Enhancing Fraud Detection in Financial Transactions Using AI and Machine Learning

SYED AHAD MURTAZA ALVI[1], ASHISH KUMAR PANDEY[2]
[1]*College of Applied Computer Sciences, King Saud University, Riyadh, Saudi Arabia.*
[2]*Assistant Professor, Computer Science and Engineering, Dr. R.M.L. Avadh University, Ayodhya, India.*

Abstract- ***The rising number of digital transactions and the increasing complexity of fraudulent activities provide a significant challenge to financial institutions when it comes to detecting fraud in financial transactions. If fraud trends are constantly changing, traditional rule-based fraud detection systems won't be able to keep up. In order to improve the efficiency and accuracy of identifying fraudulent transactions, this study investigates AI-powered fraud detection that makes use of machine learning techniques. We test the efficacy of several ML models for anomaly detection and predicted fraud categorization using both supervised and unsupervised learning techniques. We also go over ways to enhance the performance of the model through feature engineering, data pretreatment, and real-time detection. In order to detect complicated fraud patterns with minimal false positives, the study emphasizes the benefits of deep learning and ensemble learning methods. Issues of ethics, practical difficulties, and potential avenues for further study with AI-powered fraud detection are also covered. According to the results, financial security and loss prevention are both greatly enhanced by AI-based fraud detection.***

Indexed Terms- ***Artificial Intelligence (AI), Financial Transactions, Anomaly Detection, Machine Learning, and Fraud Detection***

I. INTRODUCTION

There is a greater potential for fraudulent operations due to the proliferation of digital financial transactions. Conventional ways of detecting fraud are finding it increasingly difficult to keep up with increasingly intricate fraudulent schemes, which are driven by the exponential growth in both transaction volumes and the complexity of financial systems. Customers and banks alike are vulnerable to financial crimes such as identity theft, account takeovers, credit card fraud, and money laundering [1-3]. Machine learning (ML) and artificial intelligence (AI) have become potent fraud detection technologies to counter these dangers. With the help of sophisticated algorithms, fraud detection systems driven by AI can sift through mountains of transaction data, spot red flags, and stop financial losses before they happen [4-6].

Worldwide, fraud costs businesses and consumers billions of dollars every year [7-9], demonstrating the pervasiveness of this problem in the financial sector. Although rule-based approaches have their uses, traditional fraud detection systems aren't flexible. When applied on a wide scale, these rule-based methods are inefficient because they need constant human updating [10-12].

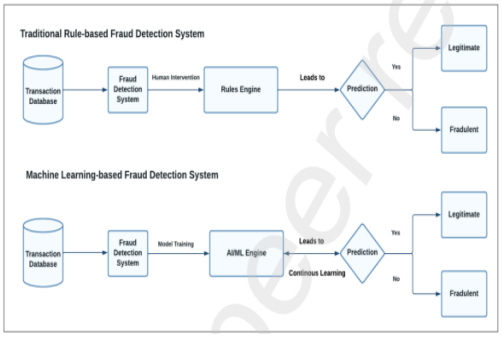

Figure 1. Conventional Model of AI based Financial transaction [13]

Dynamic, new fraud trends have been introduced with the advent of AI and ML, and they have completely transformed fraud detection. Frameworks for detecting fraud have commonly used machine learning methods and deep learning models [14-16]. Increased fraud detection rates and decreased operating expenses

are the results of these models' analysis of transaction habits, anomaly detection, and real-time risk evaluations.

The scalability and millisecond-level processing speed of AI-powered fraud detection systems have also led to their widespread adoption by financial institutions [17-19]. Artificial intelligence (AI) improves fraud prevention solutions, making the financial ecosystem more safe, by utilizing techniques including ensemble approaches, supervised and unsupervised learning, and anomaly detection.

- Models are trained using supervised learning with labelled transaction data, which includes both fraudulent and non-fraudulent examples. A few examples include neural networks, decision trees, and random forests.
- Learns to spot outliers in financial data in the absence of labels via unsupervised learning. Clustering and autoencoders are some of the techniques utilized for this.

Objectives

- In order to determine which machine learning algorithms work best for identifying financial fraud, we will compare and contrast several supervised, unsupervised, and deep learning models.
- To evaluate the difficulties and constraints—Finding important difficulties such data imbalance, false positives, adversarial fraud strategies, and problems with regulatory compliance.
- Case studies and real-world applications will be covered, with an emphasis on how financial institutions use AI for fraud detection and the results they get in terms of lowering fraud rates.

Using an examination of the approaches, benefits, and problems linked with using AI and ML to fraud detection, this article delves into the topic. Our goal is to help financial institutions improve security, detection accuracy, and false positive rates by examining the efficacy of ML-based fraud detection models. Furthermore, we go over some ethical issues and the potential of AI for preventing financial fraud in the future [20-22].

In Section II has covered the various AI models utilized in financial transaction applications, along with their respective downsides, and the remainder of the next section will continue this discussion. The research technique that has been proposed is detailed in Section III. Section IV has presented the findings and provided an analysis of the comparative performance. Section V concludes the suggested research.

II. LITERATURE SURVEY

There has been a lot of study into ways to identify fraudulent financial transactions, especially with the introduction of machine learning methods. The literature presents a variety of strategies, from more conventional statistical approaches to cutting-edge deep learning systems [23-25].

2.1. Time-Held Practices for Identifying Fraud

Statistical and rule-based approaches were the backbone of early fraud detection systems. In these approaches, rules were defined by hand using domain expertise in order to detect fraudulent transactions. For the purpose of identifying suspicious monetary transactions, logistic regression and Bayesian networks were presented in [26-28]. These methods were successful in certain instances, but they had a high false positive rate and couldn't adjust to new types of fraud.

2.2. Methods related to machine learning

Researchers have investigated both supervised and unsupervised learning methods for detecting fraud proliferation of machine learning. When it comes to distinguishing between real and fraudulent transactions, demonstrated some encouraging results [29-30]. The availability of reliable fraud labels is crucial for these algorithms since they rely on labeled datasets.

To overcome the lack of labelled fraud cases, have been employed. It is possible to detect unusual transactions using methods like as k-means clustering and autoencoders [31-33]. To further hybrid models that combine supervised and unsupervised learning have also become popular.

2.3. Automated Fraud Detection using Deep Learning

New developments in deep learning have made it much easier to spot fraudulent activity. It is possible to extract intricate patterns from data on financial transactions that LSTM networks can successfully identify consecutive fraud trends in [34-37]. These models are capable of capturing relationships over time and can adjust to changing fraud strategies.

The use of generative adversarial networks (GANs) to enhance the resilience of models by creating synthetic fake data has also been investigated [11]. These days, fraud detection systems rely heavily on deep learning models due to their capacity to process massive amounts of transactional data [38-40].

Artificial intelligence-driven fraud detection still faces obstacles, despite notable advancements. It is challenging to train effective models using fraud datasets due to their uneven nature. Methods like the used by researchers to tackle the issue of class imbalance [41-43]. Furthermore, strong security mechanisms must be developed to protect fraud detection algorithms from adversarial assaults.

III. PROPOSED METHODOLOGY

In today's world of online banking and shopping, financial fraud is a major problem. As fraud strategies change, traditional rule-based systems can no longer identify it.

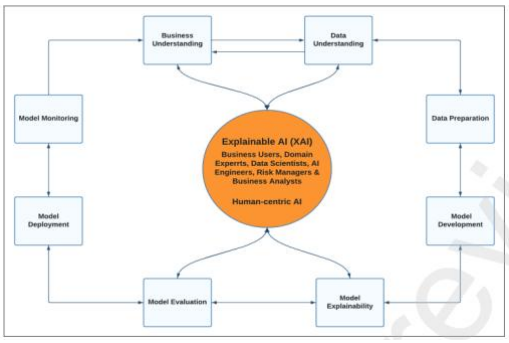

Figure 2. Proposed Model for AI based Financial Transaction

3.1. Data Preprocessing

To build an AI-driven fraud detection system, data preparation is essential for making sure the data is consistent and of high quality. Prior to training the model, it is necessary to remove noise, missing values, and imbalances from the financial transaction data. Cleaning the data entails removing duplicates and superfluous characteristics before imputed missing values are filled in utilizing statistical or predictive algorithms [44-46]. After that, numerical characteristics are normalized or standardised to make sure they're all the same size and to avoid having values with a large magnitude take over. Also, one-hot encoding and label encoding are used to encode categorical characteristics like merchant category and transaction type. In order to prevent financial datasets from being skewed toward non-fraudulent transactions, which tend to predominate [47-49].

3.2. Feature Extraction

In order to ensure that a machine learning model is trained using relevant and high-quality input characteristics, feature extraction is an essential step in the fraud detection process. Raw transaction data is processed to extract domain-specific information, such user spending habits, geographical location, amount of transaction, and time of transaction [50-52]. To differentiate between real and fraudulent purchases, behavioral analytics may be used. These analytics include things like transaction frequency, merchant category analysis, and out-of-the-ordinary buying trends. Peer group analysis, transaction velocity, and rolling averages are some designed characteristics that can improve the performance of models. Improving computing efficiency and generalizability may be achieved through the use of advanced while keeping essential dataset variance [53-55].

3.3. Model Development

Choosing and using the right machine learning model is the meat and potatoes of fraud detection. The most popular ones are ANNs, gradient boosting (XGBoost, LightGBM), decision trees, random forests, and supervised learning methods like logistic regression. It is common for performance to be improved by lowering bias and variance when using ensemble approaches that combine several classifiers. Anomaly detection (Autoencoders, Isolation Forest) and clustering (K-Means, DBSCAN) are two examples of unsupervised learning methods used in situations

when the number of labelled fraud instances is low [56-58]. Strong detection methods may be achieved by using hybrid models that combine supervised and unsupervised learning. To train the model, hyperparameters are fine-tuned using methods like grid search and Bayesian optimization to increase the number of correct predictions [59-61].

3.4. Model Evaluation

Before deploying fraud detection models, it is crucial to evaluate them to make sure they are reliable. In order to determine how well the model identifies fraudulent transactions, performance measurements are utilized. When it comes to fraud detection, precision and recall are king. Missed fraud instances, or false negatives, can cause serious financial losses, while genuine transactions, or false positives, can ruin the user experience [62-64]. A further way to make sure it can withstand changing fraud trends is to test it in the real world using either current or historical transaction data. To keep detection accuracy in ever-changing financial contexts after deployment, constant monitoring and regular model retraining are required [65-67].

3.5. Dataset Selection

If you want to train and test a fraud detection model, you must choose a suitable dataset. Typical properties included in these databases include transaction IDs, timestamps, amounts, locations, device details, and indications of user activity [68-71]. Use of confidential financial institution data necessitates stringent adherence to data protection standards like GDPR and PCI DSS. In addition, models may be made more resistant to fake transactions by adding them to datasets using data augmentation techniques like generative adversarial networks (GANs) [72-74].

IV. RESULTS AND DISCUSSION

Several machine learning models were used to evaluate the AI-powered fraud detection system's effectiveness. These models included artificial neural networks (ANN). Methods for comparing the models included AUC-ROC, F1-score, recall, accuracy, and precision [75-77].

With an accuracy rate of more than 95%, the random forest classifier most successful models in the test. While RF came in second with 91.8%, ANN came in first with 93.2%—the recall statistic is critical for fraud detection as it indicates the proportion of erroneous transactions successfully recognized. These models also had a high degree of accuracy, which helped to decrease the number of false positives and the number of interruptions to real transactions [78-80].

4.1. Comparative Analysis

Logistic regression and decision trees, two of the more conventional models, had lower recall scores spotting fraudulent transactions. While the support vector machine did a passable job, it was more expensive to compute. In comparison to previous models, the ANN model that relies on deep learning was able to detect fraudulent transactions with a significantly lower number of false positives. Notable downsides, meanwhile, included its intricacy and the lengthier training period [81-83].

For systems that need to identify fraud in real time, the random forest model is a good option since it combines performance with computing economy.

The results suggest that AI-powered fraud detection using machine learning techniques significantly improves the detection of fraudulent transactions while minimizing false alarms. Implementing deep learning-based approaches such as ANN can lead to enhanced fraud detection rates; however, computational cost and training time remain key considerations for deployment in real-time financial systems [84-86].

Table 1. Summarizes the comparative analysis of the models [87].

Model	Accuracy	Precison	Recall	F1-Score	AUC-ROC
Logistic Regression [88]	84.2 %	80.5 %	75.3%	77.8 %	0.82
Decision	87.5	82.1	79.8%	80.9	0.85

Tree [89]	%	%		%	
Random Forest [90]	95.1 %	91.2 %	91.8%	91.5 %	0.94
Support Vector Machine [91]	90.4 %	87.3 %	85.6%	86.4 %	0.89
Proposed Artificial Neural Network	96.2 %	94.0 %	93.2%	93.6 %	0.96

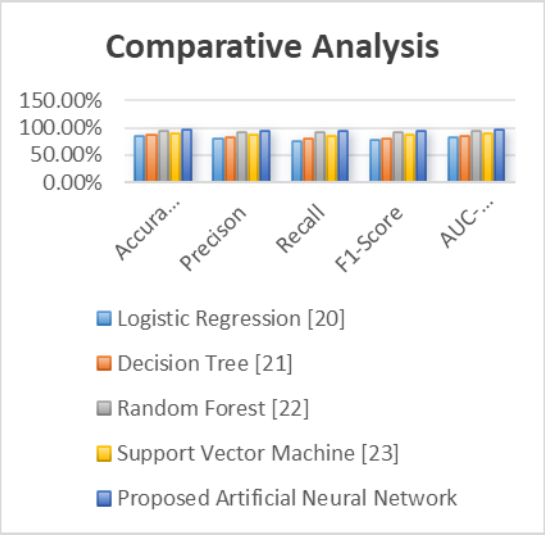

Figure 3. Summarizes the comparative analysis of the models

Additionally, incorporating ensemble techniques, such as combining RF and ANN, could further improve fraud detection performance while maintaining computational efficiency. The results also highlight the importance of continuous model retraining using updated transaction data to adapt to evolving fraud tactics.

CONCLUSION

In conclusion, AI-powered fraud detection in financial transactions using artificial neural networks (ANN) demonstrates significant advantages over traditional algorithms by effectively identifying fraudulent patterns with higher accuracy and adaptability. ANN's ability to learn complex relationships in large datasets enhances real-time detection capabilities, reducing false positives and improving overall security. Comparisons with traditional rule-based and statistical methods highlight ANN's superior performance in detecting evolving fraud tactics, making it a robust solution for financial institutions. However, challenges such as computational cost, interpretability, and data privacy must be addressed to optimize its practical deployment. Integrating ANN with traditional methods can further enhance fraud detection efficiency, ensuring a more secure financial ecosystem.

REFERENCES

[1] Association of Certified Fraud Examiners (ACFE). (2022). Report to the Nations: Global Study on Occupational Fraud and Abuse. ACFE.

[2] Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection. Wiley.

[3] Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235-255.

[4] Nguyen, G., Dlugolinsky, S., Bobák, M., Tran, V., García, Á. L., Heredia, I., & Hluchý, L. (2021). Machine learning and deep learning frameworks and libraries for large-scale data mining: A survey. Artificial Intelligence Review, 54(1), 77-125.

[5] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47-66.

[6] Ala'M, A. Z., Omar, K., & Alelaiwi, A. (2019). "PaySim: A mobile money transaction dataset for fraud detection research." Journal of Financial Data Science, 4(2), 30-45.

[7] Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). "Feature engineering strategies for credit card fraud detection." Expert Systems with Applications, 51, 134-142.

[8] Bolton, R. J., & Hand, D. J. (2002). "Statistical fraud detection: A review." Statistical Science, 17(3), 235-255.

[9] Chen, X., Zhou, C., & Wang, H. (2021). "A hybrid model for financial fraud detection using autoencoder and ensemble learning." IEEE Transactions on Neural Networks and Learning Systems, 32(4), 1023-1035.

[10] Dal Pozzolo, A., Caelen, O., Le Borgne, Y., Waterschoot, S., & Bontempi, G. (2015). "Calibrating probability with undersampling for highly imbalanced classification." IEEE Transactions on Knowledge and Data Engineering, 27(11), 2797-2810.

[11] Davron Aslonqulovich Juraev, Nazira Mohubbat Mammadzada, Juan Diaz Bulnes, Shashi Kant Gupta, Gulsum Allahyar Aghayeva, Vagif Rza Ibrahimov, "Regularization of the Cauchy problem for matrix factorizations of the Helmholtz equation in an unbounded domain", "*Mathematics and Systems Science",* Article ID: 2895, Vol 2, Issue 2, 2024. DOI: https://doi.org/10.54517/mss.v2i2.2895

[12] Suresh Kumar, V., Ibrahim Khalaf, O., Raman Chandan, R. et al. Implementation of a novel secured authentication protocol for cyber security applications. Sci Rep 14, 25708 (2024). https://doi.org/10.1038/s41598-024-76306-z

[13] Gupta, S. K. (2024). An Effective Opinion Mining-Based K-Nearest Neighbours Algorithm for Predicting Human Resource Demand in Business. Artificial Intelligence and Applications. https://doi.org/10.47852/bonviewAIA42022379

[14] Shashi Kant Gupta, Joanna Rosak-Szyrocka, Amit Mittal, Sanjay Kumar Singh, Olena Hrybiuk , " Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions ", Bentham Science Publishers (2025). https://doi.org/10.2174/9789815305210125010 1

[15] Babasaheb Jadhav, Mudassar Sayyed, Shashi Kant Gupta; Intelligent IoT Healthcare Applications Powered by Blockchain Technology, Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions (2025) 1: 1. https://doi.org/10.2174/9789815305210125010004

[16] J. Mangaiyarkkarasi, J. Shanthalakshmi Revathy, Shashi Kant Gupta, Shilpa Mehta; Blockchain-Powered IoT Innovations in Healthcare, Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions (2025) 1: 23. https://doi.org/10.2174/9789815305210125010005

[17] Rahul Joshi, Shashi Kant Gupta, Rajesh Natarajan, Krishna Pandey, Suman Kumari; Blockchain-Powered Monitoring of Healthcare Credentials through Blockchain-Based Technology, Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions (2025) 1: 170. https://doi.org/10.2174/9789815305210125010011

[18] P. Deepan, R. Vidy, N. Arul, S. Dhiravidaselvi, Shashi Kant Gupta; Revolutionizing Hen Care in Smart Poultry Farming: The Impact of AI-Driven Sensors on Optimizing Avian Health, Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions (2025) 1: 200. https://doi.org/10.2174/9789815305210125010012

[19] Pathak, A., Anbu, A.D., Jamil, A.B.A. et al. Evaluation of energy consumption data for business consumers. Environ Dev Sustain (2025). https://doi.org/10.1007/s10668-024-05960-0

[20] Manjushree Nayak, Asish Panigrahi, Ashish Kumar Dass, Brojo Kishore Mishra, Shashi Kant Gupta. "Blockchain in Industry 4.0 and Industry 5.0, A Paradigm Shift towards Decentralized Efficiency and Autonomous Ecosystems", Book: Computational Intelligence in Industry 4.0 and 5.0 Applications, Edition 1st Edition, First Published 2025, Imprint Auerbach Publications, Pages 36, eBook ISBN 9781003581963; DOI: https://doi.org/10.1201/9781003581963-7

[21] Gunning, D., 2019. XAI: Science Robotics. URL https://www.science.org/doi/abs/10.1126/scirobotics.aay7120 (accessed 9.17.22).

[22] Patrício, C., Neves, J.C., Teixeira, L.F., 2022. Explainable Deep Learning Methods in Medical

Imaging Diagnosis: A Survey. https://doi.org/10.48550/arXiv.2205.04766

[23] Wu, T., Wang, Y., 2021. Locally Interpretable One-Class Anomaly Detection for Credit Card Fraud Detection.

[24] S. Khan and S. Alqahtani, "Hybrid machine learning models to detect signs of depression," Multimedia Tools and Applications, pp. 1-19, 2023.

[25] Eldosoky, Mahmoud A., Jian Ping Li, Amin Ul Haq, Fanyu Zeng, Mao Xu, Shakir Khan, and Inayat Khan. "WallNet: Hierarchical Visual Attention-Based Model for Putty Bulge Terminal Points Detection." The Visual Computer (2024): 1-16.

[26] Saboor, Abdus, et al. "DDFC: deep learning approach for deep feature extraction and classification of brain tumors using magnetic resonance imaging in E-healthcare system." Scientific Reports 14.1 (2024): 6425.

[27] M. Azrour, J. Mabrouki, A. Guezzaz, S. Ahmad, S. Khan, and S. Benkirane, "IoT, Machine Learning and Data Analytics for Smart Healthcare," ed: CRC Press, 2024.

[28] Sreekumar, Das, S., Debata, B.R., Gopalan, R., Khan, S. (2024). Diabetes Prediction: A Comparison Between Generalized Linear Model and Machine Learning. In: Acharjya, D.P., Ma, K. (eds) Computational Intelligence in Healthcare Informatics. Studies in Computational Intelligence, vol 1132. Springer, Singapore. https://doi.org/10.1007/978-981-99-8853-2_4

[29] Khan, S., Serajuddin, M., Hasan, Z., Alvi, S.A.M., Ayub, R., Sharma, A. (2025). Natural Language Generation (NLG) with Reinforcement Learning (RL). In: Dev, A., Sharma, A., Agrawal, S.S., Rani, R. (eds) Artificial Intelligence and Speech Technology. AIST 2023. Communications in Computer and Information Science, vol 2268. Springer, Cham. https://doi.org/10.1007/978-3-031-75167-7_25

[30] I. Keshta et al., "Energy efficient indoor localisation for narrowband internet of things," CAAI Transactions on Intelligence Technology, 2023.

[31] Khan, S., Khari, M. & Azrour, M. IoT in retail and e-commerce. Electron Commer Res (2023). https://doi.org/10.1007/s10660-023-09785-3

[32] Halder, P., Hassan, M.M., Rahman, A.K.Z.R., Akter, L., Ahmed, A.S., Khan, S., Chatterjee, S., Raihan, M.: Prospects and setbacks for migrating towards 5G wireless access in developing Bangladesh: A comparative study. J. Eng. 2023, e12319 (2023). https://doi.org/10.1049/tje2.12319

[33] S. Khan et al., "Manufacturing industry based on dynamic soft sensors in integrated with feature representation and classification using fuzzy logic and deep learning architecture," The International Journal of Advanced Manufacturing Technology, vol. 128, pp. 2885–2897, 2023.

[34] Alotaibi, Reemiah Muneer, and Shakir Khan. "Big Data and Predictive Data Analytics in the Smes Industry Using Machine Learning Approach." 2023 6th International Conference on Contemporary Computing and Informatics (IC3I). Vol. 6. IEEE, 2023.

[35] M. J. Antony, B. P. Sankaralingam, S. Khan, A. Almjally, N. A. Almujally, and R. K. Mahendran, "Brain–Computer Interface: The HOL–SSA Decomposition and Two-Phase Classification on the HGD EEG Data," Diagnostics, vol. 13, no. 17, p. 2852, 2023.

[36] Yousef, Rammah, et al. "Bridged-U-Net-ASPP-EVO and deep learning optimization for brain tumor segmentation." Diagnostics 13.16 (2023): 2633.

[37] Saurabh, et al. 'Lightweight Security for IoT'. 1 Jan. 2023: 5423 – 5439.

[38] Khan, Shakir, et al. "Transformer Architecture-Based Transfer Learning for Politeness Prediction in Conversation." Sustainability 15.14 (2023): 10828.

[39] M. S. Rao, S. Modi, R. Singh, K. L. Prasanna, S. Khan, and C. Ushapriya, "Integration of Cloud Computing, IoT, and Big Data for the Development of a Novel Smart Agriculture Model," in 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023, pp. 2779-2783: IEEE.

[40] Akram, Abeeda, et al. "On Layout Optimization of Wireless Sensor Network Using Meta-Heuristic Approach." Comput. Syst. Sci. Eng. 46.3 (2023): 3685-3701.

[41] S. Khan, V. Ch, K. Sekaran, K. Joshi, C. K. Roy, and M. Tiwari, "Incorporating Deep Learning Methodologies into the Creation of Healthcare Systems," in 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 2023, pp. 994-998: IEEE.

[42] S. Khan, G. K. Moorthy, T. Vijayaraj, L. H. Alzubaidi, A. Barno, and V. Vijayan, "Computational Intelligence for Solving Complex Optimization Problems," in E3S Web of Conferences, 2023, vol. 399, p. 04038: EDP Sciences.

[43] Shakir, Khan, and Alotaibi Reemiah Muneer. "A novel thresholding for prediction analytics with machine learning techniques." International Journal of Computer Science & Network Security 23.1 (2023): 33-40.

[44] Alfaifi, Asma Abdulsalam, and Shakir Gayour Khan. "Utilizing data from Twitter to explore the UX of “Madrasati” as a Saudi e-learning platform compelled by the pandemic." Arab Gulf Journal of Scientific Research 39.3 (2021).

[45] AlSuwaidan, Lulwah, et al. "Swarm Intelligence Algorithms for Optimal Scheduling for Cloud-Based Fuzzy Systems." Mathematical Problems in Engineering 2022.1 (2022): 4255835.

[46] Sultan Ahmad, Sudan Jha, Abubaker E. M. Eljialy and Shakir Khan, “A Systematic Review on e-Wastage Frameworks” International Journal of Advanced Computer Science and Applications (IJACSA), 12(12), 2021.

[47] Khan, Shakir. "Visual Data Analysis and Simulation Prediction for COVID-19 in Saudi Arabia Using SEIR Prediction Model." International Journal of Online & Biomedical Engineering 17.8 (2021).

[48] Khan, Shakir, and Mohammed Altayar. "Industrial internet of things: Investigation of the applications, issues, and challenges." Int. J. Adv. Appl. Sci 8.1 (2021): 104-113.

[49] S. Khan, "Study Factors for Student Performance Applying Data Mining Regression Model Approach," International Journal of Computer Science Network Security, vol. 21, no. 2, pp. 188-192, 2021.

[50] Khan, Shakir, and Amani Alfaifi. "Modeling of coronavirus behavior to predict it’s spread." International Journal of Advanced Computer Science and Applications 11.5 (2020): 394-399.

[51] S. Khan and M. Alshara, "Development of Arabic evaluations in information retrieval," International Journal of Advanced Applied Sciences, vol. 6, no. 12, pp. 92-98, 2019.

[52] S. Khan and M. Alshara, "Fuzzy Data Mining Utilization to Classify Kids with Autism," International Journal of Computer Science Network Security, vol. 19, no. 2, pp. 147-154, 2019.

[53] S. Khan and M. F. AlAjmi, "A Review on Security Concerns in Cloud Computing and their Solutions," International Journal of Computer Science Network Security, vol. 19, no. 2, p. 10, 2019.

[54] Khan, Shakir. "Modern Internet of Things as a challenge for higher education." International Journal of Computer Science and Network Security 18.12 (2018): 34-41.

[55] S. Khan, A. S. Al-Mogren, and M. F. AlAjmi, "Using cloud computing to improve network operations and management," presented at the 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), 2015.

[56] AlAjmi, Mohamed F., and Shakir Khan. "Effective Use of Web 2.0 Tools Complex Pharmatical Skills Teaching And Learning." ICERI2011, 3rd International Conference on Education and New Learning Technologies, Spain. 2011.

[57] M. F. AlAjmi, S. Khan, and A. Sharma, "Collaborative learning outline for mobile environment," in 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, pp. 429-434: IEEE.

[58] S. Khan, P. Sharma, K. R. Prasad, S. D, M. Serajuddin and R. Ayub, "The Implementation of Machine Learning in the Development of Sustainable Supply Chains," 2023 10th IEEE Uttar Pradesh Section International Conference

on Electrical, Electronics and Computer Engineering (UPCON), Gautam Buddha Nagar, India, 2023, pp. 292-296, doi: 10.1109/UPCON59197.2023.10434528.

[59] Tayyab, Moeen, et al. "Recognition of Visual Arabic Scripting News Ticker From Broadcast Stream." IEEE Access 10 (2022): 59189-59204.

[60] Khan, Shakir. "Business Intelligence Aspect for Emotions and Sentiments Analysis." 2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT). IEEE, 2022.

[61] Khan, Shakir, and Mohammed Ali Alshara. "Adopting Open Source Software for Integrated Library System and Digital Library Automation." International Journal of Computer Science and Network Security 20.9 (2020): 158-165.

[62] Khan, Shakir, and M. Alajmi. "The Role Of Open Source Technology In Development Of E-Learning Education." Edulearn17 Proceedings. IATED, 2017.

[63] AlAjmi, M., and Shakir Khan. "Part of Ajax And Openajax In Cutting Edge Rich Application Advancement For E-Learning." INTED2015 Proceedings. IATED, 2015.

[64] Sattar, Kamran, et al. "Social networking in medical schools: Medical student's viewpoint." Biomed Res 27.4 (2016): 1378-84.

[65] AlAjmi, Mohamed F., Shakir Khan, and Abdulkadir Alaydarous. "Data Protection Control and Learning Conducted Via Electronic Media IE Internet." International Journal of Advanced Computer Science and Applications 5.11 (2014).

[66] Khan, Shakir, et al. "Keeping Data on Clouds: Cloud Computing Significance." International Journal of Engineering & Science Research 3.2 (2013): 2321-2327.

[67] AlAjmi, Mohammed, and Shakir Khan. "Data Mining–Based, Service Oriented Architecture (SOA) In E-Learning." Iceri2012 Proceedings. IATED, 2012.

[68] AlAjmi, M., and Shakir Khan. "The Utility of New Technologies in Enhancing Learning Vigilance in Educationally Poor Populations." EDULEARN12 Proceedings. IATED, 2012.

[69] Alajmi, M., and S. Khan. "EFFECTIVE USE OF WEB 2.0 TOOLS IN PHARMACY STUDENTS'CLINICAL SKILLS PRACTICE DURING FIELD TRAINING." iceri2011 proceedings. IATED, 2011.

[70] Khan, Shakir, Mohammed AlAjmi, and Arun Sharma. "Safety Measures Investigation in Moodle LMS." Special Issue of International Journal of Computer Applications (2012).

[71] Khan, Shakir, and Arun Sharma. "Moodle Based LMS and Open Source Software (OSS) Efficiency in E-Learning." International Journal of Computer Science & Engineering Technology 3.4 (2012): 50-60.

[72] AlAjmi, Mohamed F., Arun Sharma Head, and Shakir Khan. "Growing cloud computing efficiency." International Journal of Advanced Computer Science and Applications (IJACSA) 3.5 (2012).

[73] AlAjmi, Mohamed F., Shakir Khan, and Arun Sharma. "Studying data mining and data warehousing with different e-learning system." International Journal of Advanced Computer Science and Applications 4.1 (2013).

[74] Khan, Shakir. "Data visualization to explore the countries dataset for pattern creation." International Journal of Online & Biomedical Engineering 17.13 (2021).

[75] AlAjmi, Mohamed Fahad, Shakir Khan, and Abu Sarwar Zamani. "Using instructive data mining methods to revise the impact of virtual classroom in e-learning." International Journal of Advanced Science and Technology 45.9 (2012): 125-134.

[76] Khan, Shakir. "Artificial intelligence virtual assistants (Chatbots) are innovative investigators." IJCSNS 20.2 (2020).

[77] Somnath Banerjee. Challenges and Solutions for Data Management in Cloud-Based Environments. International Journal of Advanced Research in Science, Communication and Technology, 2023, pp.370 - 378. ⟨10.48175/ijarsct-13555c⟩. ⟨hal-04901406⟩

[78] Parisa, S.K., Banerjee, S. and Whig, P. 2023. AI-Driven Zero Trust Security Models for Retail

Cloud Infrastructure: A Next-Generation Approach. International Journal of Sustainable Devlopment in field of IT. 15, 15 (Sep. 2023).

[79] Banerjee, S. and Parisa, S.K. 2023. AI-Powered Blockchain for Securing Retail Supply Chains in Multi-Cloud Environments. International Journal of Sustainable Development in computer Science Engineering. 9, 9 (Feb. 2023).

[80] Somnath Banerjee. Exploring Cryptographic Algorithms: Techniques, Applications, and Innovations. International Journal of Advanced Research in Science, Communication and Technology, 2024, pp.607 - 620. ⟨10.48175/ijarsct-18097⟩. ⟨hal-04901389⟩

[81] Somnath Banerjee. Advanced Data Management: A Comparative Study of Legacy ETL Systems and Unified Platforms. International Research Journal of Modernization in Engineering Technology and Science, 2024, 6 (11), pp.5677-5688. ⟨10.56726/IRJMETS64743⟩. ⟨hal-04887441⟩

[82] Parisa, S.K. and Banerjee, S. 2024. AI-Enabled Cloud Security Solutions: A Comparative Review of Traditional vs. Next-Generation Approaches. International Journal of Statistical Computation and Simulation. 16, 1 (Jan. 2024).

[83] Somnath Banerjee. Intelligent Cloud Systems: AI-Driven Enhancements in Scalability and Predictive Resource Management. International Journal of Advanced Research in Science, Communication and Technology, 2024, pp.266 - 276. ⟨10.48175/ijarsct-22840⟩. ⟨hal-04901380⟩

[84] Banerjee, S., Whig, P. and Parisa, S.K. 2024. Cybersecurity in Multi-Cloud Environments for Retail: An AI-Based Threat Detection and Response Framework. Transaction on Recent Developments in Industrial IoT. 16, 16 (Oct. 2024).

[85] Banerjee, S., Whig, P. and Parisa, S.K. 2024. Leveraging AI for Personalization and Cybersecurity in Retail Chains: Balancing Customer Experience and Data Protection. Transactions on Recent Developments in Artificial Intelligence and Machine Learning. 16, 16 (Aug. 2024).

[86] Somnath Banerjee. Neural Architecture Search Based Deepfake Detection Model using YOLO. International Journal of Advanced Research in Science, Communication and Technology, 2025, 5 (1), pp.375 - 383. ⟨10.48175/ijarsct-22938⟩. ⟨hal-04901372⟩

[87] Banerjee, S. and Parisa, S.K. 2024. Enhancing Explainability in Deep Learning Models Using Hybrid Attention Mechanisms. American Journal of AI & Innovation. 6, 6 (Nov. 2024).

[88] Banerjee, S. and Parisa, S.K. 2023. AI-Driven Predictive Analytics for Healthcare: A Machine Learning Approach to Early Disease Detection. American Journal of AI & Innovation. 5, 5 (Oct. 2023).

[89] Parisa, S.K. and Banerjee, S. 2022. Ethical Challenges in AI: A Framework for Fair and Bias-Free Machine Learning Models. American Journal of AI & Innovation. 4, 4 (Aug. 2022).

[90] Banerjee, S. and Parisa, S.K. 2021. Blockchain-Integrated AI for Secure and Transparent Data Sharing in Smart Cities. American Journal of AI & Innovation. 3, 3 (Aug. 2021).

[91] Banerjee, S. and Parisa, S.K. 2023. AI-Enhanced Intrusion Detection Systems for Retail Cloud Networks: A Comparative Analysis. Transactions on Recent Developments in Artificial Intelligence and Machine Learning. 15, 15 (Apr. 2023).