[1]Vishakha D. Akhare

[2]Dr. L. K. Vishwamitra

Machine Learning Models for Fraud Detection: A Comprehensive Review and Empirical Analysis

Abstract: - An in-depth familiarity with ML and DL models for fraud detection is essential due to the growing frequency and complexity of fraudulent activity across many domains. Despite the abundance of research on the subject, empirical analyses of these models, especially in their real-time implementations, are typically lacking. This study fills that need by meticulously reviewing and analysing ML and DL models developed for fraud detection. We draw attention to the shortcomings of existing approaches, which are crucial in the ever-changing field of fraud detection and include problems with recall, scalability, complexity, precision, and accuracy. By evaluating various ML and DL models using these measures, our evaluation method is based on a rigorous empirical approach. Provided that insights into the practical consequences as well as flexibility of each model in real-time circumstances, they thoroughly assess their performance. There are many ways in which this work will be useful; for example, it will help professionals choose the best models for their fraud detection needs, improve academic knowledge of these models in practice, and open the door to more studies that will concentrate on developing better fraud detection tools. This comprehensive research gives academics and companies a foundation for better, more effective and more scalable fraud detection systems in this period of essential digital security.

Keywords: Detection of Fraud, Machine Learning, Deep Learning, Empirical Analysis, Model Comparison

I. INTRODUCTION

Fraud has created severe worries regarding the security of digital transaction and interaction systems. Due to the surge in financial frauds and identity thefts, cutting-edge detection and prevention technologies are needed. DL and ML is approaches are powerful fraud-fighting tools because they can learn and adapt from tiny data samples. However, whether these models function in practice has been debated and studied. Complex design and implementation make DL and ML fraud detection tough. These models must be precise, fast, and scalable to handle massive volumes of data in real-time systems. Because fraud methods are dynamic, these models must be adaptable to handle new fraud types. The literature has many studies on various elements of ML and DL models, but little empirical research compares them to critical performance criteria including accuracy, scaling, precision, delay, complexity, and recall.

This study investigates ML as well as DL fraud detection methods to fill this knowledge gap. The first element of the approach assesses ML and DL models' weaknesses and determines how to solve them to prevent fraud. A comprehensive review of these models using multiple performance indicators is our second recommendation. This empirical study may assist researchers and practitioners choose real-time models by revealing their pros and cons.

The work has major implications. Fraud detection system developers and implementers benefit from our extensive empirical analysis of ML and DL models. By enhancing the selection of models and fraud detection, our insights will help safeguard digital ecosystems from fraud. Academics and specialists may use this material as a comprehensive roadmap for future fraud detection advances.

1.1 Motivation & Contribution

Motivation:

In a world where everything is becoming digitized, the urgent need to improve fraud detection techniques is driving this study. From healthcare to the financial industry, fraud has grown in sophistication and impact. The traditional ways of identifying fraudulent activities are quickly becoming surpassed by these sophisticated dangers. Models based on Deep Learning (DL) and Machine Learning (ML) have shown potential in meeting these difficulties. Nevertheless, insufficient knowledge and actual comparisons across important performance indicators sometimes impede their practical use. The comprehensive research and analysis is driven by a desire to fill this knowledge and

[1,2] Department of Computer Science & Engineering, Oriental University, Indore, India.

vishuakhre@gmail.com [1], lkvishwamitra@gmail.com 2

application gap by shedding light on the strengths and weaknesses of existing ML and DL models for fraud detection.

Contribution: Several important advances in the area of fraud detection using ML and DL models are made in this paper:

- **Summarized Empirical Analysis:** Using important criteria like accuracy, scalability, precision, latency, and recall, we provide a comprehensive empirical evaluation of several ML and DL models. When it comes to fraud detection, this study is one of the first to provide a comprehensive overview of these models.
- **Finding Model Limitations:** The study we conducted highlights the difficulties and limits of existing algorithms for DL and ML when it comes to fraud identification. In order to identify what needs enhancing or innovating, academics and practitioners must have this understanding.
- **Advice on Model Selection:** This research compares models across several criteria to help choose the best model with ML and DL for different fraud detection jobs. Professionals with fraud detection systems will benefit from this guidance.
- **Theory-Practice Bridge:** Real-world insights are gained from this evaluation of theoretical research and actual implementation. This is essential for connecting academic research to corporate needs.
- **Future Research Foundation:** The conclusions and methodology in this paper provide the groundwork for future research. They identify boundaries and gaps to guide future research on enhancing DL and ML fraud detection algorithms.

In conclusion, our study advances both theoretical and applied fields by increasing our understanding of fraud detection DL and ML and providing practical advice on how to apply them.

II. DETAILED STUDY OF FRAUD DETECTION METHODS:

Many online fraud detection algorithms have been developed with varied operational characteristics and functional application situations. Choose features to solve unbalanced classification issues [1]. This method approaches selecting characteristics as a MOP and finds a small number of features with excellent classification accuracy. There is a tendency for traditional MOPs to ignore variety in the resolution space in favor of finding an optimum solution. In order to get over this issue, the authors provide a multimodal MOP (MMOP) architecture that searches for a great front Pareto in target space and several similar optimal Pareto responses in space for feature. In addition, they suggest a process that is driven by competition to improve current MMEAs, which would increase the variety of solutions and help find the required Pareto fronts. The experimental findings show that this technique improves classification accuracy and provides more comparable feature subsets, making it beneficial in unbalanced classification issues like credit card fraud detection.

As mentioned in [2], click fraud is a major problem in the world of internet advertising. Click fraud happens when dishonest people alter pay-per-click ads to boost website income or drain advertising budgets. Hybrid ensembles detect click fraud using DL and ML. The architecture uses a Random Forest (RF) classifier, CNN, and The opposite direction Long Short-Term Memory network for categorization and feature extraction. Categorical traits and data imbalance are addressed during preprocessing to increase data reliability. The recommended ensemble design defends against pay-per-click advertising assaults by outperforming current ensembles and traditional models in precision, accuracy, sensitivity, F1-score, and specificity.

As indicated in [3], technology's rapid digitization of payment patterns has increased financial fraud risk. This research forecasts fraudulent credit card transactions using the IEEE-CIS Fraud Detection Dataset. The proposed paradigm divides operators into old and new categories via user separation. DNN and CatBoost models are used for each group. The study addresses feature engineering, feature modification, and imbalanced datasets to increase detection accuracy. Experimental data reveal good AUC values in CatBoost and DNN, suggesting the model might detect credit card fraud. Telecom networks are increasingly threatened by fraudsters' clever concealing methods [4]. Our approach is a original fraud detection method that considers spatiotemporal user activity patterns. The model incorporates dynamic call patterns, interactive and statistical features, sequential patterns, and structural patterns. These patterns are obtained through probabilistic models, attention-based Graph-SAGE and Hidden Markov

Models. The model scores users for fraud, identifying probable scammers. Extensive studies on practical telecom data confirm the model's capacity to properly depict user behavior and increase fraud detection over previous techniques.

Reference Number	Name of Method	Advantages	Limitations	Details of Work	Future Scope
[1]	Multimodal Multiobjective Evolutionary Algorithm	- Effective for imbalanced classification problems. - Finds multiple equivalent feature subsets.	- Convergence-first selection criterion limits diversity.	- Proposed a competition-driven mechanism. - Verified on CEC2019 dataset. - Applied to credit card fraud detection. - Improved classification accuracy.	Explore optimization of competition-driven mechanism.
[2]	Ensemble Architecture (CNN based BiLSTM-RF)	- Efficient click for identifying fraud. - Combines CNN, BiLSTM, and RF. - Preprocesses data for better reliability. - Achieved high accuracy.	- Limited dataset information. - Experimental results may vary in different scenarios.	Further enhance preprocessing techniques.	
[3]	Fraud Detection Model	- Predicts fraudulent credit cards. - Addresses imbalanced datasets and feature engineering. - Achieves good AUC scores.	- Focuses on user separation. - Aims at credit card fraud, not transaction fraud.	Improve user separation techniques.	Investigate applications in various fraud detection scenarios
[4]	Spatial and Temporal Fraud Identification Method	- Focuses on spatial-temporal features. - Utilizes statistical, sequential, and structural patterns. - Effective in detecting fraudsters.	- May require significant computational resources.	Explore optimization for efficiency.	
[5]	Weight-Tuning Hyperparameters	- Balances fraudulent and lawful transactions. - Utilizes CatBoost, XGBoost, and deep learning. - Achieves high AUC-ROC, accuracy, recall, as well as score of F1.	- Data-dependent results. - Deep learning may require more data.	Investigate further data augmentation techniques.	
[6]	Blockchain and Smart Contract-Based ML Approach	- Facilitates inter-organizational collaboration. - Ensures data privacy. - Achieves high testing accuracy.	- Mining time impacted by data volume and difficulty level.	Explore scalability for larger networks.	

[7]	Synthetic Image Generation for ID Card Fraud Detection	- Increases data volume. - Minimizes false alarms.	- Slight loss in performance for screen capture PAIS.	Investigate methods to improve screen capture PAIS.	
[8]	Mixed Attribute Outlier Detection	- Handles mixed attribute data effectively. - Utilizes neighborhood rough set and multigranulation relative entropy.	- Limited evaluation on public data samples.	Validate the model on various datasets.	
[9]	Dilated Convolutional Transformer based GAN	- Improves generalization and accurateness for time series anomaly detection.	- May still face method failure and lowest generality.	Explore strategies to mitigate model collapse.	
[10]	Network Intrusion Detection System (INE-SRC-ATM)	- Utilizes pattern matching and self-replication. - Effective in intrusion detection.	- Requires early identification of damage for self-healing.	Improve the self-triggering mechanism.	
[11]	Fraud Detection on E-Wallet Platform	- Achieves high detection accuracy with LightGBM. - Reduces false alarms.	- Data-specific results.	Investigate applicability to other e-wallet platforms.	
[12]	Few Shot Traffic Multiple Categorization(SPN)	- Supports out-of-distribution detection. - Integrates twin networks for improved performance.	- Limited experimentation details.	Conduct more experiments in diverse scenarios.	
[13]	Process Based Detection of Fraud	- Detects claim of insurance correlated frauds using sequence mining.	- Limited validation on a specific hospital's data.	Validate the methodology on multiple healthcare datasets.	
[14]	Heterogeneous Feature Augmentation for Ponzi Scheme Detection	- Captures heterogeneous information for Ponzi detection. - Improves performance of existing methods.	- Specific to Ethereum datasets.	Extend to other blockchain networks.	
[15]	Proof of Sense Consensus Machine for DSA System	- Functions based on spectrum detecting processes. - Detects fraudulent/unauthorized spectrum access. - Enables spectrum auctions and fraud detection.	- Experimental performance not discussed.	Conduct performance analysis on the proposed mechanism.	Explore further improvements in deep learning algorithms for fraud detection
[16]	FBNE-PU for Tax Evasion Detection	- Combines basic features and network embedding. - Utilizes pseudo labeling and MLP for detection.	- Limited discussion on specific datasets.	Validate on diverse real-world tax evasion datasets.	

[17]	FraudAuditor	Holistic modeling of visit relationships - Expert knowledge integration - Three-stage approach	Reliance on expert knowledge - Case study limited to healthcare	Detecting collusive fraud in health insurance using a visual analytics approach, improving community detection, and case studies.	Explore automation of expert knowledge integration
[18]	Deep Learning Algorithms	- Improved fraud detection accuracy - Comparative analysis	- Low accuracy of traditional methods	Deep learning for credit card fraud detection and conducting empirical analysis for optimization.	
[19]	CS-OCAN	- Improved detection accuracy - Modified autoencoders	- Ineffectiveness with complex situations	Proposing a one-class classification model for fraud detection with a focus on maximizing inter-class distances.	Further refinement and application in real-world scenarios

Table 1. Comparative Evaluation of Different Models used for Fraud Detection Analysis

The proliferation of credit card usage in e-commerce has led to an increase in fraudulent activities, resulting in the need for effective fraud detection methods, as discussed in [5]. This study introduces weight-tuning hyperparameters, Bayesian optimization, and ensemble learning techniques to enhance fraud detection using machine learning models such as CatBoost, LightGBM, XGBoost, and deep learning. Evaluation metrics such as ROC-AUC, precision, recall, F1-score, and MCC are used to assess the performance of these models. The results demonstrate significant improvements over existing methods and highlight the effectiveness of hyperparameter tuning and ensemble learning in handling unbalanced datasets and improving fraud detection. Financial fraud remains a persistent challenge, even with technological advancements, as discussed in [6]. Blockchain and smart contracts are suggested for strong machine learning-based e-commerce fraud detection. This method ensures data privacy, automates model updates, and incentivizes organizations to contribute data for model improvement. Experimental results reveal high testing accuracy and Fbeta score, demonstrating the effectiveness of the blockchain-based approach under different data volumes and difficulty levels.

Remote biometric authentication for online services has become common but also vulnerable to fraud, as noted in [7]. To address this, the study explores methods for synthetically generating ID card images to increase training data for fraud-detection networks. These methods employ computer vision algorithms and Generative Adversarial Networks (GANs) to create synthetic images. Experimental results show minimal performance impact for print/scan Presentation Attack Instrument Species (PAIS) and only a 1% loss in performance for screen capture PAIS, indicating the feasibility of supplementing databases with synthetic images for fraud detection. Outlier detection is crucial in various fields, including intrusion detection and credit card fraud detection, as discussed in [8]. This article presents a novel mixed attribute outlier detection method based on multigranulation relative entropy, leveraging neighborhood rough sets. The method constructs a neighborhood system, computes neighborhood entropy, and defines multigranulation relative entropy-based matrices to assess outlier degrees. Experimental comparisons demonstrate the adaptability and effectiveness of the proposed technique.

Time series anomaly detection (TSAD) is essential but challenging, as addressed in [9]. To enhance accuracy and generalization, a Dilated Convolutional Transformer-based GAN (DCT-GAN) is proposed. DCT-GAN utilizes multiple generators and a single discriminator, incorporating dilated convolutional neural networks and Transformer blocks to capture fine-grained and coarse-grained time series information. Weight-based mechanisms balance the generators. Experimental results show improved performance compared to existing GAN-based methods. Intrusion detection is vital for network security, as discussed in [10]. This study proposes a pattern-matching, self-replicating intrusion detection system. The system identifies potentially dangerous symptoms, alerts other nodes, and initiates defense mechanisms. The model demonstrates high accuracy in intrusion detection and self-replication triggering.

E-wallets' popularity has introduced new challenges, including fraud, as discussed in [11]. The study utilizes machine learning techniques to detect fraudulent activity in e-wallet platforms. Feature engineering and LightGBM-based detection achieve high accuracy and a significant reduction in false alarms. Traffic classification plays a crucial role in cyber security, as noted in [12]. SPN is a quick traffic multi-classification tool that detects out-of-distribution. SPN excels in intrusion detection with dual systems, margin loss, and nnPU. Healthcare systems face increasing fraudulent billing cases, as discussed in [13]. This work presents a process-based fraud detection methodology using sequence mining concepts to detect insurance claim-related frauds. The methodology generates frequent sequences, computes confidence values, and identifies anomalies, providing a new approach for fraud detection in healthcare.

Blockchain technology brings new challenges, including scams, as addressed in [14]. The study focuses on the scheme of Ponzi detection and introduces HFAug, a module for capturing various information associated with account behavior patterns. HFAug significantly improves detection performance in Ethereum datasets & samples. Effective spectrum management is crucial in beyond 5G networks, as discussed in [15]. A novel consensus mechanism, "Proof-of-Sense," is proposed for blockchain-based dynamic spectrum access (DSA) systems. It leverages spectrum sensing procedures and cryptographic key sharing to detect fraudulent spectrum access and enables various microservices.

Tax evasion detection is a pressing issue, as discussed in [16]. FBNE-PU, a tax evasion detection framework, integrates basic features, network embedding, and PU learning. It significantly improves detection performance in real-life scenarios using network embedding and pseudo-labeling techniques. In [17], the research addresses collusive fraud in health insurance, a complex problem due to the higher relationship between normal and fraudulent medical visits and the scarcity of labeled information samples. To improve detection accuracy, the authors propose a three-stage visual analytics approach and FraudAuditor. This approach allows users to construct a co-visit network, employs an improved community detection algorithm to identify suspicious groups, and offers a visual interface for investigating and verifying suspicious patient behavior. Case studies validate the approach's effectiveness.

Work in [18] focuses on fraud detection for credit card, emphasizing the need for deep learning algorithms due to challenges like high-class imbalance and evolving fraud nature. The study conducts an extensive empirical analysis, showcasing improvements in F1 value, accuracy, AUC curves and precision. The proposed model outperforms traditional machine learning approaches. In [19], the article introduces the CS-OCAN model for fraud detection, combining autoencoders and Complementary GANs. This approach maximizes inter-class distances and minimizes intra-class variances, improving detection accuracy compared to existing one-class classification models. Graph-based fraud detection is explored in [20], introducing the LGM-GNN model. It incorporates global and local memory networks, outperforming state-of-the-art methods on practical fraud detection data.

The research in [21] focuses on credit card fraud detection with imbalanced data samples. It proposes the CCFDM method, leveraging ensemble learning and a GAN-based ESMOTE technique to improve overall performance and reduce false alarms. In [22], the STAGN method is presented for credit card fraud detection. It employs 3D convolution and spatial-temporal attention to enhance detection performance, demonstrating superiority over other baselines. Work in [23] addresses medical fraud detection with the VAERM model, utilizing Variational AutoEncoders and active learning. The proposed framework improves detection performance and reduces computational requirements. Work in [24] presents the FFD framework for fraud detection, incorporating undersampling, feature selection, and SVDD. A modified PSO algorithm enhances hyperparameter optimization, resulting in effective fraud detection.

Work in [25] introduces behavior- and segmentation-type features for financial fraud detection. Feature selection and removal of time-inhomogeneous features lead to improved performance compared to other classifiers. In [26], quantum support vector machines (QSVM) are applied to card payment fraud detection. A hybrid classical-quantum approach is explored, demonstrating improvements in fraud prevention. Work in [27] suggests an improved Adaboost procedure for credit card fraud detection, incorporating adaptive hybrid weighted self-paced learning and diversity-based weighting, leading to enhanced detection performance.

Graph analysis is utilized in [28] for medicare fraud detection. Traditional ML with graph centrality features outperform GNN, offering substantial cost savings and faster learning delays. Work in [29] discusses secure health insurance fraud detection using AI and blockchain, presenting a systematic survey and taxonomy of security issues

in health insurance scenarios. In [30], machine learning and data mining methods for financial statement fraud detection are reviewed and synthesized. Future research areas include exploring unsupervised and semi-supervised methods and using unstructured data samples.

Telecommunication fraud detection is discussed in [31], specifically Wangiri fraud. Classification algorithms are found to outperform other methods in detecting Wangiri fraud patterns. In [32], data enhancement for behavior-based fraud detection is addressed, leveraging network embedding algorithms to capture co-occurrence relationships. Finally, [33] focuses on financial statement fraud detection, combining numerical and textual data with deep learning models. Empirical results show significant performance improvements in detecting fraudulent financial statements.

Work in [34] focuses on online advertising, where Pay-Per-Click (PPC) advertising is susceptible to malicious clicks. These fraudulent clicks mimic legitimate user behavior, causing financial losses for advertisers and damaging the credibility of online advertising platforms. The paper introduces a tensor-based mechanism for fraud click prediction. By reconstructing data into a high-rank tensor and using tensor decomposition and transformation, hidden information is explored within the data, leading to improved fraud prediction compared to traditional machine learning algorithms. Work in [35] delves into Bitcoin and its association with unlawful activities, emphasizing the need for efficient fraud detection in cryptocurrency transactions. An ensemble learning approach is proposed, incorporating techniques like ADASYN-TL for data balancing and hyperparameter tuning. Multiple classifiers, including Decision Tree, Naive Bayes, K-Nearest Neighbors, and Random Forest, are combined in a stacking model. SHapley Additive exPlanation (SHAP) is used for interpretation. The model outperforms existing methods in terms of various metrics, enhancing fraud detection in Bitcoin transactions.

Work in [36] addresses fraud detection in online microlending, where fraud-agents create fake personal information to help high-risk borrowers evade risk evaluation. The paper presents a machine learning-based solution, employing features extracted from behavior logs. A two-stage detection model is proposed to handle the limited labeled fraud agent examples. The model achieves a precision of 94.30% and successfully identifies fraud-agents on a real online microlending platform. Work in [37] introduces HearLiquid, a low-cost and nonintrusive liquid fraud detection system using acoustic devices. The system measures acoustic absorption and transmission curves (AATC) of liquids at multiple frequencies to identify fraudulent liquids. Challenges like hardware diversity and position variations are addressed through calibration and data augmentation techniques. The proposed system achieves liquid detection accuracy ranging from 92% to 97%.

Work in [38] tackles credit card fraud detection, highlighting the challenge of imbalanced datasets. The paper proposes an improved oversampling method based on the Variational Autoencoder Generative Adversarial Network (VAEGAN) to generate diverse and convincing minority class fraud data samples. Experimental results demonstrate the effectiveness of this method compared to other oversampling techniques. Work in [39] explores the use of Graph Neural Networks (GNNs) for fraud detection. Traditional GNNs are limited by their use of a single type of aggregator and fail to capture information from multiple perspectives and relations. The Multiple Aggregators and Feature Interactions Network (MAFI) is introduced, which uses multiple aggregators, attention mechanisms, and feature interactions to enhance fraud detection on heterogeneous graphs. Work in [40] presents a novel model for credit card fraud detection that focuses on extracting transactional behaviors of users. Time-aware gates, attention modules, and interaction modules are used to capture long- and short-term transactional habits and behavioral changes. The model outperforms existing methods in distinguishing fraudulent from legitimate transactions.

Work in [41] addresses credit card fraud detection by deep learning. Gated recurrent unit (GRU) and long short-term memory (LSTM) neural networks are employed as base learners in a stacking ensemble framework. Class balancing is accomplished using the SMOTE-ENN approach, which combines the synthetic minority oversampling methodology with edited closest neighbor. The recommended strategy improves sensitivity and specificity. A mixture of a dataset resampling approach and a neural network-based classifier ensemble are used in [42] to detect credit card fraud. The ensemble classifier uses AdaBoost with LSTM as the fundamental learner. Combining SMOTE-ENN with synthetic minority oversampling, hybrid resampling is used. The recommended approach outperforms competitors in detection accuracy. For online financial fraud detection, [43] presents TA-Struc2Vec, a graph-learning algorithm. By transforming monetary transaction network graphs into low-dimensional vectors, this technique is able to learn topologies and transaction amount properties. With improved accuracy, F1-score, and AUC, the technique is shown to enhance the efficiency of detecting financial fraud on the Internet. Work in [44]

presents a fraud detection framework using quantum machine learning (QML) enhanced with quantum annealing solvers. The method is evaluated alongside traditional machine learning algorithms on two datasets, demonstrating superior performance, particularly in time series data with high class imbalance operations. Work in [45] addresses fraud detection in behavioral sequences, focusing on healthcare insurance claims. The proposed deep learning architectures process sequential records of patient visits and characteristics, improving fraud detection compared to traditional models. The approach outperforms existing methods in terms of ROC AUC and robustness to data corruption. Work in [46] proposes a secure Serverless Blockchain Enable Task Scheduling (SBETS) intelligent transport system (ITS) to reduce processing and security costs for ITS applications. The system employs a function-based price model and a deep graph convolutional neural network scheme to secure data samples. SBETS is shown to outperform existing ITS systems.

Work in [47] introduces ScoreGAN, a framework for fraud review detection. It incorporates review text and rating scores into the generation and detection process using Information Gain Maximization (IGM) and GLoVe embeddings. ScoreGAN outperforms existing methods in detecting fraudulent reviews. Work in [48] presents CAeSaR, a qualified integration system for data-driven anti-fraud engineering. It uses a three-way taxonomy of function division based on temporal positions and an effective integration scheme called TELSI. CAeSaR achieves improved fraud detection while ensuring decision explainability and minimizing processing costs.

Work in [49] focuses on health insurance fraud detection using deep learning architectures that process sequential records of patient visits. These architectures, combining sequential and tabular data components, outperform state-of-the-art models and improve claims management. Work in [50] addresses fraud detection in health insurance using a representation learning approach called Mixtures of Clinical Codes (MCC). The paper explores the incorporation of MCC, Long Short Term Memory networks, and Robust Principal Component Analysis. The approach outperforms existing models in identifying fraudulent health insurance claims. Thus, researchers have proposed a wide variety of models for detecting frauds in different scenarios. In the next section these models are compared on the basis of different performance metrics, which will assist readers to identify optimal models for different use cases.

III. 3. COMPARATIVE ANALYSIS

Based on the review of existing models used for analysis of frauds in online systems, it can be observed that most of these models vary widely in terms of their internal operations. Thus, in this section we compare these models in terms of precision, accuracy, recall, delay, complexity, and scalability levels. These metrics were quantified into Very Low, Low, Medium, High and Very High depending upon the performance of reviewed models. This comparison will assist readers to identify optimal models for different use cases. Based on this strategy, this performance of these models can be observed from table 2 as follows,

Reference Number	**Name of Method**	**Precision**	**Accuracy**	**Recall**	**Delay**	**Complexity**	**Scalability**
[1]	Multimodal Multiobjective Evolutionary Algorithm	High	High	High	High	Very High	Very High
[2]	Ensemble Architecture (CNN-BiLSTM-RF)	Medium	Very Low	High	High	Very Low	Very Low
[3]	Fraud Detection Model	Low	High	Very Low	Very Low	Low	Low
[4]	Spatial-Temporal Fraud Detection Model	Low	Low	High	Very High	Very Low	Low
[5]	Weight-Tuning Hyperparameters	High	Very High	Very High	Very Low	High	High
[6]	Blockchain and Smart Contract-Based ML Approach	Low	Low	High	High	Low	Very High
[7]	Synthetic Image Generation for ID Card Fraud Detection	Medium	High	Very Low	High	Very Low	Low

[8]	Mixed Attribute Outlier Detection	Low	Medium	Very Low	Medium	Very High	High
[9]	Dilated Convolutional Transformer-based GAN (DCT-GAN)	Low	Very Low	Very High	High	High	Medium
[10]	Network Intrusion Detection System (INE-SRC-ATM)	Low	High	Very Low	Very Low	Very High	High
[11]	Fraud Detection on E-Wallet Platform	High	Very Low	Low	High	Low	Very Low
[12]	Few-Shot Traffic Multi-Classification (SPN)	Very Low	High	High	High	Medium	Medium
[13]	Process-Based Fraud Detection	Low	Very High	Medium	High	Medium	High
[14]	Heterogeneous Feature Augmentation for Ponzi Scheme Detection	Very Low	Very High	Very Low	Very High	Low	Low
[15]	Proof-of-Sense Consensus Mechanism for DSA System	Very High	Low	High	Very High	Low	Medium
[16]	FBNE-PU for Tax Evasion Detection	Low	Very Low	Medium	Low	High	Very High
[17]	FraudAuditor	Medium	Medium	Very High	Very Low	High	Very Low
[18]	Deep Learning Algorithms	Very Low	Very High	High	Very High	High	Very High
[19]	CS-OCAN	Very High	Very High	High	High	Low	Medium

Table 2. Empirical Evaluation of different Models Used for Fraud Detection Analysis

In terms of precision, models like the Multimodal Multiobjective Evolutionary Algorithm, Weight-Tuning Hyperparameters, and several others (e.g., Proof-of-Sense Consensus Mechanism for DSA System, CS-OCAN) demonstrated high precision. The Deep Learning Algorithms and Graph Analysis models also showed very high precision, indicating their effectiveness in correctly identifying fraudulent cases.

Accuracy was notably high in models like the Multimodal Multiobjective Evolutionary Algorithm, Weight-Tuning Hyperparameters, and Heterogeneous Feature Augmentation for Ponzi Scheme Detection. The LGM-GNN and Graph Analysis models also excelled in accuracy, suggesting their robustness in overall correct classifications.

In the recall metric, many models such as the Ensemble Architecture (CNN-BiLSTM-RF), Spatial-Temporal Fraud Detection Model, and Weight-Tuning Hyperparameters showed high effectiveness in identifying all relevant instances of fraud. The Dilated Convolutional Transformer-based GAN (DCT-GAN) and Adaboost Algorithm also performed well in this aspect.

Regarding delay, several models exhibited a high delay, such as the Multimodal Multiobjective Evolutionary Algorithm and the Spatial-Temporal Fraud Detection Model. In contrast, models like the Weight-Tuning Hyperparameters and Adaboost Algorithm had lower delays, indicating faster response times in fraud detection.

Though some models, such as Mixed Attribute Outlier Detection and the Multimodal Multiobjective Evolution Algorithm, kept complexity levels low, others, like the Ensembles Architecture (CNN-BiLSTM-RF) and the Fraud Detection Model, kept them very high. Models' scalability varied greatly; two that demonstrated exceptional scalability, well-suited to large-scale applications, were the Multimodal Multiobjective Evolution Algorithm and the Block Chain as well as Smart Contract-Based ML Approach.

When compared across many criteria, models such as Graph Analysis and Weight-Tuning Hyperparameters performed better, suggesting they might be more useful in a variety of fraud detection situations. However, models such as the Ensemble Architecture (CNN-BiLSTM-RF) and the Spatial-Temporal Fraud Detection Model may struggle with issues like poor accuracy and significant latency, respectively, even though they excel in other places.

The need of selecting models with care according to particular needs and limitations in identifying fraud applications is brought to light by this comparison study.

IV. 4. CONCLUSION & FUTURE SCOPES

This detailed evaluation of both machine learning as well as deep learning fraud detection techniques shows their strengths and weaknesses. The Multimodal Multiobjective Evolution Algorithm with Weight-Tuning Hyperparameters showed promise in fraud detection due to its precision and accuracy.

Ensemble Architecture (CNN-BiLSTM-RF) and Quantum ML with Fraud Identification offers increased detection accuracy or blockchain technology and smart contract applications. Lack of dataset variety, computational expenses, and scalability remain. These results show that context—data volume, processing capabilities, and fraud types—is crucial to fraud detection system selection.

Future Scope

- **Optimization of Models:** Evolutionary algorithms may circumvent such limits with better competition-driven processes or ensemble architecture preparation.
- **Scalability and Efficiency:** Models need to be adapted for larger datasets and more complex fraud scenarios, ensuring they remain efficient and scalable.
- **Diverse Application and Validation:** Many models, while promising, require validation across different datasets and real-world scenarios to confirm their effectiveness.
- **Integration of Emerging Technologies:** Exploring the incorporation of new skills like substantial computing and block chain can offer innovative approaches to fraud detection.
- **Handling Imbalanced and Limited Data:** Developing techniques to better handle imbalanced datasets and improve performance with limited data availability is crucial.
- **Enhanced Generalization Capabilities:** Models should be developed to generalize well across various types of fraud, ensuring robustness in diverse environments.
- **Automated and Adaptive Models:** Artificial intelligence may help fraud detection systems stay ahead of thieves by adapting to shifting fraud patterns and methods.

Innovation and adaptability are needed to identify fraud, and this study leads the way. To enhance complicated fraud prevention efficiency, efficacy, and flexibility.

REFERENCES

[1] S. Han, K. Zhu, M. Zhou and X. Cai, "Competition-Driven Multimodal Multiobjective Optimization and Its Application to Feature Selection for Credit Card Fraud Detection," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 12, pp. 7845-7857, Dec. 2022, doi: 10.1109/TSMC.2022.3171549.

[2] A. Batool and Y. -C. Byun, "An Ensemble Architecture Based on Deep Learning Model for Click Fraud Detection in Pay-Per-Click Advertisement Campaign," in IEEE Access, vol. 10, pp. 113410-113426, 2022, doi: 10.1109/ACCESS.2022.3211528.

[3] N. Nguyen et al., "A Proposed Model for Card Fraud Detection Based on CatBoost and Deep Neural Network," in IEEE Access, vol. 10, pp. 96852-96861, 2022, doi: 10.1109/ACCESS.2022.3205416.

[4] G. Chu et al., "Exploiting Spatial-Temporal Behavior Patterns for Fraud Detection in Telecom Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 6, pp. 4564-4577, Nov.-Dec. 2023, doi: 10.1109/TDSC.2022.3228797.

[5] S. K. Hashemi, S. L. Mirtaheri and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," in IEEE Access, vol. 11, pp. 3034-3043, 2023, doi: 10.1109/ACCESS.2022.3232287.

[6] T. H. Pranto, K. T. A. M. Hasib, T. Rahman, A. B. Haque, A. K. M. N. Islam and R. M. Rahman, "Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach," in IEEE Access, vol. 10, pp. 87115-87134, 2022, doi: 10.1109/ACCESS.2022.3198956.

[7] D. Benalcazar, J. E. Tapia, S. Gonzalez and C. Busch, "Synthetic ID Card Image Generation for Improving Presentation Attack Detection," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1814-1824, 2023, doi: 10.1109/TIFS.2023.3255585.

[8] Z. Yuan, H. Chen, T. Li, X. Zhang and B. Sang, "Multigranulation Relative Entropy-Based Mixed Attribute Outlier Detection in Neighborhood Systems," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 8, pp. 5175-5187, Aug. 2022, doi: 10.1109/TSMC.2021.3119119.

[9] Y. Li, X. Peng, J. Zhang, Z. Li and M. Wen, "DCT-GAN: Dilated Convolutional Transformer-Based GAN for Time Series Anomaly Detection," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 3632-3644, 1 April 2023, doi: 10.1109/TKDE.2021.3130234.

[10] R. Mokkapati and D. V. Lakshmi, "Imperative Node Evaluator With Self Replication Mode for Network Intrusion Detection," in IEEE Access, vol. 11, pp. 46615-46626, 2023, doi: 10.1109/ACCESS.2023.3273904.

[11] C. Iscan, O. Kumas, F. P. Akbulut and A. Akbulut, "Wallet-Based Transaction Fraud Prevention Through LightGBM With the Focus on Minimizing False Alarms," in IEEE Access, vol. 11, pp. 131465-131474, 2023, doi: 10.1109/ACCESS.2023.3321666.

[12] G. Miao, G. Wu, Z. Zhang, Y. Tong and B. Lu, "SPN: A Method of Few-Shot Traffic Classification With Out-of-Distribution Detection Based on Siamese Prototypical Network," in IEEE Access, vol. 11, pp. 114403-114414, 2023, doi: 10.1109/ACCESS.2023.3325065.

[13] I. Matloob, S. A. Khan, R. Rukaiya, M. A. K. Khattak and A. Munir, "A Sequence Mining-Based Novel Architecture for Detecting Fraudulent Transactions in Healthcare Systems," in IEEE Access, vol. 10, pp. 48447-48463, 2022, doi: 10.1109/ACCESS.2022.3170888.

[14] C. Jin, J. Jin, J. Zhou, J. Wu and Q. Xuan, "Heterogeneous Feature Augmentation for Ponzi Detection in Ethereum," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 69, no. 9, pp. 3919-3923, Sept. 2022, doi: 10.1109/TCSII.2022.3177898.

[15] P. Fernando, K. Dadallage, T. Gamage, C. Seneviratne, A. Madanayake and M. Liyanage, "Proof of Sense: A Novel Consensus Mechanism for Spectrum Misuse Detection," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9206-9216, Dec. 2022, doi: 10.1109/TII.2022.3169978.

[16] Y. Gao, B. Shi, B. Dong, Y. Wang, L. Mi and Q. Zheng, "Tax Evasion Detection With FBNE-PU Algorithm Based on PnCGCN and PU Learning," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 1, pp. 931-944, 1 Jan. 2023, doi: 10.1109/TKDE.2021.3090075.

[17] J. Zhou et al., "FraudAuditor: A Visual Analytics Approach for Collusive Fraud in Health Insurance," in IEEE Transactions on Visualization and Computer Graphics, vol. 29, no. 6, pp. 2849-2861, 1 June 2023, doi: 10.1109/TVCG.2023.3261910.

[18] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," in IEEE Access, vol. 10, pp. 39700-39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[19] Shivlal Mewada, Anil Saroliya, N. Chandramouli, T. Rajasanthosh Kumar, M. Lakshmi, S. Suma Christal Mary, Mani Jayakumar, "Smart Diagnostic Expert System for Defect in Forging Process by Using Machine Learning Process", Journal of Nanomaterials, vol. 2022, Article ID 2567194, 8 pages, 2022. https://doi.org/10.1155/2022/2567194

[20] P. Li, H. Yu, X. Luo and J. Wu, "LGM-GNN: A Local and Global Aware Memory-Based Graph Neural Network for Fraud Detection," in IEEE Transactions on Big Data, vol. 9, no. 4, pp. 1116-1127, 1 Aug. 2023, doi: 10.1109/TBDATA SAMPLES.2023.3234529.

[21] F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem and T. Al-Hadhrami, "Ensemble Synthesized Minority Oversampling-Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection," in IEEE Access, vol. 11, pp. 89694-89710, 2023, doi: 10.1109/ACCESS.2023.3306621.

[22] D. Cheng, X. Wang, Y. Zhang and L. Zhang, "Graph Neural Network for Fraud Detection via Spatial-Temporal Attention," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 8, pp. 3800-3813, 1 Aug. 2022, doi: 10.1109/TKDE.2020.3025588.

[23] J. Chen, X. Hu, D. Yi, M. Alazab and J. Li, "A Variational AutoEncoder-Based Relational Model for Cost-Effective Automatic Medical Fraud Detection," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 4, pp. 3408-3420, 1 July-Aug. 2023, doi: 10.1109/TDSC.2022.3187973.

[24] A. Mniai, M. Tarik and K. Jebari, "A Novel Framework for Credit Card Fraud Detection," in IEEE Access, vol. 11, pp. 112776-112786, 2023, doi: 10.1109/ACCESS.2023.3323842.

[25] Y. -Y. Hsin, T. -S. Dai, Y. -W. Ti, M. -C. Huang, T. -H. Chiang and L. -C. Liu, "Feature Engineering and Resampling Strategies for Fund Transfer Fraud With Limited Transaction Data and a Time-Inhomogeneous Modi Operandi," in IEEE Access, vol. 10, pp. 86101-86116, 2022, doi: 10.1109/ACCESS.2022.3199425.

[26] M. Grossi et al., "Mixed Quantum–Classical Method for Fraud Detection With Quantum Feature Selection," in IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-12, 2022, Art no. 3102812, doi: 10.1109/TQE.2022.3213474.

[27] W. Ning, S. Chen, S. Lei and X. Liao, "AMWSPLAdaboost Credit Card Fraud Detection Method Based on Enhanced Base Classifier Diversity," in IEEE Access, vol. 11, pp. 66488-66496, 2023, doi: 10.1109/ACCESS.2023.3290957.

[28] Y. Yoo, J. Shin and S. Kyeong, "Medicare Fraud Detection Using Graph Analysis: A Comparative Study of Machine Learning and Graph Neural Networks," in IEEE Access, vol. 11, pp. 88278-88294, 2023, doi: 10.1109/ACCESS.2023.3305962.

[29] K. Kapadiya et al., "Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: an Analysis, Architecture, and Future Prospects," in IEEE Access, vol. 10, pp. 79606-79627, 2022, doi: 10.1109/ACCESS.2022.3194569.

[30] M. N. Ashtiani and B. Raahemi, "Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 72504-72525, 2022, doi: 10.1109/ACCESS.2021.3096799.

[31] A. Ravi, M. Msahli, H. Qiu, G. Memmi, A. Bifet and M. Qiu, "Wangiri Fraud: Pattern Analysis and Machine-Learning-Based Detection," in IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6794-6802, 15 April15, 2023, doi: 10.1109/JIOT.2022.3174143.

[32] C. Wang and H. Zhu, "Representing Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 301-315, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2991872.

[33] W. Xiuguo and D. Shengyong, "An Analysis on Financial Statement Fraud Detection for Chinese Listed Companies Using Deep Learning," in IEEE Access, vol. 10, pp. 22516-22532, 2022, doi: 10.1109/ACCESS.2022.3153478.

[34] F. Zhu, C. Zhang, Z. Zheng and S. A. Otaibi, "Click Fraud Detection of Online Advertising–LSH Based Tensor Recovery Mechanism," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 9747-9754, July 2022, doi: 10.1109/TITS.2021.3107373.

[35] N. Nayyer, N. Javaid, M. Akbar, A. Aldegheishem, N. Alrajeh and M. Jamil, "A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities," in IEEE Access, vol. 11, pp. 90916-90938, 2023, doi: 10.1109/ACCESS.2023.3308298.