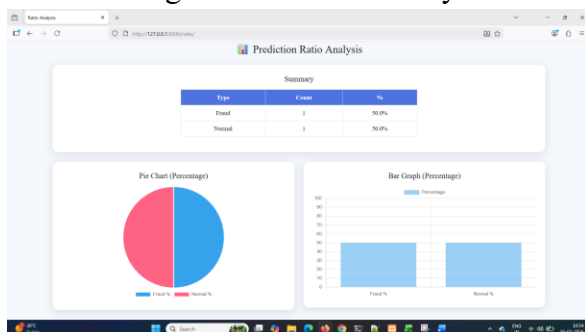


Fig.9: Prediction Results

V. CONCLUSION

Blockchain complement each other in strengthening financial fraud detection methods. In this regard, we went on a quest in the territory where mathematics and information dwell to look for the best strategies that can be embraced to curb what has become an increasing menace of fraud. This paper sought to demystify the connections that exist between AI, ML, data mining, big data, blockchain, and the financial security web as global society becomes saturated with cutting-edge technology solutions. Our purpose was to identify efficient strategies that could increase the robustness of the financial infrastructure, promote trust, and maintain the privacy and security of transactions in an environment increasingly exposed to cyber threats. Together, the results of this research demonstrate that AI and ML are capable of raising the bar on financial fraud prevention and provide a basis for subsequent developments that can help maintain the stability of the financial sphere against new types of threats. Future works must focus on improving Interpretability, integrating AI and blockchain, and employing federated learning to reinforce user privacy protection. Moreover, developing more accurate and scalable real-time fraud detection systems that we could not previously afford will become essential to combating new threats. Getting better at transparency and coordination between involved players, industry and, in effect, financial regulation will greatly depend on the symbiotic relations between the financial institutions, the regulators, and the academics to ensure that these alarm systems powered by AI

technology keep on improving and continue to ensure that the financial network boasts of strong security.

REFERENCE

- [1] U. Paschen, C. Pitt, and J. Kietzmann, "Artificial intelligence: Building blocks and an innovation typology," *Bus. Horizons*, vol. 63, no. 2, pp. 147155, Mar. 2020.
- [2] P. Yu, Z. Xia, J. Fei, and S. K. Jha, "An application review of artificial intelligence in prevention and cure of COVID-19 pandemic," *Comput., Mater. Continua*, vol. 65, no. 1, pp. 743760, 2020.
- [3] L. Shen, X. Chen, Z. Pan, K. Fan, F. Li, and J. Lei, "No-reference stereoscopic image quality assessment based on global and local content characteristics," *Neurocomputing*, vol. 424, no. 2, pp. 132142, Feb. 2021.
- [4] H. Beck, "Banking is essential, banks are not. The future of financial intermediation in the age of the Internet," *Netnomics*, vol. 3, no. 1, pp. 722, 2001.
- [5] G. N. F. Weiss, K. Pelger, and A. Horsch, "Mitigating adverse selection in P2P lending: empirical evidence from prosper.com," *SSRN Electron. J.*, vol. 19, no. 7, pp. 6593, 2010.
- [6] Y. Houston, C. Jongrong, J. H. Cliff, and H. Y. Chih, "E-commerce, R&D, and productivity: Firm-level evidence from Taiwan," *Inf. Econ. Policy*, vol. 18, no. 5, pp. 561569, 2013.
- [7] F. Allen, J. McAndrews, and P. Strahan, "E-finance: An introduction," *Center Financial Inst. Work. Papers*, vol. 22, no. 1, pp. 2527, 2012.
- [8] J. A. Kregel, "Margins of safety and weight of the argument in generating financial fragility," *J. Econ. Issues*, vol. 31, no. 2, pp. 543548, Jun. 1997.
- [9] A. Momparler, C. Lassala, and D. Ribeiro, "Efficiency in banking services: A comparative analysis of Internet-primary and branching banks in the US," *Service Bus.*, vol. 7, no. 4, pp. 641663, Dec. 2013.
- [10] V. Jambulapati and J. Stavins, "Credit CARD act of 2009: What did banks do?" *J. Banking Finance*, vol. 46, no. 9, pp. 2130, Sep. 2014.