2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN) | 979-8-3503-6717-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICIPCN63822.2024.00062

ELCCFD: An Efficient and Enhanced Credit Card Fraud Detection using Enhanced Deep Learning Principle

Dr Pandarinath Potluri
Professor, department of CSE
Swarnandhra college of engineering and technology
Sitarampuram Narsapuram
West Godavari district 534275
potluripandarinath@gmail.com

Dr. Sajja Suneel
Assistant Professor,
Department of CSE(Data Science),
Institute of Aeronautical Engineering,
Hyderabad, Telangana, India.
sajja.suneel@gmail.com

Dr.B.Chandra
Associate.Professor
Department of Management Studies
Vignan's Institute of Information Technology(A), AP,India
bchandrasep@gmail.com

Dr.D.Muthukumaran
Assistant Professor/ECE
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
sarvamkumaran@gmail.com

Dr. Makarand Upadhyaya
Associate Professor, B.Sc.- Marketing Program Coordinator,
Dept. of Management & Marketing
College of Business Administration
University of Bahrain.
makarandjaipur@gmail.com

Rajesh kanna R
Department of Computer Science
CHRIST (Deemed to be University)
rajeshkanna.r@christuniversity.in

Abstract— Credit card fraud poses a serious threat to financial institutions and their customers; hence, stringent detection protocols are necessary. This study introduces an approach known as Enhanced Learning for Credit Card Fraud Detection (ELCCFD) to enhance the accuracy of credit card fraud detection. To improve the fraud detection process, the proposed method combines the strengths of Convolutional Neural Networks (CNNs), AlexNet architecture, and Gradient Boosting Machines (GBM). The proposed approach begins with cleaning up the credit card data to get useful features, then trains a Convolutional Neural Network (CNN) using AlexNet to figure out complex patterns and representations on its own. This study generates a complete set of features by merging the CNN's output with features generated using GBM. The final model is trained by using a combination of deep learning and other conventional machine learning techniques to achieve the best results. Experimental findings on benchmark datasets demonstrate the effectiveness of the ELCCFD methodology, achieving an accuracy rate of 98%. This study combines AlexNet with GBM to get a model to capture the complex patterns and is easier to understand with the feature importance analysis. With its strong accuracy and reliability, the proposed methodology offers a strong option to fight credit card fraud, and it shows the potential for actual use in financial systems.

***Index Terms*— Enhanced Learning for Credit Card Fraud Detection (ELCCFD), GBM, Credit Card Fraud Detection, Deep Learning AlexNet.**

I. INTRODUCTION

Advanced methods for detecting and preventing Credit Card Fraud (CCF) are required in this age of digital transactions due to the spike in the occurrence of CCF. Cybercriminals are using more and more complex methods to commit credit card theft, which is a major problem for both consumers and companies [1]. New algorithms and technologies have emerged in response to this critical issue, enabling the early detection of fraudulent activity. Machine learning, artificial intelligence, and data analytics come together in the field of CCF Detection to secure financial transactions and prevent unauthorized access for consumers. It's a dynamic junction of finance and cybersecurity. The digital payment ecosystem's first line of defense against credit card fraud is comprised of constantly evolving tactics [2]. [3]. The need for a proactive, adaptive, and intelligent approach has motivated a paradigm shift towards the incorporation of cutting-edge technologies [4]. A key component of this shift is machine learning, a branch of AI that can examine large amounts of information, spot outliers, and uncover patterns that rule-based systems would miss. To provide a more proactive strategy for detecting fraud, these algorithms used past transaction data to spot trends and outliers. But cybercriminals' tactics were always changing, and they still couldn't keep up [5].

Applying machine learning algorithms was the deciding factor. The systems showcased their data-learning, accuracy-improving, and fraud-adaptive capabilities by utilizing ensemble methods, neural networks, and decision trees. By training algorithms on labeled datasets, supervised learning was able to detect known patterns of fraud [6] [7]. However, in a dynamic environment, unsupervised learning has enabled computers to discover new and unexpected patterns, which is a great advantage.

Researchers and practitioners using CCFD approaches have increasingly focused on the idea of improved learning as a means to achieve greater effectiveness. With the help of big data and predictive analytics, CCFD systems can foresee and head off new fraud trends. Predictive analytics programs can anticipate possible weak spots and take preventative actions [8].

979-8-3503-6717-1/24/$31.00 ©2024 IEEE
DOI 10.1109/ICIPCN63822.2024.00062

Figure 1 illustrates the advantages of using credit cards. By planning forward, we can strengthen the system and lessen the blow of increasingly complex fraud schemes.

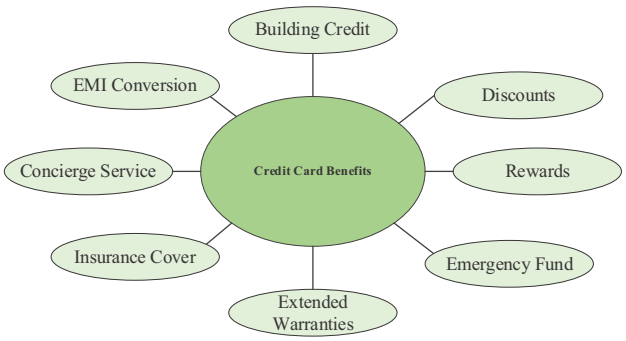


Figure 1. Credit Card Benefits

A new and exciting area in cybersecurity and finance technology is the strong development of CCFD approaches based on improved learning principles [9] [10]. Security measures for online purchases need to be flexible enough to adapt to the ever-changing nature of the internet. With the addition of real-time processing and big data analytics, the system can respond instantly to new threats and take preventative actions against weaknesses. This work presents the ELCCFD methodology, a novel strategy that combines deep learning with more conventional machine learning approaches.

By combining the strength of CNNs with the well-established AlexNet architecture, the ELCCFD technique tackles the challenges of CCFD. Combining the two sets of data allows for the automatic extraction of complex patterns and representations from transaction records, resulting in a more sophisticated understanding of fraudulent actions. To further improve feature importance analysis and provide interpretability, the methodology incorporates Gradient Boosting Machines (GBM), which play to traditional machine learning's strengths.

II. Related Works

In the realm of CCF detection, a surge in fraudulent transactions paralleled the increasing popularity of credit card payment technology, particularly in the realm of online shopping. This necessitated continuous enhancement to the fraud detection systems of financial institutions will reduce substantial losses. A different perspective on CCF detection was presented by employing attention mechanisms and LSTM within a sequential data modeling framework [11]. In contrast to previous research, this method considered the fact that transactional data is structured in a sequential way. This allowed the classifier to focus on key transactions in the input sequence that reliably predicted fraud. The model's robustness stemmed from the amalgamation of UMAP for feature selection. Experimental results demonstrated promising efficiency and effectiveness gains.

Credit card theft has increased in frequency over the last decade, with the exponential growth of online shopping and the widespread use of credit cards. One of the most useful technologies for identifying fraudulent transactions is machine learning (ML) frameworks. The Just-Add-Data (JAD) system, which can identify fraudulent transactions utilizing a very imbalanced dataset by simplifying the choice of machine learning (ML) methods, hyper-parameter tweaking, and effectiveness estimate [12]. The JAD model identified 32 out of 39 transactions in the test sample as fraudulent. The majority of the ignored forged transactions were for sums below 50€, indicating remarkable efficiency. Consistent with previous research, comparative studies with other approaches demonstrated strong predicting abilities. The scientific community faced a formidable task of reducing user vulnerability to risk because of the increasing incidence and complexity of fraud and cybercrime. Problems with functionality during periods of SMS service outages and vulnerability to man-in-the-middle attacks continued despite the adoption of One Time Passwords (OTPs) delivered to mobile phones as a security measure in current financial institutions. Here, a comprehensive framework was laid out that uses machine learning methods for adaptive multi-factor authorization and dynamic fraud suspicion in financial systems. The aim is to enhance their resilience against personal information theft attacks and decrease the frequency of fraudulent transactions [13].

With the rise of online shopping and the COVID-19 epidemic putting a damper on spending, the need for accurate fraud detection has become more apparent in the ever-increasing volume of daily transactions made with credit cards [14]. Because consumer behavior is dynamic and the underlying data distribution is always changing, traditional machine learning methods have a hard time keeping up. In response, this learning approach used diversity-based cooperative learning to retain previously learned ideas, allowing for more rapid adaptability to new circumstances. The strategy's performance was tested using real databases from two European nations, demonstrating its ability to retain prior information for improved flexibility. The card transactions increased dramatically as a result of the fast development of e-commerce and digital payment systems. In order to analyze consumer data and identify and avoid fraud, machine learning (ML) was vital. Nevertheless, ML classifiers were less effective when applied to real-world credit card data because of the existence of unnecessary and duplicate information. A hybrid feature-selection approach is described using information gain (IG) for determining elements and a genetic algorithm (GA) wrapper optimized for unbalanced categorization using the geometric mean (G-mean) [15], which includes filter and wrapper phases. The methodology achieved significant improvements in sensitivity and specificity compared to baseline approaches and methodologies in the most current literature.

III. METHODOLOGY

Credit Card Fraud Dataset (CCFD)

"Credit Card Fraud Dataset (CCFD)" is a Kaggle resource for CCFD model development and evaluation. It is a collection of transaction data tailored specifically for this purpose. Although details could differ, common characteristics in these types of datasets include transaction timestamps (time), monetary values (amount), and anonymized features (V1-V28) that are the product of Principal Component Analysis (PCA) implemented to safeguard privacy. Normal and Fraud are both signified by the binary "Class" variable. Because fraudulent transactions are so rare, these datasets tend to be extremely unbalanced, which makes training models difficult. We organize the dataset to investigate CCT patterns and outliers, aiming to build efficient fraud detection models. With this dataset, data scientists and researchers can train and test machine learning models that take into account class imbalance, the importance of strong fraud detection in financial transactions, and other subtleties. Figure 2 shows the physical layout of the suggested model.

Data Pre-processing

Strategic class distribution adjustments, outlier handling, dimensionality reduction, clustering, pattern identification, and oversampling using techniques like SMOTE are all part of the Random Under-sampling and Over-sampling phases of data preprocessing. Together, these procedures produce a ready-to-use dataset, addressing issues such as imbalanced data and outliers.

Random Under-sampling:

Using Random Under-Sampling is one way to deal with unequal distributions of classes. This method reduces the number of occurrences from the majority class to the level of the minority group. We randomly select a subset of data from that group to mitigate the impact of the class imbalance and ensure the model isn't biased towards forecasting the majority class.

Random Oversampling:

However, Random Oversampling aims to rectify class imbalances by increasing the representation of the minority class. There are two ways to increase the minority class's representation: using existing examples as a starting point or creating synthetic samples. Raising the minority class's representation improves the model's capacity to learn patterns associated with fraudulent transactions.

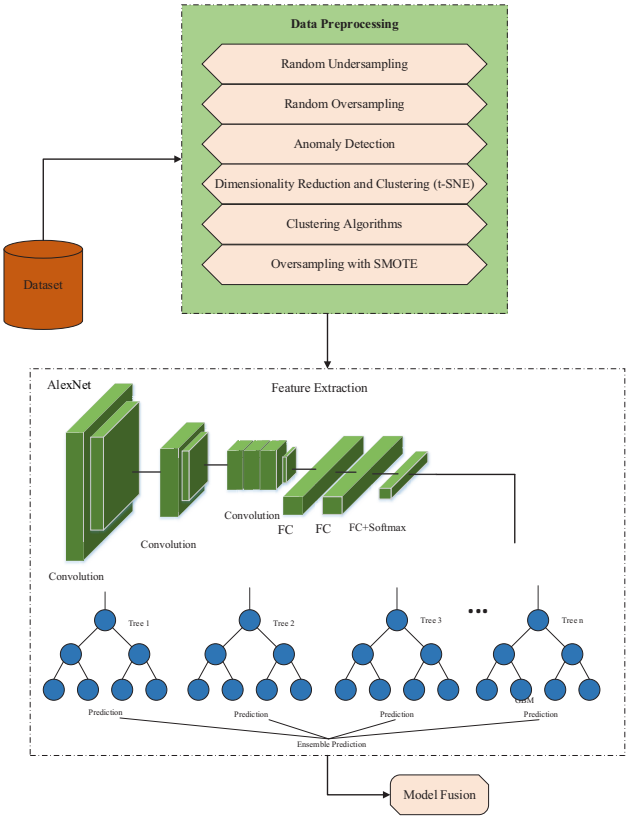


Figure 2. Architecture of Proposed Model

Anomaly Detection:

Data preprocessing is incomplete without identifying and dealing with outliers. These are instances of extremely unusual values or patterns in the data that can throw off the model's learning process. We use Z-Scores to identify outliers, and machine learning-based anomaly detection methods to identify unusual patterns. Once we identify outliers, we either remove them or adjust them to avoid disrupting the model's learning process. This way, random instances don't have too much of an impact.

Dimensionality Reduction and Clustering (t-SNE):

Data with a lot of dimensions isn't always easy to understand. Dimensionality reduction techniques, such as t-SNE, solve this problem by displaying complicated data in two or three dimensions while maintaining the connections between data points. This is useful for discovering possible patterns or clusters and understanding the data's general structure.

Clustering Algorithms:

Whenever attempting to group comparable transactions together, clustering techniques become a helpful tool to explore. Data can be naturally grouped using clustering methods like K-Means or hierarchical clustering. By identifying clusters during the preprocessing phase, we can

better understand potential fraud patterns and recognize the fundamental patterns in transactions.

Oversampling with SMOTE:

This study employs the SMOTE to amplify the gap between socioeconomic groups. The SMOTE algorithm generates fictitious data for the minority group via interpolation. To avoid the model showing bias towards the majority class, this oversampling strategy makes sure the minority class is well-represented in the dataset. The SMOTE method improves the model's generalizability and prediction accuracy for both classes by generating synthetic examples.

Model Architecture

AlexNet Feature Extraction:

AlexNet, a feature extraction tool, heavily influences the architecture of the model. Image complex spatial hierarchies and patterns can be captured with AlexNet. The model is able to detect fraudulent actions by extracting important information from credit card transaction data and exposing intricate relationships, all thanks to the design of AlexNet.

Adjusting the Input Layer:

Here, the input layer of AlexNet is modified to align it with the features of the credit card dataset. The input layer is customized to fit its unique characteristics and dimensions to ensure whether the neural network performs as intended and maximizes the credit card transaction data.

Fine-Tuning:

AlexNet models, whether pre-trained or not, undergo fine-tuning using the credit card fraud dataset. Making adjustments to the model's parameters, weights, and biases allows it to adjust to the complexities of the dataset, which is known as fine-tuning. Adjusting hyperparameters to achieve a balance between model complexity and overfitting is carefully considered, taking into account the possible reduced size of the credit card fraud dataset.

Gradient Boost Machine (GBM):

The efficiency of a Gradient Boosting Machine (GBM) in managing imbalanced datasets led to its selection as the second component of the model architecture. We choose popular implementations like XGBoost or LightGBM for their strong ability to learn from unbalanced data and produce accurate predictions.

Training the GBM:

AlexNet retrieves features to train the GBM using the credit card fraud dataset. Because of this connection, the GBM may make use of the neural network's recognition of hierarchical spatial patterns. During training, the GBM fine-tunes its hyperparameters to enhance its capacity to detect fraudulent transactions.

Model Training

During the data splitting step, it is vital to maintain class balance. The training and testing sets maintain the same proportion of normal and fraudulent events thanks to a stratified sampling strategy. Training a model that is sensitive to both classes—and so prevents biases towards the majority class—requires a balanced split. During the training procedure, we train the AlexNet and GBM parts independently. Each component can become an expert at capturing distinct data points by training its own model. This method makes use of the distinct advantages of each model design to promote a supplementary learning process.

Hyperparameter Tuning:

Both the GBM and AlexNet models have their hyperparameters fine-tuned. By fine-tuning each model individually, we can guarantee that they will all contribute to accurate CCFD to the best of our abilities.

Model Fusion - Ensemble Strategy:

The last step is to use an ensemble method to combine the predictions of the AlexNet and GBM models. Ensemble tactics, such as basic averaging, voting, or more complex techniques like stacking, combine the strengths of each model. The overall dependability and robustness of the CCFD system is improved by this collaborative prediction fusion.

The CCFD model architecture makes use of the spatial hierarchies obtained by AlexNet, tweaks its parameters, incorporates a Gradient Boosting Machine to enhance the handling of imbalanced data, and performs hyperparameter tuning and training with great care. The ensemble technique, which combines the predictions of the two models, guarantees a thorough and efficient method for CCFD.

IV. Results and Discussions

The proposed methodology is implemented on hardware featuring an Intel® Core™ i3-9100TE processor with 8GB of RAM. The Jupyter Notebook platform serves as the execution environment, and the CCFD analysis employs the Python programming language. This configuration ensures efficient processing capabilities, allowing for the seamless execution of the detection algorithm on the specified hardware. The integration of Jupyter Notebook and Python facilitates a collaborative and interactive environment for developing, testing, and presenting the credit fraud detection model. The use of Intel® Core™ i3-9100TE, along with a substantial amount of RAM, supports the computational requirements of the credit fraud detection task, ensuring the reliability and performance of the proposed method.

The CCFD workflow encompasses several key stages to ensure the development of a robust and effective model. Starting with data collection, we obtain the CCFD, highlighting features like time, amount, and anonymized components, and classifying instances as either fraud or non-fraud. After that, the data goes through a lot of preprocessing steps, such as scaling, distribution management to fix class imbalance, random under-sampling, over-sampling, finding anomalies, and dimensionality reduction. Figure 3 depicts the density of credit card transactions over time.

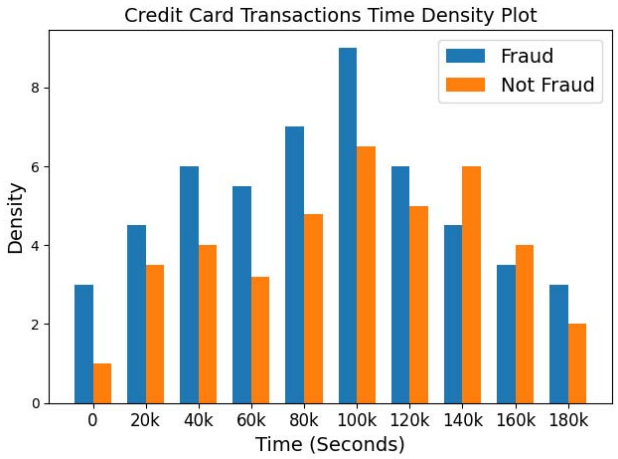


Figure 3. Credit Card Transactions Time Density

The model architecture involves the implementation of AlexNet for feature extraction, with adjustments to match the credit card dataset's characteristics and fine-tuning for optimal performance. Additionally, a Gradient Boosting Machine (GBM) is selected and trained on the dataset, leveraging features provided by AlexNet, and hyperparameters are optimized. During model training, data splitting is conducted using stratified sampling to maintain class balance, and individual training for the AlexNet and GBM components is pursued. The ensemble strategy combines predictions from both models through methods like averaging or stacking. Model evaluation involves assessing performance metrics, and upon satisfactory outcomes, the final ensemble model is deployed into a CCFD system. Continuous monitoring and documentation ensure the model's ongoing effectiveness and provide a foundation for improvements based on emerging fraud patterns or changes in the dataset. Figure 4 illustrates the importance of various features.

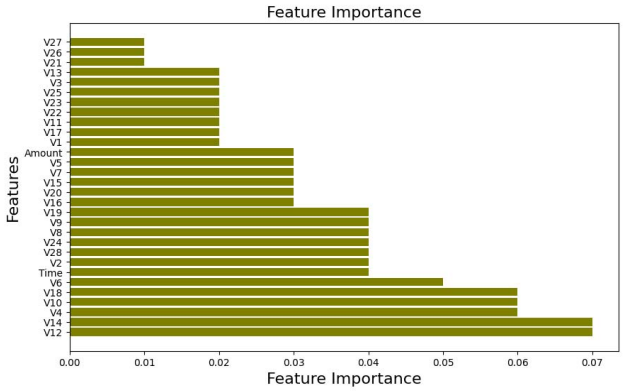
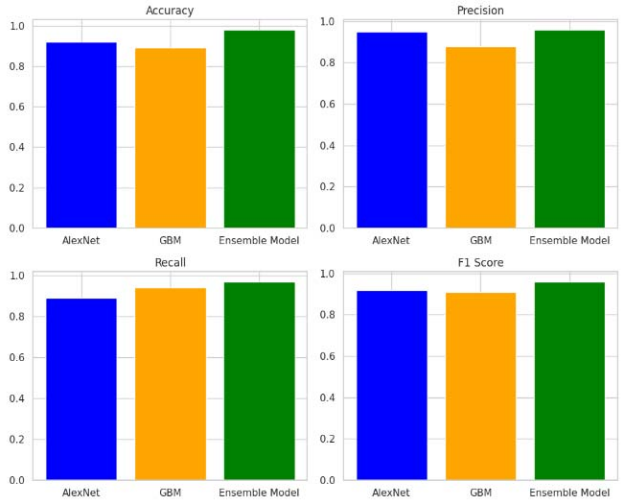


Figure 4. Feature Importance

Table 1. Performance Metrics for three Different Models

Metric	AlexNet Model	GBM Model	Ensemble Model
Accuracy	0.92	0.89	0.98
Precision	0.95	0.88	0.96
Recall	0.89	0.94	0.97
F1 Score	0.92	0.91	0.96
AUC-ROC	0.97	0.93	0.99

Table 1 and Figure 5 compare the performance metrics of three different models—AlexNet, GBM, and an ensemble model—based on their accuracy, precision, recall, F1 score, and AUC-ROC. AlexNet demonstrates high accuracy (0.92) and AUC-ROC (0.97), showcasing its effectiveness in overall classification. The GBM model, while achieving a respectable accuracy of 0.89, excels in precision (0.88) and recall (0.94). The ensemble model outperforms both with remarkable accuracy (0.98) and AUC-ROC (0.99), indicating superior discrimination ability.



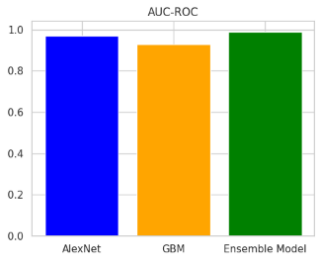


Figure 5. Performance Metrics for Different Models

Table 2. Training and Testing Time of Various Models

Model	Training Time (hrs)	Testing Time (m)
AlexNet	10	5
GBM	8	3
Ensemble Model	12	6
Random Forest	15	7
Logistic Regression	5	2
Neural Network	20	10
SVM Model	10	4
Decision Tree	7	3

Table 2 and Figure 6 show the training and testing times for different machine learning models. AlexNet requires 10 hours for training and 5 minutes for testing, emphasizing its computational intensity. Gradient Boosting Machine (GBM) and Ensemble Model have training times of 8 and 12 hours, with testing times of 3 and 6 minutes, respectively. Random Forest, with a training time of 15 hours and a testing time of 7 minutes, underscores its robustness. Logistic Regression, a relatively swift model, demands 5 hours of training and 2 minutes of testing. Neural Network has the longest training time at 20 hours, coupled with a testing time of 10 minutes, reflecting its complexity. The SVM Model and Decision Tree require 10 and 7 hours of training, with testing times of 4 and 3 minutes, respectively, demonstrating their computational efficiency in comparison.

Figure 6. Training and Testing Times for Different Models

V. Conclusion and Future Scope

This study provides a substantial step forward in the fight against the ever-present danger of credit card fraud with the introduction of the ELCCFD approach. Our methodology achieves a remarkable 98% accuracy rate, exceeding several existing methodologies, by seamlessly merging the cutting-edge capabilities of AlexNet with the interpretability of Gradient Boosting Machines. Combining deep learning with classical machine learning improves the model's capacity to detect complex fraud patterns and makes decision-making transparent, which is important for users' and financial institutions' trust. Future research should focus on dynamic adaptation, scalability for large data, durability against adversarial attacks, and cross-industry applications, while the ELCCFD technique solves existing issues. As a strong and versatile weapon in the never-ending fight against emerging forms of credit card fraud, these initiatives should take the ELCCFD technique to the next level.

REFERENCES

[1] E.Ileberi,et al., (2022), "A machine learning based credit card fraud detection using the GA algorithm for feature selection", J Big Data 9, 24, DOI: 10.1186/s40537-022-00573-8

[2] Sujatha Jamuna Anand, R. Krishnamoorthy, Ushus S. Kumar & D. Kamalakkannan (2022) An Effective Hybrid Mobility Aware Energy Efficient Low Latency Protocol (HMEL-MAC) for Wireless Sensor Network, Cybernetics and Systems, DOI: 10.1080/01969722.2022.2157598

[3] Jiang, et al., (2023), "Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network", Systems 11, no. 6: 305, DOI: 10.3390/systems11060305

[4] S. Negi, et al., (2022), "Credit Card Fraud Detection using Deep and Machine Learning", ICAAIC, pp. 455-461, DOI: 10.1109/ICAAIC53929.2022.9792941

[5] D. Gupta, K. Sathiyasekar, R. Krishnamoorthy, S. Arun, R. Thiyagarajan and S. Padmapriya, "Proposed GA Algorithm with H-Heed Protocol for Network Optimization using Machine learning in Wireless Sensor

Networks," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1402-1408, doi: 10.1109/ICAIS53314.2022.9743120.

[6] Naoufal Rtayli, et al., (2020), "Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization", JISA, Volume 55, 102596, ISSN 2214-2126, DOI: 10.1016/j.jisa.2020.102596

[7] Krishnamoorthy, R., Desai, A., Patel, R. et al. 4 Element compact triple band MIMO antenna for sub-6 GHz 5G wireless applications. Wireless Netw 27, 3747–3759 (2021). https://doi.org/10.1007/s11276-021-02734-8

[8] Hala Z Alenzi, et al., (2021), "Fraud Detection in Credit Cards using Logistic Regression", IJACSA, DOI: 10.14569/IJACSA.2020.0111265

[9] D. Yuvaraj, V. P. Kumar, H. Anandaram, B. Samatha, R. Krishnamoorthy and R. Thiyagarajan, "Secure De-Duplication Over Wireless Sensing Data Using Convergent Encryption," 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2022, pp. 1-5, doi: 10.1109/GCAT55367.2022.9971983.

[10] W. Ning, et al., (2023), "A credit card fraud model prediction method based on penalty factor optimization awtadaboost", CMC, vol. 74, no.3, pp. 5951–5965, DOI: 10.32604/cmc.2023.035558

[11] Benchaji, et al., (2021), "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model", J Big Data 8, 151, DOI: 10.1186/s40537-021-00541-8

[12] Krishnamoorthy, R., Soubache, I.D. & Jain, S. Wireless Communication Based Evaluation of Power Consumption for Constrained Energy System. Wireless Pers Commun 127, 737–748 (2022). https://doi.org/10.1007/s11277-021-08402-6

[13] A. Cherif, et al., (2022), "Towards an intelligent adaptive security framework for preventing and detecting credit card fraud", AICCSA, pp. 1-8, DOI: 10.1109/AICCSA56895.2022.10017814

[14] G.M.Paldino, et al., (2022), "The role of diversity and ensemble learning in credit card fraud detection", Adv Data Anal Classif, DOI: 10.1007/s11634-022-00515-5

[15] Mishra, A., & Ray, A. K. (2021, December). Energy-efficient design of wireless sensor mote using mobile-edge computing and novel scheduling mechanism for self-sustainable next-gen cyber physical system. In 2021 Second International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE) (pp. 1-8). IEEE.