[1]Dr. Raja Mohan

[2]Mythili Boopathi

[3]Piyush Ranjan

[4]Madhavi Najana

[5]Pranav Kumar Chaudhary

[6]Aakash Kishore Chotrani

Ai in Fraud Detection: Evaluating the Efficacy of Artificial Intelligence in Preventing Financial Misconduct

Journal of Electrical Systems

Abstract: - AI is anticipated to enhance competitive advantages for financial organisations by increasing efficiency through cost reduction and productivity improvement, as well as by enhancing the quality of services and goods provided to consumers. AI applications in finance have the potential to create or exacerbate financial and non-financial risks, which could result in consumer and investor protection concerns like biassed, unfair, or discriminatory results, along with challenges related to data management and usage. The AI model's lack of transparency may lead to pro-cyclicality and systemic risk in markets, posing issues for financial supervision and internal governance frameworks that may not be in line with a technology-neutral regulatory approach. The primary objective of this research is to explore the effectiveness of Artificial Intelligence in preventing financial misconduct. This study extensively examines sophisticated methods for combating financial fraud, specifically evaluating the efficacy of Machine Learning and Artificial Intelligence. When examining the assessment metrics, this study utilized various metrics like accuracy, precision, recall, F1 score, and the ROC-AUC. The study found that Deep Learning techniques such as "Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks /Long Short-Term Memory, and Auto encoders" achieved high precision and AUC-ROC scores in detecting financial fraud. Voting classifiers, stacking, random forests, and gradient boosting machines demonstrated durability and precision in the face of adversarial attacks, showcasing the strength of unity.

Keywords: Artificial Intelligence; Fraud Detection; Financial Misconduct; Machine Learning; Attacks.

I. INTRODUCTION

Artificial Intelligence (AI) systems are machine-based systems that possess different levels of independence and can make predictions, suggestions, or judgments depending on specific human-defined goals [1]. AI techniques are increasingly leveraging large totals of unconventional data sources and data analytics referred to as 'big data'. Information is used to improve machine learning models, making them more accurate and efficient without the need for manual coding [2,3]. The use of AI in finance is anticipated to boost competitive advantages for financial firms by enhancing efficiency and productivity, leading to increased profitability.

[1] Research Scholar, Mangalayatan University, Uttar Pradesh, India

Email Id: grmohan68@gmail.com

[2]Associate Professor, Vellore Institute of Technology, Vellore, Tamil Nadu, India

Email Id: nmythili@vit.ac.in

[3]Assistant Vice President - Software Development Engineer, New Jersey, USA

Email Id: piyush.ranjan@outlook.com

[4]Software Engineering Manager, Cincinnati, Ohio, USA

Email Id: nmn092021@gmail.com

[5]Senior Software Development Engineer, Seattle, USA

Email Id: chaudhary.pranav@gmail.com

[6]PhD in IT, University of the Cumberlands, Williamsburg, Kentucky (KY)

Email Id: achotrani60715@ucumberlands.edu

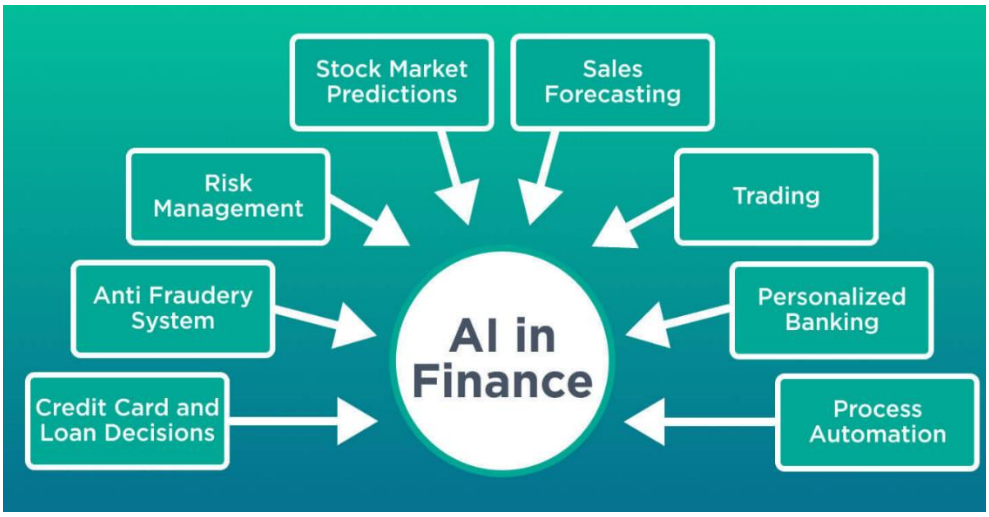

Figure 1: Role of AI in Finance[2]

This involves enhanced decision-making procedures, automated implementation, enhanced risk management, adherence to regulations, and process streamlining [4]. Moreover, AI has the potential to enhance the quality of financial services and products provided to customers through the introduction of new product options and personalised offerings. This competitive edge can benefit financial consumers by enhancing product quality, providing additional choices and customisation, and reducing costs [5].

AI applications in finance may increase financial and non-financial risks, raising worries about consumer and investor safety [6]. The utilization of AI increases risks that could impact a financial institution's stability due to the lack of clarity or interpretability of AI model operations, thereby leading to pro-cyclicality and systemic risk in the markets. The complexity of comprehending how the model produces outcomes could lead to potential conflicts with current financial oversight and internal management systems, and could also question the technology-agnostic approach to policy development [7,8]. AI has specific consumer protection risks, including biased, unfair, or discriminating outcomes for consumers, as well as concerns related to data management and utilization. Many AI-related financial concerns are not unique to AI, but the complexity of approaches, the dynamic flexibility of AI-based models, and the high autonomy of sophisticated AI applications may accentuate these vulnerabilities [9,10].

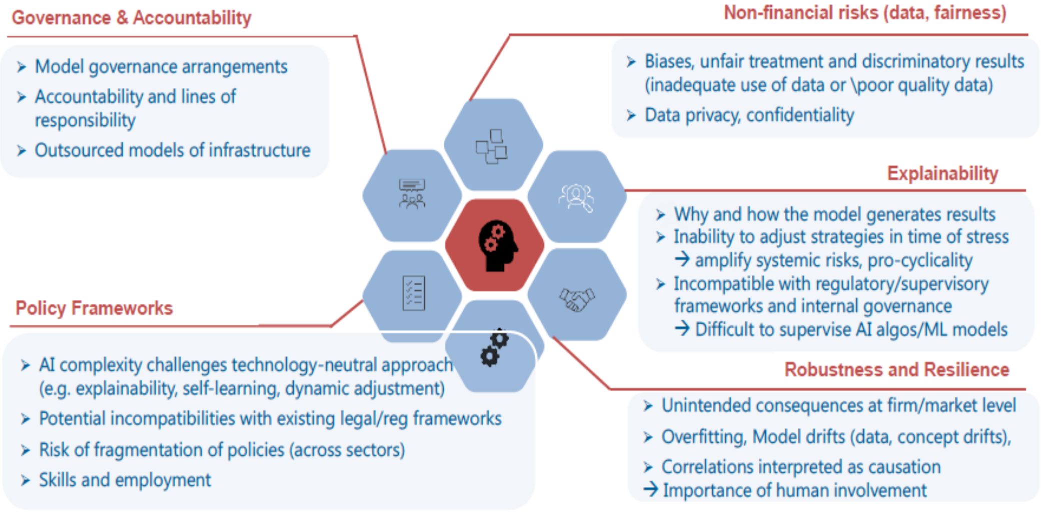
Governance & Accountability
➤ Model governance arrangements
➤ Accountability and lines of responsibility
➤ Outsourced models of infrastructure
Non-financial risks (data, fairness)
➤ Biases, unfair treatment and discriminatory results (inadequate use of data or \poor quality data)
➤ Data privacy, confidentiality
Explainability
➤ Why and how the model generates results
➤ Inability to adjust strategies in time of stress
→ amplify systemic risks, pro-cyclicality
➤ Incompatible with regulatory/supervisory frameworks and internal governance
→ Difficult to supervise AI algos/ML models
Policy Frameworks
➤ AI complexity challenges technology-neutral approach (e.g. explainability, self-learning, dynamic adjustment)
➤ Potential incompatibilities with existing legal/reg frameworks
➤ Risk of fragmentation of policies (across sectors)
➤ Skills and employment
Robustness and Resilience
➤ Unintended consequences at firm/market level
➤ Overfitting, Model drifts (data, concept drifts),
➤ Correlations interpreted as causation
→ Importance of human involvement

Figure 2: Finance AI deployment issues and hazards[3]

[2] https://jelvix.com/blog/ai-in-finance

[3] https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf

Explanations of previous literatures that are relevant to this study are provided in the following section.

II. LITERATURE SURVEY

The section that follows provides an overview of the previous research that has been conducted on the topic of the effectiveness of artificial intelligence in preventing financial misconduct.

Table 1: Related Works

AUTHORS AND YEAR	METHODOLOGY	FINDINGS
BuckleY et al., (2021) [11]	This article provides a framework for understanding and addressing finance's growing use of AI.	This paper suggests that the most efficient regulatory strategies for AI in finance include personal accountability systems that remove the black box argument as a defence against legal responsibility for AI actions and decisions.
Hilal et al., (2022) [12]	This survey examined and reviewed the most common and effective anomaly detection methods used to detect financial fraud, focusing on semi-supervised and unsupervised learning advances.	This study emphasized the importance of detecting fraud and its negative impact on the financial industry. It also addresses the challenges of using anomaly detection techniques to address this rising issue.
Rangineni & Marupaka (2023) [13]	This paper suggested data engineering methods to enhance analytical model performance while maintaining interpretability. The data engineering method involves multiple phases, each focusing on a specific area of feature and instance engineering.	Despite expanding the data set to include more features, the number of fraudulent transactions remains higher than legal ones. Using over-sampling algorithms, this study balanced the training set with 90% valid instances and 10% fraud cases.
Ahmadi (2023) [14]	Qualitative research methodology employed in this study.	According to this study, “financial fraud detectors use neural networks, decision trees, algorithms, natural language processing, and machine learning to create solid security mechanisms that thwart fraud efforts. Stripe and Mastercard have seen OpenAI's fraud detection gains and want to expand their AI operations.
Khalid et al., (2024) [15]	This study introduced a new ensemble model using SVM, KNN, RF, Bagging, and Boosting classifiers. This ensembled model uses under-sampling and SMOTE on machine learning methods to address the dataset imbalance problem in most credit card datasets.	Ensemble approaches are effective in fighting fraud, as shown in this research. As credit card fraud strategies change, more resilient and adaptable fraud detection systems will be needed. The findings presented set the framework for this.

Research Gap

Previous studies suggested that financial fraud has consequences beyond immediate financial losses, impacting consumer trust, reputation, and potentially leading to regulatory fines. Financial systems' integrity is crucial for maintaining economic stability, like to Atlas holding up the world. Every breach, like a storm in the financial world, has ripples that affect individuals, businesses, and the overall economy. Fraud detection is not just a reactive response to illicit activities; it is a proactive measure that strengthens the financial infrastructure. Swift identification and removal of fraudulent activities are crucial for safeguarding the integrity of transactions, ensuring a fair and secure financial environment, and protecting the interests of numerous individuals. The current situation requires sophisticated, flexible, and data-driven methods capable of unravelling complex patterns inside large datasets, a task that traditional methods struggle to achieve. This inquiry explores how Machine Learning (ML) and AI might enhance fraud detection to create strong defences against the increasing financial malfeasance.

III. METHODOLOGY

Financial fraud detection uses various AI and ML techniques to detect patterns, abnormalities, and probable fraudulent activity. The choice of approaches relies on the characteristics of the data, the specific type of fraud under consideration, and the preferred trade-off between accuracy and computing speed. The following are primary AI and ML techniques used in cutting-edge research: Supervised Learning Algorithms, Unsupervised Learning Methods, Deep Learning Approaches, and Ensemble Methods.

Studying the effectiveness of supervised learning algorithms in the ever-changing field of financial fraud detection is a crucial focus in modern research. This part thoroughly examines the many metrics used to measure the effectiveness of these algorithms, showcasing detailed results tables that reveal their success. The performance indicators for algorithms include Accuracy, Precision, Recall, F1 Score, and Area under the Receiver Operating Characteristics curve (AUC-ROC), each providing a detailed insight of algorithmic proficiency.

IV. RESULTS AND DISCUSSIONS

In supervised learning, Logistic Regression achieves a peak accuracy of 92% and precision of 89%, showcasing its skill in distinguishing between normal and harmful data with statistical expertise. However, despite this impressive accomplishment, there is a delicate balance of compromises to consider when the recall rate reaches 85%, perhaps allowing cases of real fraud to go unnoticed. Examining Decision Trees, a tool that helps balance different measurements, that observe impressive statistics: 94% accuracy and 91% precision. These data demonstrate its ability to distinguish between fake and legitimate cases. An AUC-ROC score of 0.96 indicates exceptional discrimination ability in distinguishing between different classes. Explore Support Vector Machines (SVM), known for its consistent performance with an accuracy of 93% and precision of 90%, making them reliable in fraud detection. An 87% recall suggests a moderate net, where some instances of deceit may still escape detection. The Gradient Boosting Machine (GBM) achieves a 95% accuracy and 93% precision, surpassing other algorithms. It carefully balances the task of reducing false positives while remaining watchful. GBM stands out with a recall rate of 91% in fraud detection, striking a harmonious balance between precision and recall.

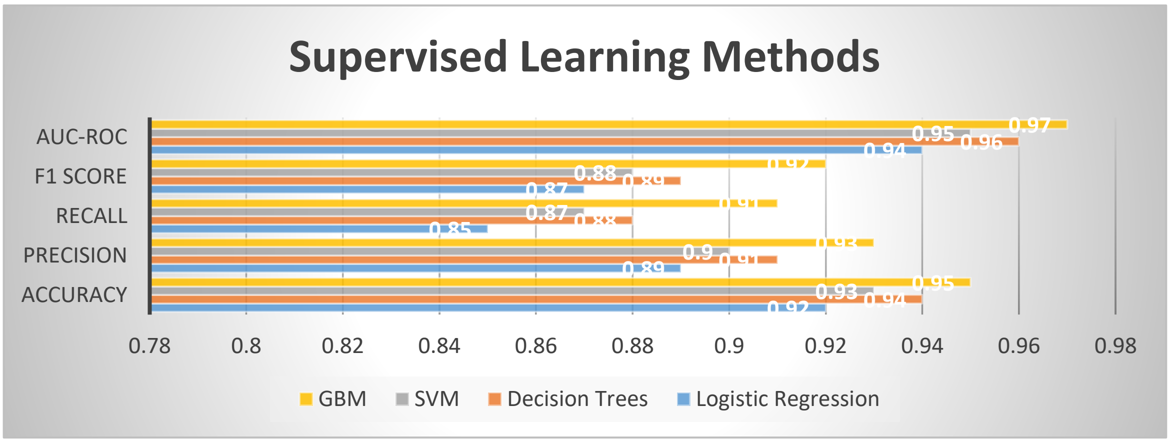

Figure 3: Results of Supervised Learning Methods

K-Means Clustering in Unsupervised Learning has a modest accuracy of 85%, highlighting its capability to create clusters and classify data points. The silhouette score of 0.60 indicates a satisfactory distinction across clusters, demonstrating the model's ability to group comparable data points effectively. Isolation Forests have strong discrimination capability with an AUC-ROC score of 0.92. This indicates a strong capacity to identify abnormalities in the dataset. The lack of precision and silhouette score hinders a thorough assessment of its overall performance and cluster quality. DBSCAN attains an AUC-ROC score of 0.87, demonstrating effective differentiation between normal and abnormal occurrences. Similar to Isolation Forests, the lack of accuracy and silhouette score hinders a comprehensive evaluation of its performance. Auto encoders exhibit high discrimination capability with an AUC-ROC score of 0.94, indicating their effectiveness in capturing intricate patterns associated with fraud. Evaluating the overall performance and cluster quality fully requires considering the accuracy and silhouette score.

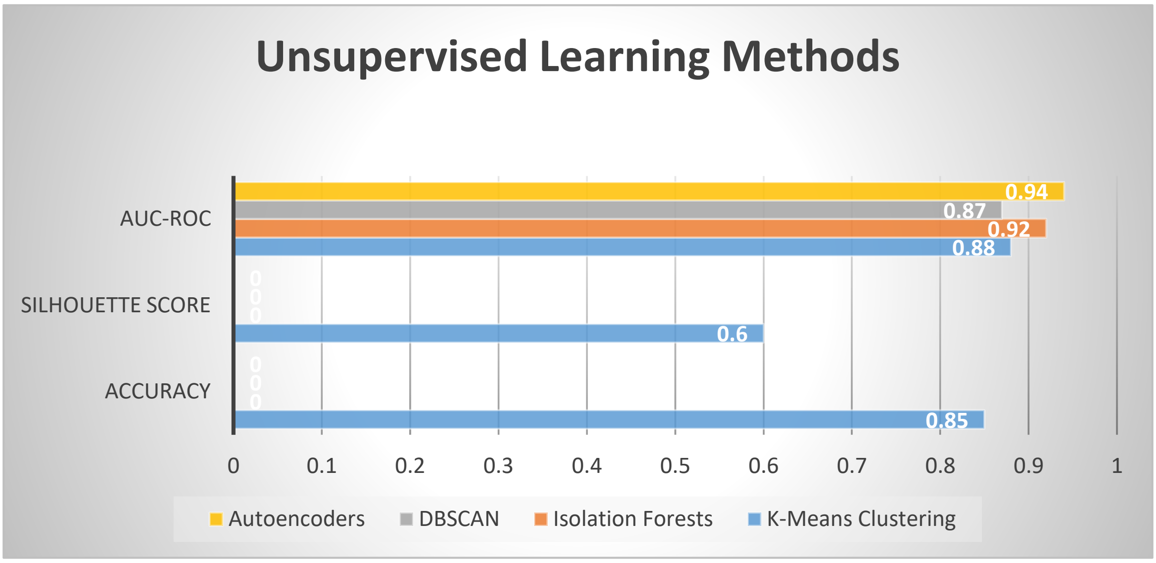

Figure 4: Results of Unsupervised Learning Methods

Neural Networks demonstrate strong performance in Deep Learning approaches, achieving an amazing 94% accuracy in categorizing transactions. Neural Networks demonstrate a balanced combination of precision (91%) and recall (88%), showcasing its effectiveness in reducing false positives and accurately identifying cases of fraud. Convolutional Neural Networks (CNNs) demonstrate a high AUC-ROC score of 0.97, showcasing their exceptional ability to accurately differentiate between normal and fraudulent transactions. CNNs demonstrate exceptional effectiveness in fraud detection with a 95% accuracy rate and a well-balanced precision-recall trade-off, effectively reducing false positives and negatives. Recurrent Neural Networks (RNNs) and Long Short-Term Memory Networks (LSTMs) consistently achieve high performance with an accuracy of 93%, precision rate of 89%, and recall rate of 87%. While slightly behind in precision and recall compared to certain competitors, their overall performance indicates versatility in various fraud detection situations. Auto encoders have achieved the highest AUC-ROC score of 0.98, demonstrating their excellent ability to identify patterns related to fraudulent transactions. With a remarkable 96% accuracy rate and strong precision-recall metrics, auto encoders are a reliable option for complex fraud detection applications. The AUC-ROC is a key metric that highlights the effectiveness of Auto encoders and CNNs in distinguishing between normal and fraudulent anomalies, since they achieve the highest scores.

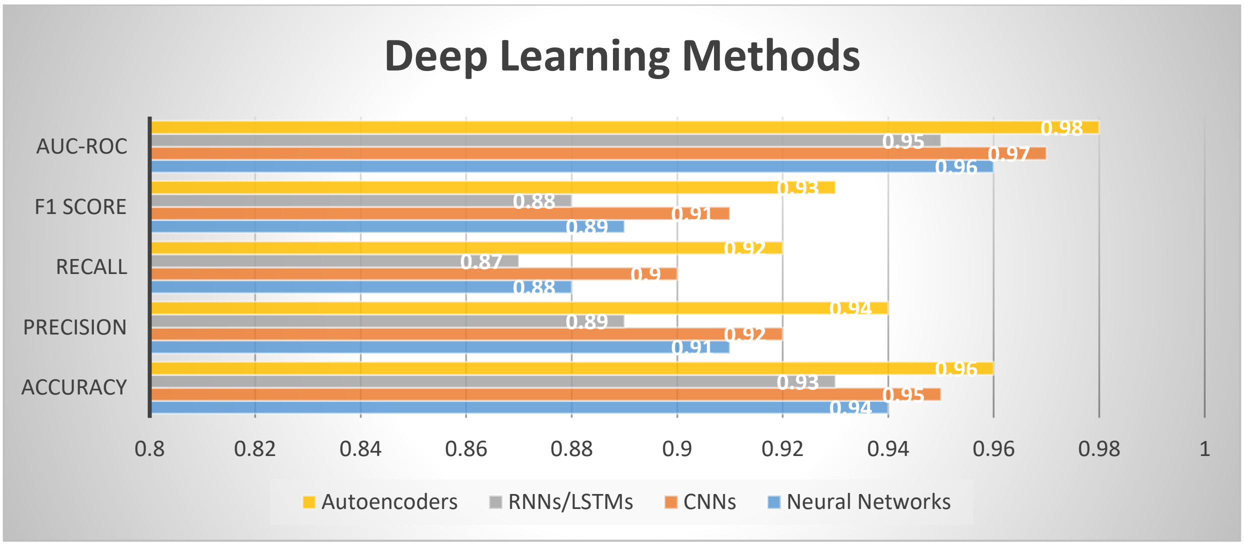

Figure 5: Results of Deep Learning Methods

Ensemble Methods, namely Voting Classifiers, demonstrate a high accuracy of 95% in effectively classifying transactions. These classifiers effectively balance precision at 92% and recall at 89%, skilfully reducing both erroneous positives and false negatives. Voting Classifiers are a versatile solution for various fraud detection scenarios, excelling in the complexities of classification tasks. Introducing stacking, a demonstration of strong performance, with an impressive 96% accuracy that highlights its ability to precisely outline transactions. The impressive combination of 94% precision and 92% recall demonstrates the effectiveness of stacking in managing the balance between reducing false positives and false negatives. Stacking stands out as a strong and reliable performer in the quest for precise categorization. Random Forests demonstrate a strong 94% accuracy, showcasing their consistent reliability in transaction classification. Random Forests demonstrate adaptability in fraud detection by maintaining a balanced equilibrium with 91% precision and 88% recall. Witness the impressive performance of GBM, which demonstrates exceptional accuracy of 97% and an outstanding AUC-ROC score of 0.98, showcasing its unmatched overall capability. The masterpiece maintains a high level of accuracy with 95% precision and 93% recall, while the Gradient Boosting Machine (GBM) expertly balances to reduce errors. GBM is the top solution for difficult fraud detection tasks due to its unwavering performance in handling intricate nuances.

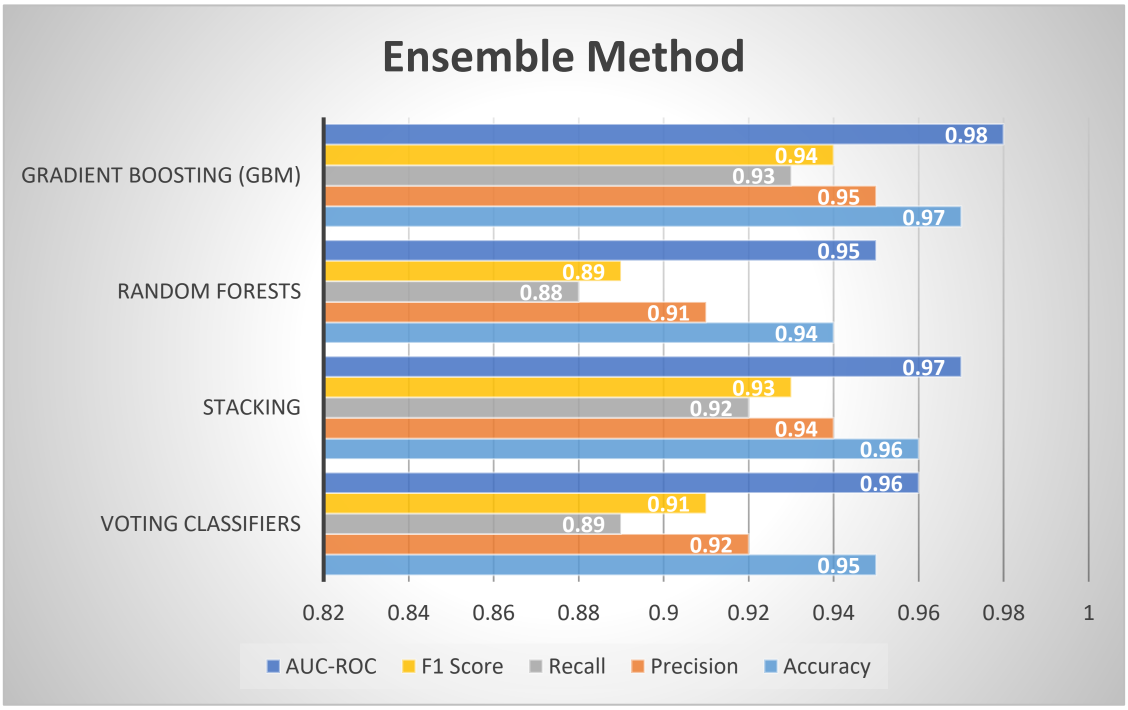

Figure 6: Results of Ensemble Methods

V. CONCLUSION

This study revealed significant findings that demonstrated the remarkable effectiveness of AI and machine learning in enhancing bank fraud detection systems. Utilizing deep learning techniques such as Neural Networks, CNNs, RNNs/ LSTM, and auto encoders. The processes created a precise symphony of AUC-ROC scores, illuminating the depths of financial fraud. Voting classifiers, stacking, random forests, and GBM demonstrated durability and precision in the face of adversarial attacks.

REFERENCES

[1] Mehbodniya, A., Alam, I., Pande, S., Neware, R., Rane, K. P., Shabaz, M., & Madhavan, M. V. (2021). Financial fraud detection in healthcare using machine learning and deep learning techniques. *Security and Communication Networks*, *2021*, 1-8.

[2] Kamuangu, P. (2024). A Review on Financial Fraud Detection using AI and Machine Learning. *Journal of Economics, Finance and Accounting Studies*, *6*(1), 67-77.

[3] Omar, S. J., Fred, K., & Swaib, K. K. (2018, May). A state-of-the-art review of machine learning techniques for fraud detection research. In *Proceedings of the 2018 International Conference on Software Engineering in Africa* (pp. 11-19).

[4] Raghavan, P., & El Gayar, N. (2019, December). Fraud detection using machine learning and deep learning. In *2019 international conference on computational intelligence and knowledge economy (ICCIKE)* (pp. 334-339). IEEE.

[5] Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, *76*, 130-157.

[6] Donning, H. A. N. N. A., Eriksson, M. A. T. H. I. A. S., Martikainen, M. I. N. N. A., & Lehner, O. M. (2019). Prevention and detection for risk and fraud in the digital age–the current situation. *ACRN Oxford Journal of Finance and Risk Perspectives*, *8*, 86-97.

[7] Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University-Computer and Information Sciences*, *35*(1), 145-174.

[8] Ashtiani, M. N., & Raahemi, B. (2021). Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review. *IEEE Access*, *10*, 72504-72525.

[9] Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). Credit card fraud detection using machine learning: a study. *arXiv preprint arXiv:2108.10005*.

[10] Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change*, *17*(2), 164-196.

[11] Buckley, R. P., Zetzsche, D. A., Arner, D. W., & Tang, B. W. (2021). Regulating artificial intelligence in finance: Putting the human in the loop. *Sydney Law Review, The*, *43*(1), 43-81.

[12] Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications*, *193*, 116429.

[13] Rangineni, S., & Marupaka, D. (2023). Analysis Of Data Engineering For Fraud Detection Using Machine Learning And Artificial Intelligence Technologies. *International Research Journal of Modernization in Engineering Technology and Science*," *5*(7), 2137-2146.\

[14] Ahmadi, S. (2023). Open AI and its Impact on Fraud Detection in Financial Industry. *Sina, A.(2023). Open AI and its Impact on Fraud Detection in Financial Industry. Journal of Knowledge Learning and Science Technology ISSN*, 2959-6386.

[15] Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: an ensemble machine learning approach. *Big Data and Cognitive Computing*, *8*(1), 6.