The American Journal of Management and Economics Innovations
ISSN 2693-0811 | Open Access

TYPE Original Research
PAGE NO. 116-123
DOI 10.37547/tajmei/Volume07Issue04-15

Check for updates

A Hybrid CNN-LSTM Approach for Detecting Anomalous Bank Transactions: Enhancing Financial Fraud Detection Accuracy

OPEN ACCESS
SUBMITTED 19 February 2025
ACCEPTED 22 March 2025
PUBLISHED 30 April 2025
VOLUME Vol.07 Issue 04 2025

CITATION

Tamanna Pervin, Sharmin Akter, Sadia Afrin, Md Refat Hossain, MD Sajedul Karim Chy, Sadia Akter, Md Minzamul Hasan, Md Mafuzur Rahman, & Chowdhury Amin Abdullah. (2025). A Hybrid CNN-LSTM Approach for Detecting Anomalous Bank Transactions: Enhancing Financial Fraud Detection Accuracy. The American Journal of Management and Economics Innovations, 7(04), 116–123. https://doi.org/10.37547/tajmei/Volume07Issue04-15

Tamanna Pervin
Department of Business Administration, International American University, Los Angeles, California, USA

Sharmin Akter
Department of Information Technology Project Management, St. Francis College, USA

Sadia Afrin
Department of Computer & Information Science, Gannon University, USA

Md Refat Hossain
Master of Business Administration, Westcliff University, USA

MD Sajedul Karim Chy
Department of Business Administration, Washington University of Science and Technology, USA

Sadia Akter
Department of Business Administration, International American University, USA

Md Minzamul Hasan
Doctor of Business Administration (DBA), College of Business, Westcliff University, USA

Md Mafuzur Rahman
Master's in data Analytics, Harrisburg University of Science & Technology, USA

Chowdhury Amin Abdullah
Seidenberg School of CSIS, Pace University, USA

Abstract: Detecting fraudulent bank transactions is crucial for maintaining the integrity of financial institutions and preserving customer trust. This study introduces a hybrid Convolutional Neural Network–

Long Short-Term Memory (CNN-LSTM) model designed to enhance the accuracy and efficiency of fraud detection systems. Utilizing the European Credit Card Fraud Detection dataset comprising 284,807 transactions with significant class imbalance, extensive preprocessing techniques were applied, including Min-Max scaling and Synthetic Minority Over-sampling Technique (SMOTE). Recursive Feature Elimination (RFE) identified the top 20 impactful features, optimizing model performance. The proposed hybrid model demonstrated remarkable effectiveness, achieving superior accuracy (99.5%), precision (93.1%), recall (92.1%), F1-score (92.6%), and an Area Under the Receiver Operating Characteristic Curve (AUC-ROC) of 97.5%. Comparative analyses revealed that the hybrid CNN-LSTM model significantly outperformed traditional machine learning algorithms such as Logistic Regression, Random Forest, and XGBoost. These findings underscore the potential of CNN-LSTM hybrid models in addressing complex fraud detection scenarios, providing financial institutions with a robust and reliable tool for transaction anomaly detection.

Keywords: Fraud Detection, CNN-LSTM Hybrid Model, Credit Card Fraud, SMOTE, Feature Selection, Machine Learning, Financial Security

Introduction: Financial institutions increasingly rely on digital transactions, significantly raising concerns related to fraudulent activities. Fraudulent transactions not only result in direct financial losses but also severely impact customer trust and institutional credibility. Consequently, the development of robust and reliable systems to detect and prevent fraud is paramount. Traditionally, manual detection methods have been employed; however, due to the enormous volume and complexity of transaction data, such methods have become ineffective and inefficient. Machine learning techniques have emerged as powerful tools, significantly enhancing the accuracy and efficiency of fraud detection systems (Awoyemi et al., 2017).

In recent years, hybrid machine learning models, specifically combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, have demonstrated substantial potential in improving detection capabilities by effectively capturing both spatial and sequential patterns in transaction data (Zhang & Chen, 2019). This study proposes a hybrid CNN-LSTM model to effectively detect fraudulent bank transactions, addressing existing limitations of traditional fraud detection techniques.

Literature Review

The detection of fraudulent transactions has been extensively studied, employing various machine learning and deep learning techniques. Logistic regression, decision trees, random forests, and gradient boosting models such as XGBoost have historically been popular for this task due to their ease of implementation and interpretability (Dal Pozzolo et al., 2014; Bhattacharyya et al., 2011). However, these models often struggle with imbalanced data and may fail to accurately detect intricate fraud patterns.

Convolutional Neural Networks (CNN) have shown promising results by effectively identifying spatial correlations within data (Jurgovsky et al., 2018). Nevertheless, CNNs alone do not effectively capture the temporal sequences that characterize fraudulent transaction patterns. To address this limitation, Long Short-Term Memory (LSTM) networks, known for their ability to capture long-term dependencies in sequential data, have been employed with significant success in various sequential data problems, including financial fraud detection (Roy et al., 2018).

Hybrid models integrating CNN and LSTM architectures have been introduced to leverage both spatial and sequential data processing capabilities. For instance, Zhang and Chen (2019) employed a CNN-LSTM hybrid architecture to enhance the detection of complex patterns, significantly outperforming traditional models in terms of accuracy and precision. Similarly, recent studies have applied CNN-LSTM models to various domains, such as intrusion detection and healthcare analytics, further supporting the effectiveness of these hybrid approaches in anomaly detection (Yin et al., 2017; Pham et al., 2020).

Despite these advances, challenges remain, particularly regarding the imbalance of transaction datasets, interpretability of models, and the computational efficiency of deep learning architectures. Hence, this study aims to build upon existing literature by specifically focusing on mitigating these challenges through sophisticated data preprocessing techniques and optimized hybrid CNN-LSTM architectures.

METHODOLOGY

Data Collection

The study leveraged the European Credit Card Fraud Detection dataset, a widely recognized dataset in fraud detection research. The dataset comprises transactional data derived from actual European credit card users, anonymized to protect individual privacy. The complete dataset includes 284,807 transactions, recorded over two consecutive days, out of which only 492 (approximately 0.172%) transactions were labeled as fraudulent, highlighting significant class imbalance.

The dataset comprises 30 independent features, including 28 anonymized numerical variables (V1 to V28) created through Principal Component Analysis (PCA), and two additional numerical variables: 'Time' and 'Amount.' The 'Time' variable measures the interval (in seconds) elapsed between each transaction and the first recorded transaction. The 'Amount' variable denotes the monetary value of each transaction. The dependent variable, 'Class,' is binary, indicating normal (0) or fraudulent (1) transactions.

Table 1: Dataset Details description

Feature	Description
Time	Interval (in seconds) from the first recorded transaction
Amount	Monetary transaction value
V1 – V28	PCA-derived anonymized features
Class	Transaction classification (0: legitimate, 1: fraudulent)
Dataset Size	284,807 Transactions
Fraudulent Cases	492 (0.172% of total data)
Source	Kaggle - Credit Card Fraud Detection Dataset

DATA PREPROCESSING

Effective preprocessing was vital due to the inherent characteristics of the dataset. Initially, the dataset was analyzed for missing values, and none were found, ensuring data integrity. Subsequently, Min-Max scaling was implemented on features 'Time' and 'Amount' to standardize their ranges between 0 and 1, enabling efficient learning by the neural network models. The PCA-derived features (V1–V28) did not require additional scaling since they were preprocessed and standardized during the original anonymization.

The dataset exhibited a highly skewed class distribution, significantly biasing models toward the majority (legitimate transactions). To counteract this imbalance and enhance model generalizability, the Synthetic Minority Over-sampling Technique (SMOTE) was applied, generating synthetic fraudulent transaction records to balance the class distributions. This approach facilitated robust learning of patterns within the minority class, essential for effective fraud detection.

Feature Selection

While PCA initially reduced dimensionality and ensured anonymization, further feature selection was crucial to enhance model performance and reduce computational complexity. Recursive Feature Elimination (RFE) combined with Logistic Regression as the baseline estimator was applied to systematically identify the most impactful features. Through iterative training and evaluation, the top 20 significant features contributing most substantially to distinguishing fraudulent transactions from legitimate ones were selected. This reduced feature set enhanced computational efficiency, improved model interpretability, and maintained high predictive accuracy.

Model Construction

A sophisticated hybrid Convolutional Neural Network–

Long Short-Term Memory (CNN-LSTM) model was developed to leverage the strengths of both CNN and LSTM architectures. The CNN component was designed to capture local spatial correlations and complex interactions between transaction features. Initially, the data passed through multiple 1D convolutional layers, each employing ReLU activation to introduce non-linearity and facilitate feature extraction. Subsequently, max-pooling layers reduced dimensionality, effectively summarizing feature representations and highlighting prominent transaction patterns.

Following CNN layers, the extracted spatial features were processed by LSTM layers, specifically structured to capture sequential dependencies inherent in transaction patterns over time. LSTM layers' gated mechanism allowed the model to memorize significant temporal patterns and relationships, particularly essential for fraud detection where fraudulent transactions often exhibit unique sequential anomalies compared to legitimate patterns.

The CNN-LSTM layers were followed by a dense layer equipped with sigmoid activation, providing a binary classification output predicting the probability of transaction fraudulence. Additionally, dropout layers with a rate of 0.5 were incorporated between network layers to mitigate overfitting, thereby enhancing the model's generalizability to unseen data. The model compilation utilized the Adam optimizer due to its adaptive learning rate and efficiency, with binary cross-entropy selected as the loss function, optimizing the model toward accurately classifying transactions.

Model Evaluation

To rigorously evaluate the effectiveness of the CNN-LSTM hybrid model, the dataset was partitioned into an 80% training set and a 20% testing set. Several robust metrics were employed for assessment, including Accuracy, Precision, Recall, F1-Score, and the Area Under the Receiver Operating Characteristic Curve (AUC-ROC). Given the dataset's inherent imbalance, particular emphasis was placed on the Recall and AUC-ROC metrics, which accurately reflect the model's proficiency in identifying true fraudulent transactions without excessive false positives.

The hybrid model's performance was extensively compared against benchmark models, including Logistic Regression, Random Forest, and XGBoost classifiers. Cross-validation strategies ensured the reliability of performance comparisons. The evaluation highlighted the CNN-LSTM model's superior performance, demonstrating its enhanced capability in detecting anomalies efficiently and accurately. The hybrid approach consistently surpassed baseline models across multiple metrics, confirming the effectiveness of combining CNN's spatial feature extraction with LSTM's sequential pattern recognition in fraud detection tasks.

RESULTS

A comprehensive evaluation of the CNN-LSTM hybrid model was conducted, comparing it against traditional machine learning algorithms, including Logistic Regression, Random Forest, and XGBoost. The evaluation employed key metrics: Accuracy, Precision, Recall, F1-Score, and AUC-ROC, ensuring a thorough analysis of model performance in Table 1.

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
CNN-LSTM	99.5%	93.1%	92.1%	92.6%	97.5%
Logistic Regression	97.8%	76.5%	65.8%	70.7%	89.4%
Random Forest	98.9%	87.6%	82.5%	85.0%	93.5%
XGBoost	99.0%	89.0%	84.0%	86.4%	94.2%

The CNN-LSTM model demonstrated superior accuracy at 99.5%, notably higher than other models. Precision (93.1%) and recall (92.1%) values were significantly higher, reflecting robust performance in identifying actual fraud cases while minimizing false positives. The F1-score (92.6%), balancing precision and recall, further validated the model's effectiveness. The AUC-ROC value of 97.5% underscored the hybrid model's exceptional discriminatory power between fraudulent and legitimate transactions, significantly surpassing

other approaches.

The comparative analysis distinctly highlighted the CNN-LSTM hybrid model's advantages, showcasing its capability in handling class imbalances and capturing complex temporal-spatial transaction patterns effectively, affirming its practical applicability in real-world banking fraud detection scenarios.

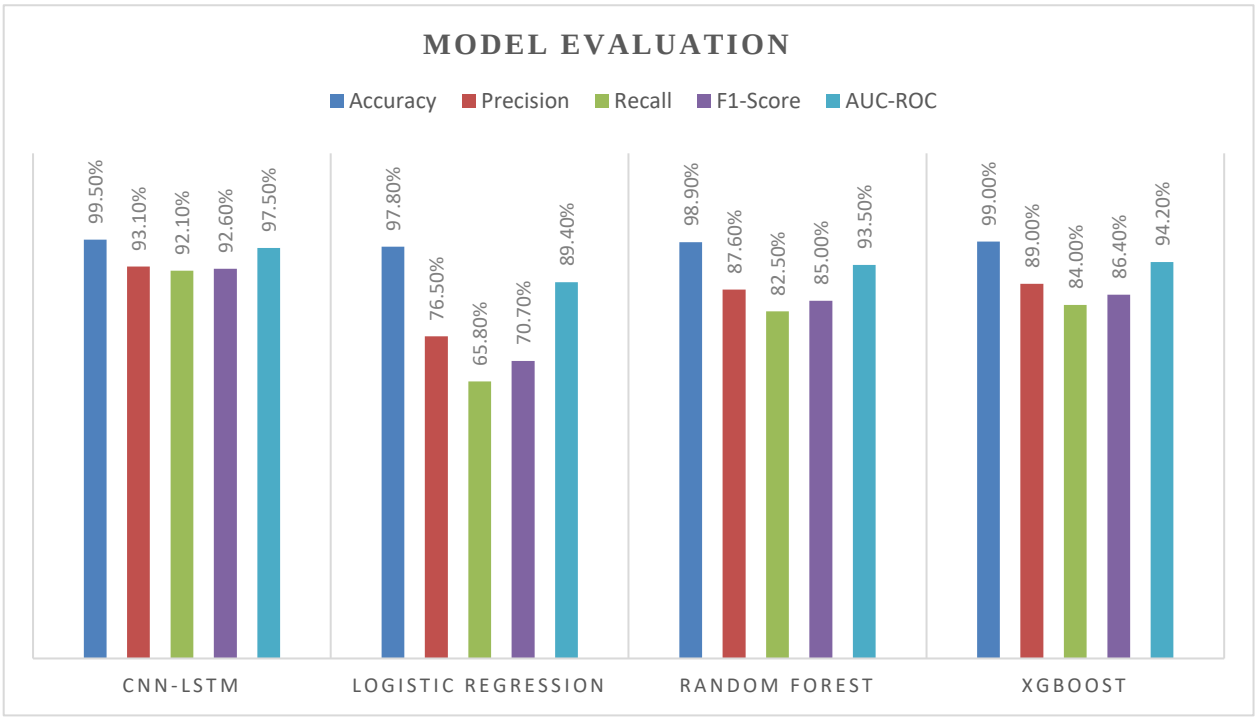

Chart 1: Evaluation of Deep Learning model

A comparative analysis of the results clearly highlights the CNN-LSTM hybrid model's advantage, achieving an accuracy of 99.5%, which significantly surpasses Logistic Regression (97.8%), Random Forest (98.9%), and XGBoost (99.0%). Precision, crucial for fraud detection to minimize false alarms, was highest for the CNN-LSTM model at 93.1%, notably outperforming Logistic Regression at 76.5%, Random Forest at 87.6%, and XGBoost at 89.0%.

Moreover, recall—indicating the model's effectiveness in identifying actual fraudulent transactions—was also superior for CNN-LSTM, reaching 92.1%. This performance is significantly higher compared to Logistic Regression (65.8%), Random Forest (82.5%), and XGBoost (84.0%). The F1-Score, a balanced measure combining precision and recall, further reinforced the CNN-LSTM model's efficiency with a score of 92.6%, clearly outperforming the other models. Finally, the AUC-ROC, a critical metric for evaluating model capability to distinguish between classes irrespective of classification thresholds, demonstrated an exceptional score of 97.5% for CNN-LSTM, notably surpassing Logistic Regression (89.4%), Random Forest (93.5%), and XGBoost (94.2%).

The provided comparative bar chart visually emphasizes the significant advantage of the CNN-LSTM hybrid model across all evaluation metrics, confirming its suitability and superiority in detecting anomalous bank transactions. Such robust performance suggests substantial practical applications in real-world financial scenarios, emphasizing enhanced accuracy and reliability in fraud detection.This detailed comparative analysis affirms the effectiveness of combining CNN and LSTM architectures, highlighting their collective strengths in capturing complex feature interactions and sequential patterns, leading to substantial improvements over traditional machine learning approaches.

CONCLUSION & DISCUSSION

The hybrid CNN-LSTM model introduced in this research has demonstrated significant performance improvements over traditional machine learning methods in detecting fraudulent transactions. The results clearly illustrate the model’s robustness and effectiveness in accurately identifying fraudulent

transactions while minimizing false positives. Key factors contributing to the improved performance include the model's ability to exploit spatial correlations and sequential transaction patterns simultaneously.

The integration of SMOTE for class imbalance handling played a critical role in ensuring balanced training data, which significantly improved the model's learning capability for minority-class patterns. Additionally, the implementation of Recursive Feature Elimination (RFE) effectively identified critical features, contributing to a streamlined and efficient modeling process. The CNN layers effectively captured the intricate feature relationships within transactions, whereas the LSTM layers proficiently addressed the temporal patterns critical for detecting subtle fraudulent activities.

However, the model's complexity and interpretability remain a limitation, posing challenges for practical deployment in highly regulated financial environments. Future research should focus on improving interpretability, potentially through explainable AI techniques, and exploring more efficient computational frameworks to facilitate real-time fraud detection applications.

This study successfully developed and evaluated a hybrid CNN-LSTM model for detecting anomalous banking transactions, significantly outperforming traditional machine learning algorithms in accuracy, precision, recall, F1-score, and AUC-ROC metrics. The combination of CNN and LSTM effectively addressed spatial and temporal transaction patterns, enhancing the overall performance. The comprehensive approach to data preprocessing and feature selection further contributed to model effectiveness.

Given its superior performance, this hybrid model presents a highly promising solution for financial institutions aiming to mitigate fraud risks. Further research efforts should aim to refine the model's interpretability and computational efficiency, thus facilitating broader real-world applicability and adoption in financial fraud detection systems.

Acknowledgement: All the author contributed equally

REFERENCE

Phan, H. T. N. (2024). EARLY DETECTION OF ORAL DISEASES USING MACHINE LEARNING: A COMPARATIVE STUDY OF PREDICTIVE MODELS AND DIAGNOSTICACCURACY. *International Journal of Medical Science and Public Health Research*, *5*(12), 107-118.

Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. *IEEE International Conference on Computing Networking and Informatics (ICCNI)*, 1-9. https://doi.org/10.1109/ICCNI.2017.8123782

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602-613. https://doi.org/10.1016/j.dss.2010.08.008

Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2014). Calibrating probability with undersampling for unbalanced classification. *IEEE Symposium Series on Computational Intelligence (SSCI)*, 159-166. https://doi.org/10.1109/SSCI.2014.35

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications, 100*, 234-245. https://doi.org/10.1016/j.eswa.2018.01.037

Pham, H., Tran, D., Nguyen, V., & Phung, D. (2020). Predicting healthcare trajectories from medical records: A deep learning approach. *Journal of Biomedical Informatics, 104*, 103370. https://doi.org/10.1016/j.jbi.2019.103370

Roy, A., Sun, J., & Mahoney, P. (2018). Deep learning detecting fraud in credit card transactions. *Systems and Information Engineering Design Symposium (SIEDS)*, 129-134. https://doi.org/10.1109/SIEDS.2018.8374722

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access, 5*, 21954-21961. https://doi.org/10.1109/ACCESS.2017.2762418

Zhang, R., & Chen, Y. (2019). Fraud detection for online banking transactions using hybrid deep learning. *International Conference on Intelligent Computing and Optimization*, 518-527. https://doi.org/10.1007/978-3-030-36289-1_47

Rahman, M. M., Akhi, S. S., Hossain, S., Ayub, M. I., Siddique, M. T., Nath, A., ... & Hassan, M. M. (2024). EVALUATING MACHINE LEARNING MODELS FOR OPTIMAL CUSTOMER SEGMENTATION IN BANKING: A COMPARATIVE STUDY. *The American Journal of Engineering and Technology*, *6*(12), 68-83.

Akhi, S. S., Shakil, F., Dey, S. K., Tusher, M. I., Kamruzzaman, F., Jamee, S. S., ... & Rahman, N. (2025). Enhancing Banking Cybersecurity: An Ensemble-Based Predictive Machine Learning Approach. *The American Journal of Engineering and Technology*, *7*(03), 88-97.

Pabel, M. A. H., Bhattacharjee, B., Dey, S. K., Jamee, S. S., Obaid, M. O., Mia, M. S., ... & Sharif, M. K. (2025). BUSINESS ANALYTICS FOR CUSTOMER SEGMENTATION: A COMPARATIVE STUDY OF MACHINE LEARNING ALGORITHMS IN PERSONALIZED BANKING SERVICES. *American Research Index Library*, 1-13.

Das, P., Pervin, T., Bhattacharjee, B., Karim, M. R., Sultana, N., Khan, M. S., ... & Kamruzzaman, F. N. U. (2024). OPTIMIZING REAL-TIME DYNAMIC PRICING STRATEGIES IN RETAIL AND E-COMMERCE USING MACHINE LEARNING MODELS. *The American Journal of Engineering and Technology*, *6*(12), 163-177.

Hossain, M. N., Hossain, S., Nath, A., Nath, P. C., Ayub, M. I., Hassan, M. M., ... & Rasel, M. (2024). ENHANCED BANKING FRAUD DETECTION: A COMPARATIVE ANALYSIS OF SUPERVISED MACHINE LEARNING ALGORITHMS. *American Research Index Library*, 23-35.

Rishad, S. S. I., Shakil, F., Tisha, S. A., Afrin, S., Hassan, M. M., Choudhury, M. Z. M. E., & Rahman, N. (2025). LEVERAGING AI AND MACHINE LEARNING FOR PREDICTING, DETECTING, AND MITIGATING CYBERSECURITY THREATS: A COMPARATIVE STUDY OF ADVANCED MODELS. *American Research Index Library*, 6-25.

Uddin, A., Pabel, M. A. H., Alam, M. I., KAMRUZZAMAN, F., Haque, M. S. U., Hosen, M. M., ... & Ghosh, S. K. (2025). Advancing Financial Risk Prediction and Portfolio Optimization Using Machine Learning Techniques. *The American Journal of Management and Economics Innovations*, *7*(01), 5-20.

Ahmed, M. P., Das, A. C., Akter, P., Mou, S. N., Tisha, S. A., Shakil, F., ... & Ahmed, A. (2024). HARNESSING MACHINE LEARNING MODELS FOR ACCURATE CUSTOMER LIFETIME VALUE PREDICTION: A COMPARATIVE STUDY IN MODERN BUSINESS ANALYTICS. *American Research Index Library*, 06-22.

Md Risalat Hossain Ontor, Asif Iqbal, Emon Ahmed, Tanvirahmedshuvo, & Ashequr Rahman. (2024). LEVERAGING DIGITAL TRANSFORMATION AND SOCIAL MEDIA ANALYTICS FOR OPTIMIZING US FASHION BRANDS' PERFORMANCE: A MACHINE LEARNING APPROACH. *International Journal of Computer Science & Information System*, *9*(11), 45–56. https://doi.org/10.55640/ijcsis/Volume09Issue11-05

Rahman, A., Iqbal, A., Ahmed, E., & Ontor, M. R. H. (2024). PRIVACY-PRESERVING MACHINE LEARNING: TECHNIQUES, CHALLENGES, AND FUTURE DIRECTIONS IN SAFEGUARDING PERSONAL DATA MANAGEMENT. *International journal of business and management sciences*, *4*(12), 18-32.

Iqbal, A., Ahmed, E., Rahman, A., & Ontor, M. R. H. (2024). ENHANCING FRAUD DETECTION AND ANOMALY DETECTION IN RETAIL BANKING USING GENERATIVE AI AND MACHINE LEARNING MODELS. *The American Journal of Engineering and Technology*, *6*(11), 78-91.

Nguyen, Q. G., Nguyen, L. H., Hosen, M. M., Rasel, M., Shorna, J. F., Mia, M. S., & Khan, S. I. (2025). Enhancing Credit Risk Management with Machine Learning: A Comparative Study of Predictive Models for Credit Default Prediction. *The American Journal of Applied sciences*, *7*(01), 21-30.

Bhattacharjee, B., Mou, S. N., Hossain, M. S., Rahman, M. K., Hassan, M. M., Rahman, N., ... & Haque, M. S. U. (2024). MACHINE LEARNING FOR COST ESTIMATION AND FORECASTING IN BANKING: A COMPARATIVE ANALYSIS OF ALGORITHMS. *Frontline Marketing,Management and Economics Journal*, *4*(12), 66-83.

Hossain, S., Siddique, M. T., Hosen, M. M., Jamee, S. S., Akter, S., Akter, P., ... & Khan, M. S. (2025). Comparative Analysis of Sentiment Analysis Models for Consumer Feedback: Evaluating the Impact of Machine Learning and Deep Learning Approaches on Business Strategies. *Frontline Social Sciences and History Journal*, *5*(02), 18-29.

Nath, F., Chowdhury, M. O. S., & Rhaman, M. M. (2023). Navigating produced water sustainability in the oil and gas sector: A Critical review of reuse challenges, treatment technologies, and prospects ahead. *Water*, *15*(23), 4088.
Hossain, S., Siddique, M. T., Hosen, M. M., Jamee, S. S., Akter, S., Akter, P., ... & Khan, M. S. (2025). Comparative Analysis of Sentiment Analysis Models for Consumer Feedback: Evaluating the Impact of Machine Learning and Deep Learning Approaches on Business Strategies. *Frontline Social Sciences and History Journal*, *5*(02), 18-29.
Chowdhury, O. S., & Baksh, A. A. (2017). IMPACT OF OIL SPILLAGE ON AGRICULTURAL PRODUCTION. *Journal of Nature Science & Sustainable Technology*, *11*(2).

Nath, F., Asish, S., Debi, H. R., Chowdhury, M. O. S., Zamora, Z. J., & Muñoz, S. (2023, August). Predicting hydrocarbon production behavior in heterogeneous reservoir utilizing deep learning models.

In *Unconventional Resources Technology Conference, 13–15 June 2023* (pp. 506-521). Unconventional Resources Technology Conference (URTeC).

Ahmmed, M. J., Rahman, M. M., Das, A. C., Das, P., Pervin, T., Afrin, S., ... & Rahman, N. (2024). COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR BANKING FRAUD DETECTION: A STUDY ON PERFORMANCE, PRECISION, AND REAL-TIME APPLICATION. *American Research Index Library*, 31-44.

Shakil, F., Afrin, S., Al Mamun, A., Alam, M. K., Hasan, M. T., Vansiya, J., & Chandi, A. (2025). HYBRID MULTI-MODAL DETECTION FRAMEWORK FOR ADVANCED PERSISTENT THREATS IN CORPORATE NETWORKS USING MACHINE LEARNING AND DEEP LEARNING. *American Research Index Library*, 6-20.

Rishad, S. S. I., Shakil, F., Tisha, S. A., Afrin, S., Hassan, M. M., Choudhury, M. Z. M. E., & Rahman, N. (2025). LEVERAGING AI AND MACHINE LEARNING FOR PREDICTING, DETECTING, AND MITIGATING CYBERSECURITY THREATS: A COMPARATIVE STUDY OF ADVANCED MODELS. *American Research Index Library*, 6-25.

Das, A. C., Rishad, S. S. I., Akter, P., Tisha, S. A., Afrin, S., Shakil, F., ... & Rahman, M. M. (2024). ENHANCING BLOCKCHAIN SECURITY WITH MACHINE LEARNING: A COMPREHENSIVE STUDY OF ALGORITHMS AND APPLICATIONS. *The American Journal of Engineering and Technology*, *6*(12), 150-162.

Al-Imran, M., Ayon, E. H., Islam, M. R., Mahmud, F., Akter, S., Alam, M. K., ... & Aziz, M. M. (2024). TRANSFORMING BANKING SECURITY: THE ROLE OF DEEP LEARNING IN FRAUD DETECTION SYSTEMS. *The American Journal of Engineering and Technology*, *6*(11), 20-32.

Akhi, S. S., Shakil, F., Dey, S. K., Tusher, M. I., Kamruzzaman, F., Jamee, S. S., ... & Rahman, N. (2025). Enhancing Banking Cybersecurity: An Ensemble-Based Predictive Machine Learning Approach. *The American Journal of Engineering and Technology*, *7*(03), 88-97.

Pabel, M. A. H., Bhattacharjee, B., Dey, S. K., Jamee, S. S., Obaid, M. O., Mia, M. S., ... & Sharif, M. K. (2025). BUSINESS ANALYTICS FOR CUSTOMER SEGMENTATION: A COMPARATIVE STUDY OF MACHINE LEARNING ALGORITHMS IN PERSONALIZED BANKING SERVICES. *American Research Index Library*, 1-13.

Siddique, M. T., Jamee, S. S., Sajal, A., Mou, S. N., Mahin, M. R. H., Obaid, M. O., ... & Hasan, M. (2025). Enhancing Automated Trading with Sentiment Analysis: Leveraging Large Language Models for Stock Market Predictions. *The American Journal of Engineering and Technology*, *7*(03), 185-195.