IRJEMS International Research Journal of Economics and Management Studies
Published by Eternal Scientific Publications
ISSN: 2583 – 5238 / Volume 3 Issue 12 December 2024 / Pg. No: 109-114
Paper Id: IRJEMS-V3I12P113, Doi: 10.56472/25835238/IRJEMS-V3I12P113

Original Article

Harnessing AI and Machine Learning for Enhanced Fraud Detection and Risk Management in Financial Services

[1]**Rakesh Kopperapu**
[1]*Cognizant Technology Solutions U.S. Corporation*.

Received Date: 15 November 2024 Revised Date: 25 November 2024 Accepted Date: 30 November 2024 Published Date: 11 December 2024

Abstract: *The paper can go on to review the application of AI and ML to fraud detection and, in a wider context, to financial service risk management. AI-based anomaly detection and predictive modeling will, for enhanced risk assessment, be introduced into the GNN and XAI frameworks. Performance is investigated regarding each model through the precision score, the recall, and F1, which can take either supervising, unsupervised learning, or reinforcement. It addresses the challenges of data scalability, algorithmic bias, and regulatory compliance to underline hybrid model adoption gaps and real-world scalability. The following research can apply the thematic analysis of secondary data in order to propose effective AI and ML frameworks for fraud prevention and decision-making.*

Keywords: *Artificial Intelligence (AI), Machine Learning (ML), Fraud Detection, Risk Management, Anomaly Detection, Predictive Modeling, Explainable AI (XAI), Graph Neural Networks (GNNs).*

I. INTRODUCTION

Fraud detection and risk management in financial services maintain transactional integrity and operational resilience among the most critical components. Traditional methods fall short when it comes to the challenging patterns of fraud and threats that emerge. AI and ML algorithms, such as those based on anomaly detection, predictive modeling, and neural networks, transform these domains into a real-time possibility for monitoring and adapting [1]. The analysis uses a combination of secondary data analysis backed by thematic discussion to support its discussion on how AI and ML are going about doing work on automating fraud prevention and improving risk assessment [2]. This research underlines growth in use and dependence upon advanced analytics, big data, and algorithmic precision as ways of stemming financial risks and preserving trust in institutions.

II. AIMS AND OBJECTIVES

A) Aim

The main aim of this research is to focus on the way AI and ML integrations have helped in fraud detection and risk management to algorithmic precision, supported by big data analytics.

B) Objectives

The objectives of this research are:

- To employ AI-based anomaly detection and predictive modeling in identifying complex fraud patterns in financial transactions.
- To evaluate the performance of supervised, unsupervised, and reinforcement learning models with respect to fraud detection.
- To identify implementation challenges, including data scalability, algorithmic bias, and regulatory compliance in financial services.
- To propose advanced AI/ML frameworks to improve real-time risk assessment and decision-making in financial institutions.

III. RESEARCH QUESTIONS

The main Research questions are:

- How do we employ AI-based anomaly detection and predictive modeling to identify complex fraud patterns in financial transactions?
- How do we evaluate the performance of supervised, unsupervised, and reinforcement learning models with respect to fraud detection?
- How do we identify implementation challenges, including data scalability, algorithmic bias, and regulatory compliance in financial services?

- How do we propose advanced AI and ML frameworks to improve real-time risk assessment and decision-making in financial institutions?

IV. LITERATURE REVIEW

The literature on applying AI and ML to fraud detection and risk management in financial services is very promising. It depicts the development, challenges, and new opportunities arising. This review currently focuses on only a few research works relevant to the identified thematic categories outlined in the main research questions, such as anomaly detection and predictive modeling, performance evaluation of ML models, challenges during implementation, and advanced framework design.

A) AI-Based Anomaly Detection and Predictive Modeling in Financial Transactions

The outlier detection in transactional data for fraud prevention, using techniques such as clustering, isolation forests, and autoencoders, forms the bedrock. Several works underpin the efficiency of unsupervised models, including Principal Component Analysis and K-means clustering, in finding abnormal patterns when there are no labeled datasets [3]. Deep autoencoders can be used in the real-time detection of fraudulent credit card transactions with high detection rates while at the same time realizing very low false positives. Predictive modeling supplements anomaly detection through supervised algorithms, namely, decision trees, logistic regression, and ensemble algorithms such as Random Forest and Gradient Boosting Machines [4]. It has been pointed out that the ensemble models significantly improve upon single models by bringing up accuracy and robustness to handle imbalanced datasets, which is quite typical for fraud detection tasks [5]. Its most significant dependence is on supervised learning, which greatly inhibits scalability when fraud tactics keep changing.

B) Performance Evaluation of Supervised, Unsupervised, and Reinforcement Learning Models

Precision, recall, F1 score, and AUC are general metrics on which different machine learning models are tested. The supervised learning techniques-SVM and Neural Networks-manage to stay ahead owing to the precision they give in most classifications. Algorithms based on machine learning can help banking workers gather important data on the lifetime value of clients [6]. Unsupervised learning allows discovering unknown fraud patterns by clustering and dimensionality reduction techniques, although usually at the cost of interpretability. For instance, DBSCAN, or Density-Based Spatial Clustering, has been used successfully but does not cope well with noisy data [7]. Though reinforcement learning might also show promise in dynamic environments while agents learn through trial and error, even fraud detection is not well explored. The application of reinforcement learning to risk management by dynamic updating of credit risk scores for financial institutions [8]. Another limitation toward the training of reinforcement learning models is related to a lack of real-world datasets, which holds back the adoption of the same.

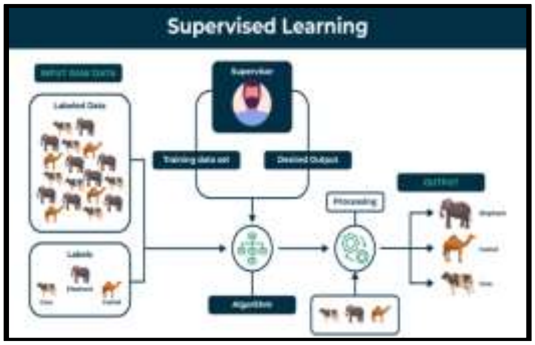

Fig. 1 Supervised and Unsupervised Learning

C) Implementation Challenges: Data Scalability, Algorithmic Bias, and Regulatory Compliance

Other challenges involve the problem of data scalability with respect to the use and implementation of AI and ML in financial institutions. The exponential rise of transactional data brings an urgent requirement to develop model development techniques that can handle a greater volume of data in real-time [9]. Large-scale model deployment can be enabled by frameworks like Hadoop and Spark, although these can raise latency concerns in applications that involve time-sensitive decisions, such as fraud detection. The other crucial issue is algorithmic bias, such as biased training, which can lead to prejudicial outcomes. Machine learning models, which have been built on biased datasets, can ultimately flag minority groups as a high-risk population-a fact with both ethical and legal implications [10]. Methods to mitigate these issues are adversarial debiasing and re-sampling. However, their effectiveness remains limited. Besides this, compliance with regulations also makes the task of deploying AI in financial services all the more difficult. Most of the models are expected to be explainable and auditable. Research has to be focused on interpretable AI frameworks without losing performance and, at the same time, satisfying the demands of regulatory requirements [11]. The GDPR demands that institutions be transparent in relation to automated decision-making processes, which again directly clashes with the incomprehensibility of advanced ML models, such as deep neural networks.

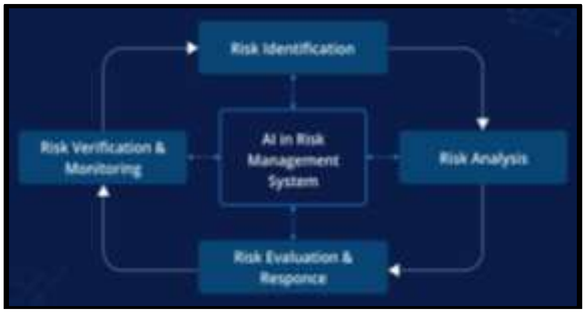
Risk Identification
Risk Verification & Monitoring
AI in Risk Management System
Risk Analysis
Risk Evaluation & Responce

Fig. 2 AI in risk management

D) Designing Advanced AI and ML Frameworks for Real-Time Risk Assessment

Advanced real-time risk assessment frameworks utilize AI techniques along with domain knowledge to develop improved decision-making capabilities. Most recently, Graph neural networks capture the relationships of entities participating in financial transactions. Graph-based models have taken significant importance in representing transaction networks [12]. Hence, they provide fraud detection with deeper context awareness. Other key developments include explainable AI, which has placed an emphasis on interpretability in machine learning models. Techniques such as SHAPE and LIME have provided insight into decisions taken by models that can address regulatory requirements to build stakeholders' trust [13]. The integration of XAI into deep learning to create well-balanced models that possess high performance and interpretability. Besides, federated learning is a distributed approach to training models on decentralized data, emerging as a solution to data privacy concerns [14]. Federated learning allows for privacy preservation while leveraging global patterns by training on-device and aggregating insights without sharing raw data. The potential of federated learning in cross-border fraud detection [15]. It also characterizes literature that there is an interest, which is increasingly growing, in the incorporation of advanced techniques along the lines of GNN, XAI, and federated learning for constructing robust and secured frameworks with the aim of real-time risk assessment.

E) Literature gap

There have been significant advancements in using AI and ML for risk management and fraud detection, but the literature also reveals several shortcomings. There is a serious lack of research on the way hybrid models that combine supervised, unsupervised, and reinforcement learning can be used in an integrated manner for further optimization of fraud detection across diverse scenarios. While anomaly detection and predictive modeling are independently explored, most of them remain underdeveloped for adaptive integration towards real-time applications. Furthermore, the way different advanced techniques such as XAI, GNNs, and federated learning can pay off in practical, scalable deployments has not been well studied [16]. In order to fill these gaps and satisfy the constantly changing requirements of the financial sector and regulatory norms, efforts are being made to develop strong, flexible frameworks that strike a balance between accuracy, transparency, and compliance.

V. METHODOLOGY

This qualitative study utilizes thematic analysis to explore the manner in which Artificial Intelligence and Machine Learning have been so far integrated into fraud detection and risk management within financial services. The methodologies include secondary data analyses that are drawn from a peer-reviewed journal, industry reports, and case studies to identify recurring patterns, themes, and insights that relate to the objectives of the study [17]. Thematic analysis enables the nuanced extraction of interpretations that afford a more insightful, detailed look at the way AI and ML technologies apply in dealing with the challenges of financial fraud and risk management. This collection focuses on material dealing authoritatively with AI anomaly detection, predictive modeling, performance evaluation of machine learning algorithms, challenges during the implementation of AI technology in banking, and new, state-of-the-art frameworks for risk assessment in real time [18]. This analysis initiates the familiarization of data and identifies some key areas where AI and ML have high potential, such as AI-based anomaly detection, evaluation of different supervised and unsupervised learning models, challenges of deployment, and proposals of advanced frameworks.

The first was anomaly detection and predictive modeling, with the great potential of ML algorithms such as clustering analysis, neural networks, and decision trees. In this respect, the methodology underlines how unsupervised models manage to disclose new fraud patterns owing to their adaptability and the way the choice fell to the approach of supervised learning to achieve predictive accuracy [19]. The contribution offered by the identified patterns allows a look at hybrid approaches concerning fraud detection dynamicity. The second theme assesses different versions of ML models concerning performance against secondary metadata measures, including precision, recall, F1 score, and model computational power. This eventually leads to the identification of existing lacunae in the comparative performance of standalone models while pointing out the key strengths of integrated models that use techniques such as ensemble and reinforcement learning [20]. The thematic focus captures insights into addressing the comparative strengths of such models with their several limitations, thus laying a potential groundwork for exploring more sophisticated AI-driven fraud detection frameworks.

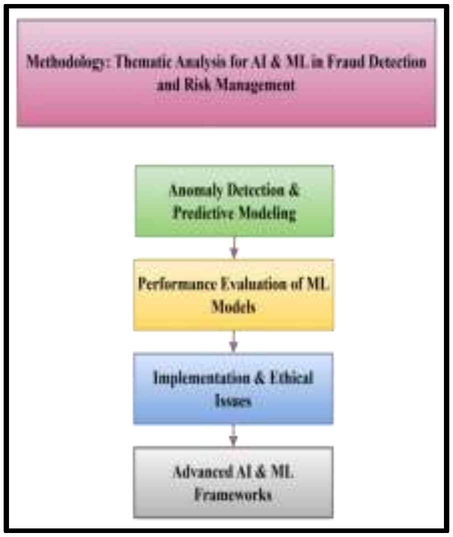
Methodology: Thematic Analysis for AI & ML in Fraud Detection and Risk Management
Anomaly Detection & Predictive Modeling
Performance Evaluation of ML Models
Implementation & Ethical Issues
Advanced AI & ML Frameworks

Fig. 3 Flowchart

Mostly regarding issues around scaling data, bias in algorithm creation, and conformance with regulations, while data can be found for each important point, the third most compelling theme relates to implementation. The thematic analysis brings out patterns related to ethical implications of deployment into financial services because of potential biases that emerge from the training dataset to transparency in models' decisions [21]. It also reviews secondary data on the regulatory framework of the GDPR and its effect on the design and deployment of AI systems. The findings are organized in themes that speak to scalability concerns and the desirability of interpretable AI models in view of compliance considerations. The last theme can be to propose advanced AI and ML frameworks by extracting insights from secondary data about emergent technologies such as federated learning, Explainable AI, and Graph Neural Networks [22]. It has been seen in this analysis that these techniques can improve fraud detection and risk assessment, thereby giving a nuanced interpretation of the practical and scalable application of such techniques.

VI. DATA ANALYSIS

Thematic analysis is done for qualitative data analysis to identify a certain key pattern and understanding from the secondary sources of data. This approach ensures a structured and detailed review with respect to the way artificial intelligence and machine learning alter fraud detection and risk management across Fin-service. The following analyses are organized around four keys: AI-based anomaly detection and predictive modeling, performance evaluation of machine learning models, challenges that come with the implementation, and advanced frameworks that can be laid down for real-time management of risk.

A) Theme 1: AI-Based Anomaly Detection and Predictive Modeling

This theme will enable the application of AI-driven techniques in anomaly detection and fraud prediction across financial transactions. The works will range from anomaly detection algorithms such as isolation forest, one-class support vector machines, and auto-encoders-important to identifying outliers whose behaviors are abnormal. A full review of secondary data reveals these methods to be very good in the detection of unknown or evolving fraud schemes, especially when applied to large datasets where traditional rule-based systems fail [23]. While predictive modeling employs a variety of machine learning techniques, including Logistic Regression, Random Forests, and Gradient Boosting Machines, all in a supervised learning fashion to classify any transaction as fraudulent or genuine, several case studies underline the fact that often the ensembles outperform the single models because of reduced bias and variance. In this direction, anomaly detection coupled with predictive modeling gives a hybrid system that will enable continuous learning and adaptation to new patterns of fraud [24]. Among them, one salient analysis is that predictive modeling relies upon labeled datasets, which may well not exist, while anomaly detection methods, though flexible, do not have the predictive precision of supervised algorithms. Each compensates for the weaknesses of the others and, brought together, offers a robust mechanism for fraud handling in real time.

B) Theme 2: Performance Evaluation of Machine Learning Models

Performant assessment by various ML models- Apart from multiple detection capabilities, this may be a very critical success-oriented area to analyze. Its study, among secondary ones, is made according to properties such as accuracy, precision, recall, F1 score, and Area under the Receiver Operating Characteristic Curve. Though supervised modeling like Neural Networks or SMV has had good performances in terms of precision, recall, and flag fraud statements, it also creates substantial challenges, such as computationally heavy and sensitive solutions developing on imbalanced datasets sometimes may end up flagging fraudulent transactions [25]. Unsupervised models include clustering and dimensionality reduction techniques that use labeled data a bit less and are much better at finding unknown fraud patterns. For example, PCA and DBSCAN have been useful in anomaly detection within high-dimensional financial data [26]. However, most of the models developed using unsupervised learning face a lot of problems with interpretability, making it difficult for financial institutions to justify decisions to stakeholders and regulators. The key point with reinforcement learning models is that they are dynamic. Hence, they can adapt to eventual changes within an environment and a strategy. Possible applications involve the field of credit risk management, where one can present the risk scores that change over actual changes in real data. Comparisons of state-of-the-art reinforcement learning against classical, unsupervised, and supervised fraud detection tasks are absolutely absent from the literature.

C) Theme 3: Implementation Challenges in AI and ML Deployment

There are several challenges for deploying AI and ML in fraud detection and risk management. Financial transactions are growing exponentially, which raises the issue of data scalability. Secondary data shows that using a distributed computing framework like Hadoop or Apache Spark allows scalability but at the cost of latency issues in real-time applications. Big data technologies remain to be integrated with ML pipelines, an area of further research and development. Another critical challenge pertains to algorithmic bias [27]. Several studies have proved that prejudice in the dataset used for training often turns out to be discriminatory performances against demographics. Several techniques were mooted as mitigants, such as re-sampling, adversarial debiasing, and fairness-aware algorithms. However, these are rather limited in large-scale uses in financial services due to model complexity and possible regulatory scrutiny. Then, there is also the layer of regulatory complexity, such as financial institutions needing to follow data privacy legislation and provide explainable AI solutions [28]. The GDPR, at least in Europe, calls for transparency regarding any automated decision-making. Again, though, some deep learning and complex models can be opaque. Therefore, their compliance can be difficult. One promising solution identified in developing this is through explainability in AI, using techniques such as SHAP and LIME.

D) Theme 4: Advanced Frameworks for Real-Time Risk Management

The last theme envelops the design and implementation of state-of-the-art AI and ML frameworks for real-time risk assessment. For example, newer techniques, such as GNNs, have more advanced capabilities since transactional data is modeled as graphs, capturing complex relationships and dependencies between entities. Research has shown that GNNs outperform traditional models in detecting fraud within multi-entity networks, such as money laundering schemes [29]. Another promising approach is federated learning, enabling model training in decentralized datasets locally while sharing aggregated insights. This can ensure data privacy while enabling institutions to collaborate on fraud detection models across borders. Case studies in cross-border fraud detection highlight the potential of federated learning to improve detection rates while maintaining compliance with privacy regulations. The explanatory AI frameworks in the risk management system architecture structure become an essential ingredient of better interpretability-in [30]. Secondary data highlight the approaches that include XAI and provide improved insight into model prediction that might bring value in decision-making among other useful drivers, alignment toward regulatory requirements. On the other hand, cloud computing and edge AI enable the deployment of fraud detection in real time with very minimal latency, especially in high-volume financial environments.

VII. FUTURE DIRECTIONS

Future studies can be conducted on integrating XAI into GNNs to enhance interpretability and accuracy in fraud detection. The focus is shifting toward developing scalable, federated learning frameworks that handle privacy concerns for cross-border financial transactions. The investigation of QML also looks promising, as it opens new ways of processing high-dimensional financial data [31]. Besides, designing adaptive algorithms for algorithmic bias mitigation and ensuring regulatory compliance becomes a critical focus area. In particular, edge AI with real-time deployment through the cloud accelerates fraud detection, improving risk management systems.

VIII. CONCLUSION

This research has pointed out how AI and ML will eventually change fraud detection and risk management in the financial industry. It realizes that hybrid methods using supervised, unsupervised, and reinforcement learning can be much better in detecting complex fraudulent patterns. Advanced frameworks such as Explainable AI, GNNs, and federated learning may overcome some of the abovementioned challenges, such as algorithmic bias, scalability, and regulatory compliance. It thus focused on developing real-time deployment technologies, including edge AI and cloud computing, to improve the accuracy of the decision-making process. Thus, this research work lays the foundation for further development related to financial AI systems.

IX. REFERENCES

[1] Sambrow, V.D.P. and Iqbal, K., 2022. Integrating Artificial Intelligence in Banking Fraud Prevention: A Focus on Deep Learning and Data Analytics. *Eigenpub Review of Science and Technology*, *6*(1), pp.17-33.

[2] Nimmagadda, V.S.P., 2022. AI-Powered Risk Management Systems in Banking: A Comprehensive Analysis of Implementation and Performance Metrics. *Australian Journal of Machine Learning Research & Applications*, *2*(1), pp.280-323.

[3] Bello, O.A., Folorunso, A., Ogundipe, A., Kazeem, O., Budale, A., Zainab, F. and Ejiofor, O.E., 2022. Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection. *International Journal of Network and Communication Research*, *7*(1), pp.90-113.

[4] Kalusivalingam, A.K., Sharma, A., Patel, N. and Singh, V., 2020. Enhancing Financial Fraud Detection with Hybrid Deep Learning and Random Forest Algorithms. *International Journal of AI and ML*, *1*(3).

[5] Sahu, M.K., 2020. Machine Learning Algorithms for Personalized Financial Services and Customer Engagement: Techniques, Models, and Real-World Case Studies. *Distributed Learning and Broad Applications in Scientific Research*, *6*, pp.272-313.

[6] Archana Todupunuri. " Develop Machine Learning Models to Predict Customer Lifetime Value for Banking Customers, Helping Banks Optimize Services" *International Journal of All Research Education and Scientific Methods* Vol. 12, No. 10, pp. 1254-1259, 2024.

[7] Gayam, S.R., 2020. AI-Driven Fraud Detection in E-Commerce: Advanced Techniques for Anomaly Detection, Transaction Monitoring, and Risk Mitigation. *Distributed Learning and Broad Applications in Scientific Research*, *6*, pp.124-151.

[8] Zanke, P. and Sontakke, D., 2021. Leveraging Machine Learning Algorithms for Risk Assessment in Auto Insurance. *Journal of Artificial Intelligence Research*, *1*(1), pp.21-39.

[9] Sasmal, S., 2021. Preventing Card Fraud and Scam Using Artificial Intelligence.

[10] Arlagadda, J.S. and Kamuni, N., 2022. Harnessing Machine Learning in Robo-Advisors: Enhancing Investment Strategies and Risk Management. *Journal of Innovative Technologies*, *5*(1).

[11] Shah, V., 2021. Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Espanola de DocumentacionCientifica*, *15*(4), pp.42-66.

[12] Lakhchini, W., Wahabi, R. and El Kabbouri, M., 2022. Artificial Intelligence & Machine Learning in Finance: A literature review. *International Journal of Accounting, Finance, Auditing, Management and Economics*.

[13] Putha, S., 2022. AI-Driven Wealth Management Solutions in Banking: Enhancing Portfolio Optimization and Client Advisory Services. *Australian Journal of Machine Learning Research & Applications*, *2*(2), pp.417-455.

[14] Haider, L. 2021. Artificial intelligence in ERP (Bachelor's thesis). Metropolia University of Applied Sciences, Finland.

[15] Xiaoli, W. and Nong, N.B., 2021. Evaluating Big Data Strategies for Risk Management in Financial Institutions. *Journal of Computational Social Dynamics*, *6*(3), pp.34-45.

[16] Gupta, S., 2021. Impact of artificial intelligence on financial decision making: A qualitative study. *Journal of Cardiovascular Disease Research,,12*(6), pp.2130-2137.

[17] Nimmagadda, V.S.P., 2021. Artificial Intelligence and Blockchain Integration for Enhanced Security in Insurance: Techniques, Models, and Real-World Applications. *African Journal of Artificial Intelligence and Sustainable Development*, *1*(2), pp.187-224.

[18] Pothumsetty, R., 2020. Implementation of Artificial Intelligence and Machine learning in Financial services. *International Research Journal of Engineering and Technology*, *7*(03).

[19] Pamulaparthyvenkata, S. and Avacharmal, R., 2021. Leveraging Machine Learning for Proactive Financial Risk Mitigation and Revenue Stream Optimization in the Transition Towards Value-Based Care Delivery Models. *African Journal of Artificial Intelligence and Sustainable Development*, *1*(2), pp.86-126.

[20] Shende, A., 2022. Leveraging Distributed Computing for Enhanced Risk Management and Compliance in Banking: A Pathway to Financial Success. *Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-213. DOI: doi. org/10.47363/JAICC/2022 (1)*, *199*, pp.2-6.

[21] Nassar, A. and Kamal, M., 2021. Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), pp.51-63.

[22] Zanke, P., 2022. Exploring the Role of AI and ML in Workers' Compensation Risk Management. *Human-Computer Interaction Perspectives*, *2*(1), pp.24-44.

[23] Archana Todupunuri. "The Future of Conversational AI in Banking: A Case Study on Virtual Assistants and Chatbots*: Exploring the Impact of AIPowered Virtual Assistants on Customer Service Efficiency and Satisfaction" *International Research Journal of Economics and Management Studies*, Vol. 3, No. 10, pp. 206-212, 2024.

[24] Machireddy, J.R., Rachakatla, S.K. and Ravichandran, P., 2021. Leveraging AI and Machine Learning for Data-Driven Business Strategy: A Comprehensive Framework for Analytics Integration. *African Journal of Artificial Intelligence and Sustainable Development*, *1*(2), pp.12-150.

[25] Fritz-Morgenthal, S., Hein, B. and Papenbrock, J., 2022. Financial risk management and explainable, trustworthy, responsible AI. *Frontiers in artificial intelligence*, *5*, p.779799.

[26] Perumalsamy, J., Althati, C. and Shanmugam, L., 2022. Advanced AI and Machine Learning Techniques for Predictive Analytics in Annuity Products: Enhancing Risk Assessment and Pricing Accuracy. *Journal of Artificial Intelligence Research*, *2*(2), pp.51-82.

[27] Cheng, Y. and Wang, L., 2022. Enhancing Bank Risk Management and Fraud Detection through Computer Vision Applications. *Innovative Computer Sciences Journal*, *8*(1).

[28] Boppana, V.R., 2022. Machine Learning and AI Learning: Understanding the Revolution. *Journal of Innovative Technologies*, *5*(1).

[29] Kalusivalingam, A.K., Sharma, A., Patel, N. and Singh, V., 2022. Enhancing B2B Fraud Detection Using Ensemble Learning and Anomaly Detection Algorithms. *International Journal of AI and ML*, *3*(9).

[30] Nicholls, J., Kuppa, A. and Le-Khac, N.A., 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access*, *9*, pp.163965-163986.

[31] Sahu, M.K., 2020. Machine Learning for Anti-Money Laundering (AML) in Banking: Advanced Techniques, Models, and Real-World Case Studies. *Journal of Science & Technology*, *1*(1), pp.384-424.