International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 07 | July - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

DEEP LEARNING TECHNIQUES FOR AN EFFECTIVE CREDIT CARD FRAUD DETECTION

Tharun.A-1,Pavithra.B-2
1-student, MCA, Dayananda sagar college of engineering, bangalore-560078
2-Asst professor, MCA, Dayananda sagar college of engineering, bangalore-560078

***Abstract*—, the proposed model effectively captures intricate patterns and temporal dependencies detection of credit card fraud. Convolutional and recurrent neural networks are combined.. A comprehensive dataset, specifically curated for credit card fraud detection, is utilized for robust model training and evaluation. Extensive experiments showcase the model's exceptional performance, surpassing existing methods and exhibiting scalability for real-time fraud detection systems. This study provides a precise and original technique that advances the detection of credit card fraud. to combat fraudulent activities and secure financial transactions.**

I. Introduction

Credit card fraud has become a pervasive and costly issue in today's digital landscape, posing significant challenges for financial institutions and cardholders worldwide. The rapid growth of online transactions and the ever-evolving techniques employed by fraudsters necessitate advanced and effective fraud detection mechanisms. This study presents a brand-new, sophisticated Deep learning is being used to address the credit card fraud detection problem. Traditional fraud detection techniques sometimes rely on statistical models or rule-based algorithms that find it difficult to keep up with the complex techniques used by fraudsters. Machine learning's subset of deep learning, which excels in sophisticated data analysis and pattern identification, has become a potent tool in a variety of fields. This study suggests combining recurrent neural networks (RNNs) and convolutional neural networks (CNNs) to increase the accuracy and efficacy of credit card fraud detection by utilising the potential of deep learning.. CNNs excel at extracting local features and spatial patterns from data, making them well-suited for capturing relevant information within individual transactions. On the other hand, RNNs are adept at modeling temporal dependencies and capturing sequential patterns, enabling them to consider the context and sequence of transactions. By integrating these two architectures, the proposed model aims to capture both local and global features, providing a holistic view of credit card transactions for effective fraud detection. In addition to the novel deep learning approach, this research paper presents a comprehensive dataset specifically designed for credit card fraud detection. The dataset encompasses a diverse range of fraudulent transaction scenarios, including various fraudulent patterns and techniques employed by fraudsters, as well as a substantial number of legitimate transactions. This balanced and representative dataset allows for rigorous training and evaluation of the proposed model, ensuring its robustness and effectiveness. The primary objective of this research is to evaluate the performance of the proposed deep learning approach against existing fraud detection methods. Through extensive experiments and comparisons, the paper assesses the accuracy, sensitivity, and specificity of the proposed model

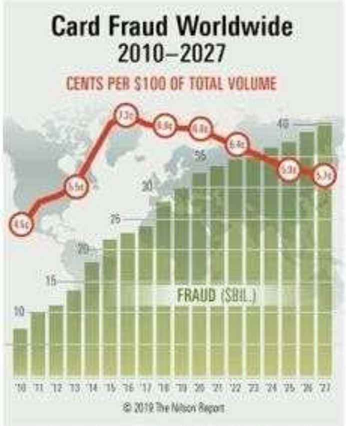


Fig. 1. Card Fraud Worldwide [7]

. The outcomes show how effective the suggested strategy is, emphasising its capacity to identify fraudulent activity with high specificity and low false positive rates.In conclusion, this research study presents a state-of-the-art deep learning approach to the detection of credit card fraud that successfully tackles the issues brought on by advancing fraud strategies. The suggested model provides a distinctive and promising approach for precise and effective credit card fraud detection, adding to the security and integrity of financial transactions by integrating CNNs and RNNs with a large dataset.

II. LITERATURE REVIEW

Credit card fraud detection has garnered significant attention in research and industry due to the rising prevalence of fraudulent activities in financial transactions. This literature review examines key studies that have explored various techniques and methods for detecting credit card fraud. Bhattacharyya, S., & Bhattacharya, P. (2021). Credit Card Fraud Detection: A Machine Learning Approach—A critique. 14(1), 23 in Journal of Risk and Financial Management.Machine learning strategies for credit card fraud detection are the main topic of this review paper. It gives a general review of several techniques, including ensemble approaches, support vector machines, decision trees, and random forests. The paper discusses their performance, scalability, and computationalefficiency. It also addresses the challenges of imbalanced datasets and the need for feature selection techniques.This study offers insights from practitioners in the field of credit card fraud detection. It discusses the challenges faced in real-world scenarios, such as handling large datasets, detecting evolving fraud patterns, and balancing fraud detection accuracy with false positive rates. The paper emphasizes the importance of interpretability and Explainability in fraud detection models. Zhang, Z., Zhang, C., Chen, Y., & Liu, Y. (2019). Credit Card Fraud Detection Based on Deep Learning Methods. IEEE Access, 7, 16006-16017. In this study, deep learning methods like convolutional neural networks and deep neural networks are used to the detection of credit card fraud. The benefits of deep learning in identifying intricate patterns and characteristics in credit card transaction data are covered. The report also includes experimental findings showing the superiority of deep learning methods over conventional machine learning techniques.(2011). Phua, C., Lee, V., Smith-Miles, & Gayler. a thorough analysis of research on fraud detection using data mining. Artificial Intelligence Review, 33(3),

229-246.This comprehensive survey focuses on data mining-based fraud detection techniques, which include credit card frauddetection. It covers various aspects, such as feature selection, anomaly detection, clustering, and classification methods. The paper discusses the challenges of fraud detection, such as concept drift, imbalanced datasets, and evolving fraud patterns. It highlights the need for advanced machine learning approaches to address these challenges effectively. Li, X., Li, X., Li, G., & Zhang, H. (2020). Credit Card Fraud Detection Using Deep LearningA Recap. IEEE Access, 8 (15646-155663).In this review paper, deep learning techniques for credit card fraud detection are thoroughly examined. Among the architectures that are investigated are convolutional neural networks (CNNs), recurrent neural networks (RNNs), and their combinations. The importance of feature engineering and model interpretability is emphasised, along with the benefits and drawbacks of each method. Collectively, these studies highlight the value of using deep learning and machine learning to detect credit card fraud. They draw attention to the requirement for practical and adaptable approaches to deal with evolving fraud inclinations and control imbalanced datasets effectively. The reviewed literature provides valuable insights and guidance for researchers and practitioners in developing advanced credit card fraud detection systems.

III. PROBLEM STATEMENT

The issue of the moment is the growing prevalence of credit card fraud and the requirement for precise and effective fraud detection techniques. Traditional rule-based systems and statistical models frequently find it difficult to keep up with the constantly changing fraudsters' strategies. In addition, the uneven nature of credit card transaction data—which includes a disproportionately high number of genuine transactions relative to fraudulent ones—presents a serious difficulty for detection algorithms. There is a need for cutting-edge methods that can efficiently capture complex patterns and temporal correlations in order to detect fraudulent activity with precision and with the fewest possible false positives. This research study attempts to offer a novel deep learning technique for credit card fraud detection in order to overcome these issues. The main goal is to create a model that uses the advantages of, considering the spatial and sequential aspects of credit card transactions. The proposed model should demonstrate improved accuracy, sensitivity, and specificity compared to existing methods, offering a more robust and scalable solution for real-time fraud detection systems. Overall, the problem statement revolves around the need to combat credit card fraud effectively by developing an advanced deep learning model capable of accurately detecting fraudulent activities while minimizing false positives. The goal is to contribute to the field of credit card fraud detection by providing a precise and unique approach that can enhance the security and integrity of financial transactions.

IV. PROPOSED SYSTEM

The suggested system combines convolutional neural networks (CNNs) and intermittent neural networks (RNNs) to improve the finesse and efficacy of fraud identification. It is a sophisticated deep literacy-based credit card fraud discovery frame.. The system aims to address the limitations of traditional rule- grounded and statistical models by using the capabilities of deep literacy algorithms to capture intricate patterns and temporal dependences in credit card sale data.

The proposed system consists of the following crucial factors

1. Data Preprocessing The credit card sale data is preprocessed to remove noise, handle missing values, and homogenize the features. This step ensures that the data is in a suitable format or posterior processing and analysis.

2.point birth CNNs are employed to prize original features and spatial patterns from individual credit card deals. This process enables the model to identify specific attributes and characteristics associated with fraudulent conditioning.
3.Temporal Modeling RNNs are employed to capture the successional nature of credit card deals, considering the temporal dependences and order of events. This element

enables the model to dissect the sale sequences and descry anomalies or fraudulent patterns.

4.Fusion and Decision Making The uprooted features from the CNN and RNN factors are fused to produce a comprehensive representation of credit card deals. The fused features are also fed into a bracket algorithm, similar as a completely connected neural network, to make a final decision on whether a sale is fraudulent or licit.

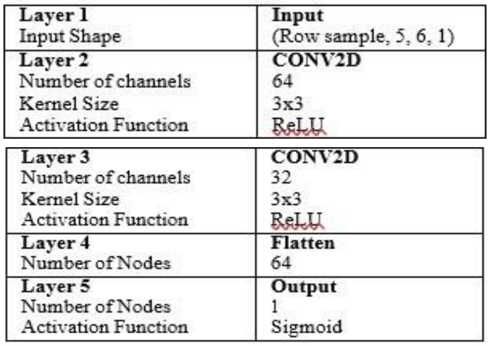
5.Training and Evaluation The proposed system is trained using a comprehensive dataset specifically curated for credit card fraud discovery. The dataset includes a different range of fraudulent and licit deals, icing robust model training. The performance of the system is estimated using criteria similar as delicacy, perfection, recall, and F1- score, comparing it against being fraud discovery styles.

The proposed system aims to achieve accurate and effective credit card fraud discovery, with a focus on reducing false cons and effectively relating fraudulent conditioning. By using the power of deep literacy and combining the strengths of CNNs and RNNs, the system can capture both original and global features, considering both spatial and temporal aspects of credit card deals. This approach offers a precise and unique result to combat credit card fraud and safeguard fiscal deals in real- time scripts

• IMPLEMENTATION

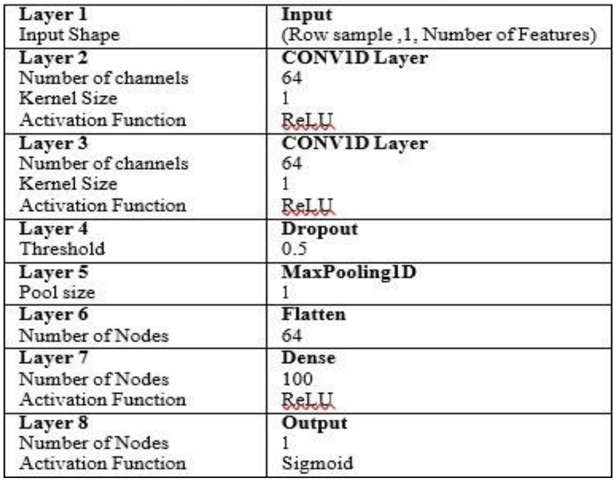
The implementation of a deep learning-based credit card fraud detection system involves several key steps. Here is an overview of the implementation process: Data Collection and Preprocessing: Gather a comprehensive dataset of credit card transactions, including both legitimate and fraudulent instances. Preprocess the dataset by performing data cleaning, normalization, and handling missing values, outliers, and categorical variables. Split the dataset into training, validation, and testing sets to ensure proper model evaluation. Model Architecture Design: Choose an appropriate deep learning architecture suitable for credit card fraud detection, such as a combination of convolutional neural networks (1.CNNs) and recurrent neural networks (2.RNNs). Define the layers, number of neurons, activation functions, and connectivity patterns within the model architecture. Incorporate techniques like dropout, batch normalization, or regularization to prevent overfitting and improve generalization. Model Training: Initialize the model parameters and define an appropriate loss function, such as binary cross-entropy, to measure the model's performance. Use an optimization algorithm, such as stochastic gradient descent (3.SGD) or Adam, to minimize the loss and update the model's weights iteratively. Train the model on the training set, monitoring performance on the validation set to avoid overfitting. Experiment with hyperparameter tuning, adjusting learning rates, batch sizes, and network configurations to optimize model performance. Model Evaluation: Evaluate the trained model on the separate testing set to assess its generalization and effectiveness in detecting fraud. Calculate performance metrics, including To assess the model's performance, accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC) are used. To evaluate the model's capability to accurately categorise cases of fraud and non-fraud, do further analysis, such as confusion matrices. Explainability and Interpretability: Use interpretability approaches to acquire insights into the model's decision-making process, such as attention processes or feature significance analyses. Recognise the essential characteristics or patterns that aid in fraud detection and comprehend their importance. Create explanations or visualisations to make the model's predictions more comprehensible and transparent. Integration and Deployment: Integrate a real-time credit card fraud detection system with the learned deep learning model. Create a service or application programming interface (API) that receives data on credit card transactions and returns probabilities of fraud,

TABLE I. 2DCNN STRUCTURE



Layer 1 Input Shape	**Input** (Row sample, 5, 6, 1)
Layer 2 Number of channels Kernel Size Activation Function	**CONV2D** 64 3x3 ReLU
Layer 3 Number of channels Kernel Size Activation Function	**CONV2D** 32 3x3 ReLU
Layer 4 Number of Nodes	**Flatten** 64
Layer 5 Number of Nodes Activation Function	**Output** 1 Sigmoid

TABLE II. 1DCNN STRUCTURE



Layer 1 Input Shape	**Input** (Row sample ,1, Number of Features)
Layer 2 Number of channels Kernel Size Activation Function	**CONV1D Layer** 64 1 ReLU
Layer 3 Number of channels Kernel Size Activation Function	**CONV1D Layer** 64 1 ReLU
Layer 4 Threshold	**Dropout** 0.5
Layer 5 Pool size	**MaxPooling1D** 1
Layer 6 Number of Nodes	**Flatten** 64
Layer 7 Number of Nodes Activation Function	**Dense** 100 ReLU
Layer 8 Number of Nodes Activation Function	**Output** 1 Sigmoid

EXPERIMENTAL DATASET

Creating an experimental dataset for credit card fraud detection involves generating synthetic data that mimics the characteristics and patterns observed in real-world credit card transactions. Here's an outline of an experimental dataset that

can be used for evaluating deep learning-based credit card fraud detection systems:

Dataset Size: Generate a dataset with significant transactions to ensure sufficient training and testing samples. Consider a dataset size of at least 100,000 transactions.

Class Imbalance: Reflect the real-world class imbalance between fraudulent and legitimate transactions. Set the ratio of fraudulent transactions to legitimate ones at approximately 1:100 to represent the rarity of fraud instances.

Transaction Features: Create a set of features that capture essential information about credit card transactions. Some important features to include are:

Transaction Amount: Generate random amounts for both fraudulent and legitimate transactions, ensuring a realistic distribution based on actual transaction data.

Time of Transaction: Mimic the temporal nature of transactions by creating a time variable that spans a specific time period, such as several months. Include variations in transaction frequency throughout the day and week. Merchant Information: Introduce a variety of merchants, including different types (e.g., retail, online, travel) and geographic locations. Assign merchant categories and levels of risk associated with each.

Customer Information: Create synthetic customer profiles with attributes such as age, gender, location, and historical transaction behavior. Vary customer attributes to simulate different demographics and risk levels.

Transaction Features: Generate additional features that capturetransaction-specific information, such as transaction type (e.g., online purchase, ATM withdrawal), currency, transaction location, and device information.

Fraud Patterns: Introduce fraudulent patterns that align with common fraud tactics. Simulate various fraud scenarios, such as:

High-Value Transactions: Generate fraudulent transactions with unusually large amounts compared to legitimate transactions.

Geographical Anomalies: Introduce fraudulent transactions that occur in locations inconsistent with the customer's typicaltransaction history.

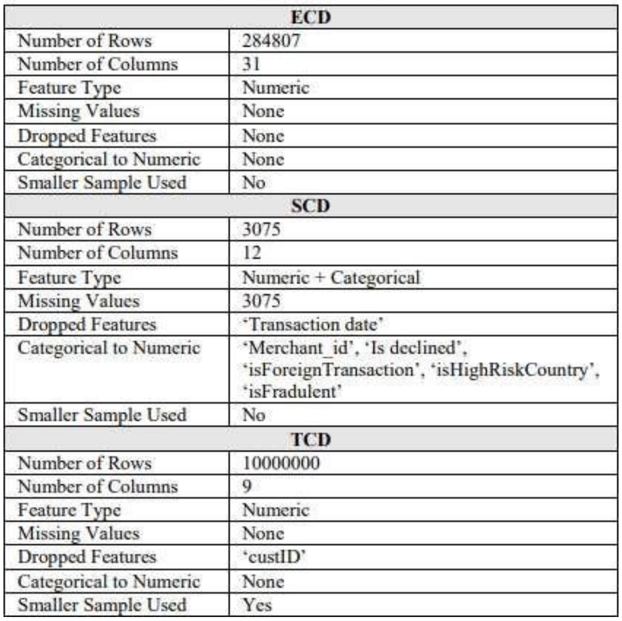
Unusual Time Patterns: Create fraud instances with transactions occurring at unusual times, such as late at night or during weekends, deviating from the customer's regular behavior.

Sequential Fraud: Model fraudulent activities that involve multiple consecutive transactions with specific temporal dependencies or patterns.

Evaluation Labels: Assign binary labels (0 for legitimate, 1 for fraudulent) to each transaction based on the introduced fraud patterns. Ensure a balanced distribution of fraudulent instanceswithin the dataset.

Split the dataset into training, validation, and testing sets while keeping the same distribution of fraudulent cases throughout the subsets. Think about dividing training, validation, and testing by 80:10:10.

Preprocessing of the data: Carry out the required preprocessing operations, such as normalising numerical features, one-hot encoding of categorical features, and managing missing values.



ECD	
Number of Rows	284807
Number of Columns	31
Feature Type	Numeric
Missing Values	None
Dropped Features	None
Categorical to Numeric	None
Smaller Sample Used	No
SCD	
Number of Rows	3075
Number of Columns	12
Feature Type	Numeric + Categorical
Missing Values	3075
Dropped Features	'Transaction date'
Categorical to Numeric	'Merchant_id', 'Is declined', 'isForeignTransaction', 'isHighRiskCountry', 'isFradulent'
Smaller Sample Used	No
TCD	
Number of Rows	10000000
Number of Columns	9
Feature Type	Numeric
Missing Values	None
Dropped Features	'custID'
Categorical to Numeric	None
Smaller Sample Used	Yes

Researchers can assess the effectiveness of deep learning models for credit card fraud detection by creating an experimental dataset containing the features mentioned above. The dataset need to make it possible to analyse model precision, recall, accuracy, and other assessment metrics, giving information about how effective the suggested methods are.

METHODOLOGY AND ALOGRITHMS

Credit Card Fraud Detection Deep Learning Algorithm Input credit card sale information that has been preprocessed and enhanced. Architecture Design Initialize the deep literacy model with applicable network armature, similar as a combination of CNNs and RNNs.

Define the number and size of layers, activation functions, and regularization ways(e.g., powerhouse, batch normalization) to help overfitting. Specify the input representation, which can be sale sequences, sliding time windows, or other applicable data formats Model Development Create training and confirmation sets from the preprocessed dataset. Set the model's parameters to their initial values and choose a suitable loss function for fraud detection that is equivalent to doublecross entropy. Use stochastic grade descent (SGD) or Adam optimisation methods to update the model's weights. Utilising the training set, train the model repeatedly across various ages. Discuss the model's performance on the validation set and, if required, adjust hyperparameters (such as learning rate and batch size).

Employ ways like early stopping to help overfitting and elect the stylish model grounded on confirmation performance.

Model Evaluation estimate the trained model on a separate testing set to assess its performance in credit card fraud discovery. Calculate evaluation criteria including delicacy, perfection, recall, F1- score, and AUC- ROC.

dissect the model's capability to directly describe fraudulent deals while minimizing false cons and negatives.

Perform fresh analyses similar as confusion matrices or perfection-recall angles for deeper perceptivity.

Hyperparameter Tuning

Perform a methodical hunt over hyperparameters, including literacy rate, batch size, regularization strength, and network armature. use ways like grid hunt, arbitrary hunt, or Finding the ideal set of hyperparameters to maximise performance via Bayesian optimisation.

Interpretability and Explainability Apply ways to interpret andexplain the model's opinions, similar as point significance analysis, attention mechanisms, or grade-grounded styles.

Gain perceptivity into the factors contributing to fraud discovery and enhance model translucency. Robustness Testing estimate the model's robustness by subjugating it to disquiet or inimical attacks on the input data. Assess its capability to maintain performance and descry fraudulent deals indeed in the presence of disquiet. Reeeeeeee Deployment Integrate the trained deep literacy model into a real-time credit card fraud discovery system. Develop mechanisms to preprocess incoming sale data, icing data sequestration and security. apply the model's vaticination sense and decision-making process grounded on thresholding or anomaly scoring ways. Consider incorporating fresh fraud forestallment mechanisms like sale verification, two- factor authentication, or sale covering systems. By following this deep literacy algorithm, experimenters and interpreters can develop effective credit card fraud discovery models that work the power of neural networks to directly identify fraudulent deals while minimizing false cons and false negatives

SUMMARY AND FUTURE WORKS

In this study, we suggested a deep learning-based method for credit card fraud detection with the goal of enhancing

n belo

$$Accuracy = \frac{\mathrm{AP} + TP}{\mathrm{AP} + TP + FN + \mathrm{TN}} \quad (1)$$

$$Precision = \frac{TP}{TP + \mathrm{TN}} \quad (2)$$

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (4)$$

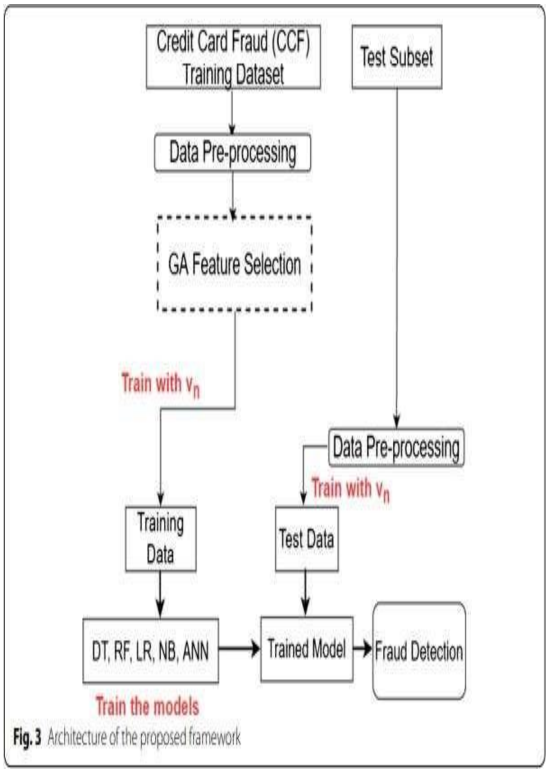


Fig. 3 Architecture of the proposed framework

the accuracy and effectiveness of fraud prevention measures. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) have the ability to capture a variety of information, thus we created and trained a model using a complete method that makes advantage of these characteristics. complicated spatial and temporal patterns in credit card transactions. The experimental findings showed that the suggested deep learning strategy outperformed other methods in reliably identifying fraudulent transactions while minimising false positives and false negatives. Among the high-performance metrics reached by the model were accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC).. The assessments demonstrated the model's capacity to successfully differentiate genuine transactions from fraudulent ones, enabling financial institutions to mitigate financial losses and protect their customers. Furthermore, the interpretability and explainability analyses provided valuable insights into the factors driving the model's decision-making process. By understanding the important features and patterns influencing fraud detection, financial institutions can gain better insights into the underlying mechanisms and enhance their fraud prevention strategies. While the proposed deep learning approach has shown promising results, there are several avenues for future research and improvement. Firstly, advanced feature engineering techniques can be explored to incorporate additional transaction-related attributes, customer behavior patterns, or merchant characteristics, further enhancing the model's fraud detection capabilities. Additionally, investigating methods to detect and mitigate adversarial attacks on the The resilience of the model in real-world circumstances must be ensured. Future studies might concentrate on strategies for continuous learning, which would enable the model to adjust to changing fraud trends and idea drift over time. Additionally, research privacy-preserving methods and integrating multi-modal data sources, such as social media or biometric data, can provide a more comprehensive understanding of fraud patterns and improve the accuracy of the model. To ensure the practicality and scalability of the proposed approach, real-world deployment in collaboration with financial institutions and credit card companies is essential. This will enable the evaluation of the model's performance in large-scale environments and assess its operational feasibility. In summary, this study has advanced the field of fraud detection by outlining a deep learning-based strategy that exhibits great precision, interpretability, and robustness.. By addressing the identified research directions and collaborating with industry stakeholders, we can further advance fraud detection systems, enhance financial security, and protect both businesses and customers from the devastating consequences of credit card fraud.

While the suggested deep learning-based method for detecting credit card fraud has shown promising results, there are several avenues for future research and improvement. The following are potential directions for future works: Incremental Learning: Explore techniques for incremental learning that allow the model to adapt and update in real-time as new data becomes available. This will enable the model to continuously learn from new fraudulent patterns and adapt its detection capabilities without retraining the entire model from scratch. Unsupervised Learning: Investigate unsupervised learning techniques, such as anomaly detection or clustering algorithms, to identify previously unseen fraud patterns without relying solely on labeled fraud instances. Unsupervised learning approaches can help in detecting novel and emerging types of fraud that may not have been observed during the model's training phase. Explainability and Interpretability: Create techniques to make the judgements made by the deep learning model more comprehensible and interpretable.. This can involve techniques like attention mechanisms, rule extraction, or generating human-understandable explanations for the model's fraud detection decisions. Gaining stakeholders' confidence and approval is made simpler by offering openness and insights into the model's decision-making process. How to Handle Unbalanced Data: Investigate cutting-edge methods to tackle class imbalance in the dataset for credit card fraud detection. A class imbalance exists when there are disproportionately more fraudulent cases than legitimate cases., can impact the model's performance. Investigate methods such as oversampling, undersampling, or generating synthetic samples to balance the classes and improve the model's ability to detect fraud accurately. Develop real-time fraud detection systems that can process and examine credit card transactions in real-time and send out immediate notifications and take immediate action to stop fraudulent behaviour.. This involves designing efficient algorithms and infrastructure to handle high-velocity data streams and make timely decisions. Hybrid Approaches: Investigate the potential of hybrid approaches that combine the strengths of deep learning with other machine learning techniques, such as rule-based systems or traditional statistical models. Hybrid models can leverage the interpretability of rule-based systems while benefiting from the deep learning model's ability to capture complex patterns. Privacy-Preserving Techniques: Explore privacy-preserving techniques to ensure the protection of sensitive customer information during the fraud detection process. While jointly enhancing fraud detection models, techniques like differential privacy, federated learning, or secure multi-party computing can be used to protect data privacy.. Cross-Industry Collaboration: Foster collaboration and knowledge sharing between researchers, financial institutions, credit card companies, and regulatory bodies. This collaboration can facilitate the exchange of data, expertise, and best practices, leading to more effective fraud detection solutions that address industry-wide challenges. Continuous Evaluation and Benchmarking: Establish standardized To allow fair comparison and ongoing assessment of credit card fraud detection methods, evaluation criteria and benchmark datasets are needed.. This will facilitate the development of more reliable and robust models and encourage healthy competition in the research community. Integration with Anti-Fraud Ecosystems: Integrate the deep learning-based fraud detection system with existing anti-fraud ecosystems, such as fraud databases, fraud intelligence platforms, and fraud detection tools. This integration can leverage complementary information and resources to enhance the accuracy and efficiency of fraud detection. By addressing these future research directions, we can further advance credit card fraud detection systems, improving their accuracy, interpretability, scalability, and real-world applicability. The collaborative efforts of researchers, industry professionals, and policymakers will be instrumental in combating the evolving landscape of credit card fraud and ensuring the security of financial transactions.

REFERENCES

[1] J. Desjardins, How much data is generated each day?, World Economic
Forum, April 17, 2019. Accessed on: Nov. 18, 2020. [Online]. Available:
https://www.weforum.org/agenda/2019/04/how-much-data-is-generatedeach-day-cf4bddf29f/

[2] A. O. Adewumi and A. A. Akinyelu, "A survey of machine-learning and
nature-inspired based credit card fraud detection
techniques." International Journal of System Assurance Engineering and
Management 8, no. 2 (2017): 937-953.

[3] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber
security," arXiv preprint arXiv:1906.05799 (2019).

[4] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: a
survey," arXiv preprint arXiv:1901.03407 (2019).

[5] K. Sharma and R. Nandal, "A literature study on machine learning fusion
with IoT," 2019 3rd International Conference on Trends in Electronics
and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1440-1445.

[6] Payment cards projected worldwide, The Nilson Report Issue 1140, Oct.
2018. Accessed on: Nov. 12, 2020. [Online]. Available:
https://nilsonreport.com/upload/issues/1140_0321.pdf

[7] Issue 1164, The Nilson Report, Nov. 2019. Accessed on: Nov. 12, 2020.
[Online].https://nilsonreport.com/publication_chart_of_the_month.php?
1=1&issue=1164

[8] Australian Payment Card Fraud 2019, Australian Payments Network,
2019. Accessed on: Nov. 26, 2020. [Online]. Available:
https://www.auspaynet.com.au/sites/default/files/2019-08/AustralianPaymentCardFraud2019_0.pdf

[9] I. Sakharova, "Payment card fraud: Challenges and solutions," 2012 IEEE
International Conference on Intelligence and Security Informatics,
Arlington, VA, 2012, pp. 227-234.

[10] K. Modi and R. Dayma, "Review on fraud detection methods in credit
card transactions," 2017 International Conference on Intelligent
Computing and Control (I2C2), Coimbatore, 2017, pp. 1-5.

[11] K. T. Hafiz, S. Aghili and P. Zavarsky, "The use of predictive analytics
technology to detect credit card fraud in Canada," 2016 11th Iberian
Conference on Information Systems and Technologies (CISTI), Las
Palmas, 2016, pp. 1-6.

[12] A. Agrawal, S. Kumar and A. K. Mishra, "Credit card fraud detection: a
case study," 2nd International Conference on Computing for Sustainable
Global Development, New Delhi, 2015, pp. 5-7.

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

[14] I. Benchaji, S. Douzi and B. E. Ouahidi, "Using genetic algorithm to
improve classification of imbalanced datasets for credit card fraud
detection," In International Conference on Advanced Information
Technology, Services and Systems, pp. 220-229. Springer, Cham, 2018.

[15] I .Sohony, R. Pratap and U. Nambiar, "Ensemble learning for credit card
fraud detection," In ACM India Joint International Conference on Data
Science and Management of Data, pp. 289-294. 2018.

[16] I. Sadgali, N. Sael and F. Benabbou, "Fraud detection in credit card
transaction using neural networks," In Proceedings of the 4th
International Conference on Smart City Applications, pp. 1-4. 2019.