A Improving Ad Click Fraud Detection Through Machine Learning and Deep Learning Models

Mrs. S.S. Raja Kumari[1], K. Veerendra Kumar[2], Golla Veeresh[3], Kandlagari Santhosh Reddy[4], Kuruva Siva[5]
[1,2,3,4,5]*Dept. Of Computer Science and Engineering, St. Johns College of Engineering and Technology, Yemmiganur, 518301, India*

***Abstract*— Due to the swift development of the mobile advertising market, the cases of fraudulent clicks of advertisements have grown considerably, causing considerable financial expenses to advertisers. This work provides a comparative research on different machine learning (ML) and deep learning (DL) models to identify ad click fraud. The suggested solution would combine classical machine learning (Logistic Regression, Random Forest, and XGBoost) and deep learning (Convolutional Neural Networks, CNN, Long Ssshort-Term Memory, and Gated Recurrent Units, respectively) in a single solution. Such models are chosen on ground of their ability to differentiate legit and fraudulent ad-click. In order to further boost the performance of the detection, Stacking Classifier is used to utilize the positive aspects of several models. The implementation of the system is based on Flask to facilitate fraud detection in mobile advertising campaigns and offer an easy way of tracking and minimizing the losses. The results of the experiments also prove that the Maximum accuracy of 92 was achieved by the Random Forest, and the deep learning models including CNN and LSTM demonstrated competitive results of 90 and 91, respectively. The Stacking Classifier was found to be more effective with a balanced precision-recall score of 0.92, which shows that the classifier gives good results in fraudulent clicks. The proposed system will contribute to increasing the validity of mobile advertising platforms and minimizing the financial loss caused by ad click fraud recognition.**

Keywords: Ad Click Fraud, Machine Learning, Deep Learning, Fraud Detection, Stacking Classifier, Random Forest, XGBoost, Logistic Regression, CNN, LSTM.

I. INTRODUCTION

The accelerated growth of digital advertising (and mobile advertising in particular) has dramatically enhanced the rate of fraudulent ad clicks and that is why, click fraud becomes one of the most acute concerns of the online advertisement environment. Ad click fraud laws not only cause advertisers to lose a significant amount of money but also manipulates important performance indicators, which negatively affects the success of advertising campaigns. Such fraud is usually characterized by artificial increase in the number of clicks with the help of automated bots or malevolent users who do not have any real interest in the advertised material and this leads to a decrease in the return on investment (ROI) to organizations.

In a bid to solve this problem, this paper aims at assessing the effectiveness of intelligent methods of fraud detection based on various performance measures such as accuracy, precision, recall, F1-score and the area under the ROC curve (AUC). These indicators of evaluation will ensure a holistic evaluation of the effectiveness of the models in terms of correctly identifying a legitimate and fraudulent ad click. The proposed solution will make the existing fraud detection processes more reliable and efficient, which will help advertisers to safeguard their advertising budgets and gain more benefits out of their campaigns.

The current project suggests a powerful ad click detection system, which utilizes machine learning and deep learning to meet the overall objectives. The system uses both traditional machine learning algorithms and deep learning architectures namely Logistic Regression, Random Forest, XGBoost, Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) in order to serve as an effective classifier of ad clicks as to whether it is a genuine or a fraudulent click. To further enhance predictive performance, a Stacking Classifier is applied which combines the advantages of two or more models in one decision making model.

The system is built in such a way that it can handle the huge amount of ad click data and derive meaningful insights out of the characteristics of IP address, gadget type, operating system version, and timestamps of ad clicks. The suggested solution allows identifying the presence of fraudulent actions quite accurately, and helps advertisers to optimize advertising spending and preserve the integrity of the digital advertising system. Altogether, the given work is dedicated to the increased need to have secure, scaled, and intelligent systems of fraud detection in a changing digital advertising landscape. The merger of machine learning and deep learning technologies is an important step towards ad click fraud fight and leads to making online marketing systems, both trustworthy and transparent.

II. RELATED WORK

Fraud detection in ad clicks has been identified as a serious issue in the domain of digital advertisement due to the fast growth of mobile advertisement and the advancement of fraud-related crime rate. As an illustration, the ML models that have been deployed extensively owing to their simplicity and success in dealing with large data have been the Random Forest, Logistic Regression, and XGBoost models. These algorithms can be used to categorize ad clicks as valid or fraudulent and are based on different characteristics, including IP addresses, the type of the device, and timings [1][2] [3]. The traditional ML models, however, sometimes do not work with high dimensional and complex data, which is the case with deep learning models.

The convolutional neural networks, Long short-term memory and Gated recurrent units are deep learning models that will be more efficient in detecting more complex patterns in ad clicks. The models are particularly useful in as far as their ability to learn hierarchical properties and long term dependencies in sequential data is concerned. [4] [5]. Through the force of such models it is possible to detect the fraudulent clicks with a greater precision so the financial losses suffered by advertisers are minimized. Moreover, hybrid solutions of ML and DL techniques have demonstrated substantial increase in the predictive quality. [6] [7]. Transau et al. (2013) can be used as the example of stacking classifiers that use the predictions of numerous base models and modify the total detection performance by taking advantage of the strengths of other algorithms.

This problem of skewed data which is a frequent problem in fraud detection has been solved by high quality methods such as K-SMOTEENN that integrates over-sampling and under-sampling to normalize the data prior to the model training [8]. Besides, federated learning has been introduced to the fraud detection systems to improve privacy and also enable the models to be trained on decentralized data without the need of transmitting sensitive samples [9][10]. Another recent area of knowledge examines the implementation of the reinforcement learning and optimization algorithms to enhance the flexibility and effectiveness of the fraud detection systems [11] [12]. To sum up, the combination of ML and DL with the new methods of detection, i.e. stacking classifiers, federated learning, offers a powerful framework to ad click fraud detection. Such techniques will be able to enormously increase the accuracy of detection, will decrease the false positives as well as will provide scalable solutions to the continuously changing world of the digital advertising market [13] [14] [15].

III. PROPOSED METHODOLOGY

The proposed system will identify ad click frauds with the help of machine learning (ML) and deep learning (DL). The approach has three significant stages as the data collection, data preprocessing and model development and evaluation.

A. Data Collection and Preprocessing

The system captures the ad click statistics of advertisement sources that are available. The data consists of the following attributes; IP address, application ID, device type, operating system version, channel identifier, and click timestamp and attribution time. These characteristics are necessary to study the user interaction patterns and detect abnormal click behavior which is related to fraudulent activities. The target variable would show the user that would either install the application after clicking on an advertisement which is one of the primary variables that are used in fraud detection.

B. Data Preprocessing

Raw ad click data usually have missing values, inconsistencies, and noise. To overcome these challenges, data preprocessing is used to deal with the missing values, encode categorical variables and to normalize numerical values. The temporal features e.g., timestamps when clicking a button are extracted into meaningful elements (e.g. hour of the day or day of the week) to extract time behavior patterns. Categorical variables, such as device type and operating system version, are coded into one of the numerical versions that can be used to train a model. These preprocessing stages provide data consistency, better quality features and efficient model learning.

C. Model Development and Evaluation

The dataset which has been preprocessed is separated into training and testing sets to test the generalization ability of the proposed forms. Seconds sampling is used to maintain the class distribution although this is especially needed in a fraud detection case where the instances of fraud are normally underrepresented.

The training phase is carried out between the conventional machine learning and deep learning methods and these include Logistic Regression, Random Forest, XGBoost, Convolutional Neural Networks (CNN) which is also known as the Long Short-Term Memory (LSTM). The models have been focused at the linear and non-linear ad click behavior patterns. Hyperparameter optimization techniques which help to tune the learning parameters to give the best results also contribute to model performance. The stacking approach is used to integrate the outputs of many models taking advantage of their complementary benefits to enhance the overall detection.

Evaluation of the model is done using typical performance assessment criteria (accuracy, precision, recall, F1-score, area under the receiver operating characteristic) (ROC-AUC). These metrics present an overall evaluation of the models in terms of the capacity to assign frauding as accurate and reduce a false positive. Comparison is done to choose the best model to be deployed.

D. Prediction Module

After being trained and evaluated the chosen model then classifies incoming ad click data. The system takes the input features of the IP address, application ID, device type, operating system version, channel identifier and click time. Following these inputs, the model estimates the legitimacy and or fraudulentness of a certain ad click and provides the classifier with the outcome.

E. User Interaction Modules

Login Module:

The system has secured authentication credentials, which are accessible by registered users. The session management mechanisms provide restrictions to the access to the system functionalities.

Registration Module:

The users who are new can make an account by entering minimal details like name, email address, and password. On successful registration one is redirected to the log-in interface.

Dataset Upload Module:

This module provides the possibility to upload datasets to be used in training or testing. The system also verifies the format and structure of the file and then processes the data.

Model Performance Module:

Evaluation results and performance measures of the trained models, which may be the accuracy and other classification measures, are available to the users.

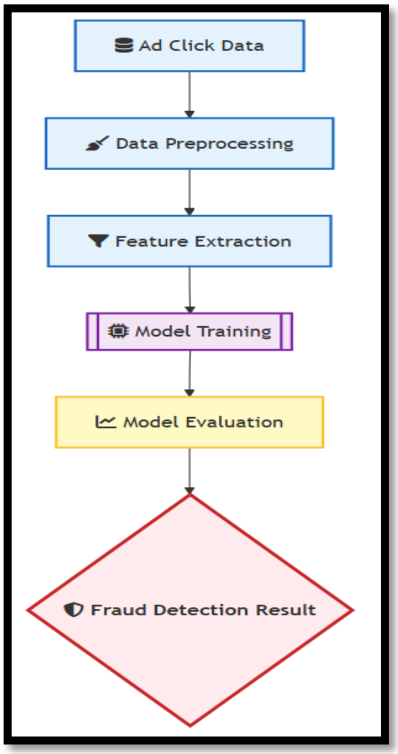

Figure 1 Proposed Methodology flow

IV. ARCHITECTURE DETAILS

Machine learning and deep learning techniques will also be applied in the given system to identify fraudulent clicks in mobile advertising. The system derives key attributes of ad click records; IP address, application identifier, the type of the device of which the web record belongs, version number of operating system, publisher channel identifier, and click timestamp and status of attribution is made in order to comprehend whether installing an application after clicking or not. Based on these features, all ad clicks would be termed as either quality or a fake advertisement.

One-followed ensemble has been used instead of ensemble-based one to obtain better prediction and higher power on various data. The system will employ different types of learning: the Decision Tree, Random Forest, LightGBM, and Stacking Classifier, Recurrent Neural Network, and Long Short-Term Memory the prediction of which will be added to create a more effective fraud identification.

Tree-based approach

A tree-based learning approach is applied, which makes a classification through the operation of the recursive partition of the dataset into subsets with the help of the most informative attributes. Any decision point consists of the feature based rule and terminal nodes are used to make predictions of classes. On the one hand, it is a simple and easy-to-understand method, but the depth can easily overfit simple, limiting its projection to unknown data on the other hand.

Ensemble learning method

To improve this, further, a procedure of learning in a group is adopted to induce stability in classification by integrating outcomes of a sequence of tree based predictors. This process influences predictive performance by preventing the bias wilderness of picking data sample at random and indicators that are ranked highly, in particular in high-dimensional data sets and this method decreases the variance and enhances predictive achievement. It is computationally more costly, but a more resistant approach to overfitting than multivariate predictors such as a single-tree approach.

Gradient-boosting technique

It also incorporates in the scheme a form of gradient-boosting scheme, in which weak learners are trained in an order, to specialize on the instances in which prediction error is greater. The technique is effective in the learning process particularly when handling large data volumes. Tuning is however a very critical parameter and should be tuned carefully so as to avoid overfitting especially with a small amount of data.

Mean strategy of meta-learning.

This is further enhanced by a stacking based ensemble mechanism with the aim of enhancing the performance of the classification. In this process a number of base models are themselves trained and the output of the models is then the input of a more significant meta-model that provides the final prediction. The hierarchical learning model enables the system to exploit the complementary nature of the different algorithms which in most instances would be more effective than the individual models, but demand more complexity of computation.

Sequence-based neural architecture.

A neural network structure that processes sequential data can be employed to analyses the data on sequential and time-dependent click behavior. This model maintains the memory within itself in order to have temporal dependencies and sequences of behavioral formulas at the nearby of the sequences of clicks. Even though effective in the short-term dependencies, these architectures would not work effectively in long term information storage, and therefore, improved memory-based extensions are advocated.

Memory enhanced Network of recurring type.

A better recurrence architecture that incorporates blocked memory schemes is introduced in an attempt to address the issue of long-term dependency. This design is such that it could selectively retain and eliminate information on long sequences and therefore is rather proficient at modeling temporal ad click sequence behavior. Even though this has a high learning power, much computational power and larger dataset is required in order to be effectively trained.

The overall system architecture consists of three major components. The frontend provides the user with easy to use and secure user interface and includes register and log-in functionality. After a person has successfully managed to authenticate, he/she is redirected onto a prediction interface on which one can key in attributes of click. All the inputs are forwarded to the backend that does data preprocessing, model training, evaluation and prediction. The resultant end classification is then displayed in the resultant interface in the form of whether the ad click is a fraud or not.

V. RESULTS AND DISCUSSION

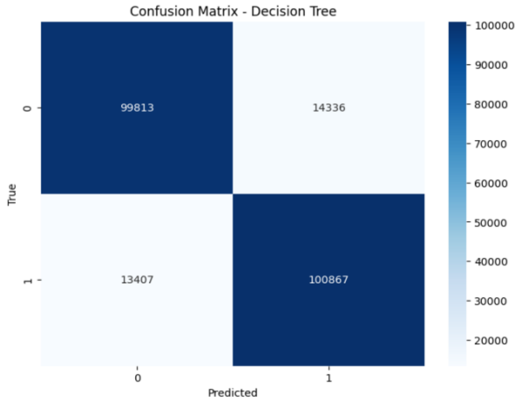

Figure 2 Decision Tree Confusion Matrix

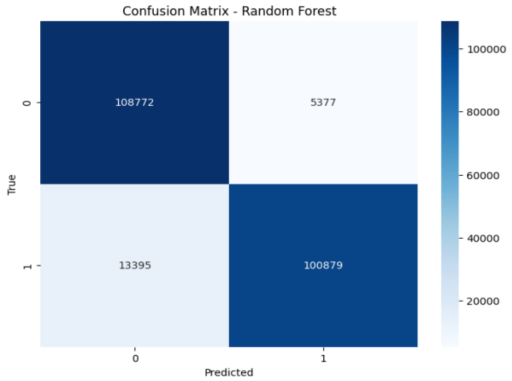

Figure 3 Random Forest Confusion Matrix

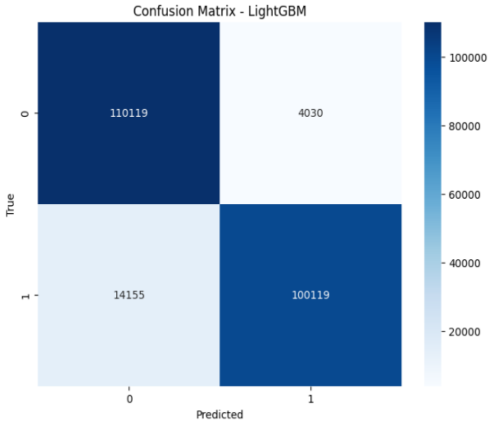

Figure 4 LightGBM Confusion Matrix

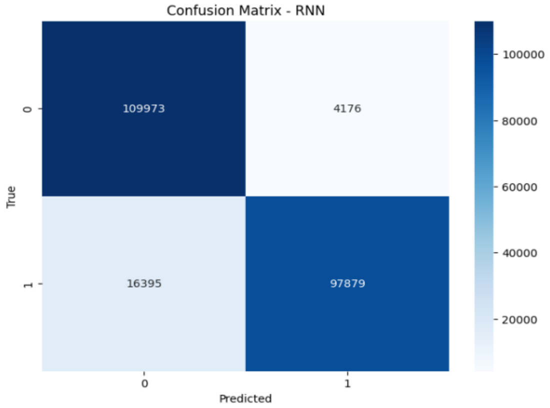

Figure 5 RNN Confusion Matrix

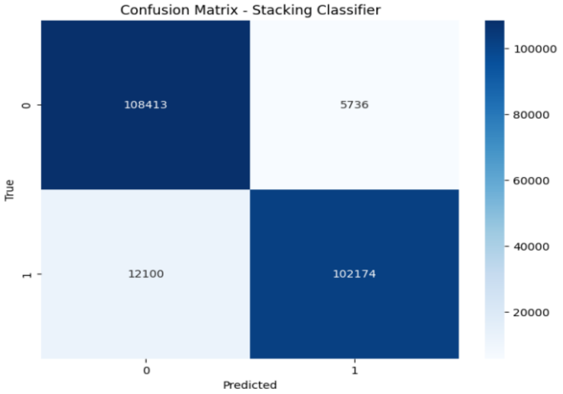

Figure 6 Stacking Classifier Confusion Matrix

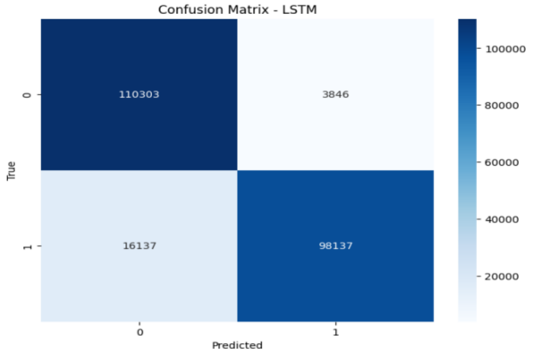

Figure 7 LSTM Confusion Matrix

In the detection of ad click fraud, the ad click fraud detection system displayed high classification using various machine and deep learning models that consisted of Decision Tree, Random Forest, LightGBM, Recurrent Neural Network (RNN), Long short term memory (LSTM), and a Stacking Classifier. The Decision Tree model generated a balanced classification, as indicated in Figure 2, accurately classifying most of the fraudulent and legitimate clicks, having high precision, recall, and F1-scores of both collections of classes. Figure 3 shows that the

Random Forest method, which increased the overall accuracy to 92, had better performance in reducing false positives and better recall of the two categories of clicks. In the same way the LightGBM model (Figure 4) scored the same level of accuracy hence indicating a specific level of strength in reducing the occurrence of misclassification of legitimate clicks. Figure 5 The RNN model (Figure 5) had a high accuracy of 91% and the performance of the Stacking Classifier (Figure 6) improved it to 92% accuracy balancing the high-precision and high-recall on both classes by using the ensemble prediction. Lastly, with respect to Figure 7 the LSTM model also attained 91 percent overall accuracy, displaying high recall and high precision of the two classes with a confusion matrix indicating equal F1-scores amongst the two classes. All these findings point towards the fact that ensemble and advanced sequence-based models are better than the more basic models and can capture complex spatial and sequential patterns in ad click behavior effectively, whereas mid-range models are also effective, but with minor variations, within the best-performing models.

VI. CONCLUSION

In the Ad Click Fraud Detection System created within the framework of this project, machine learning and deep learning methods are used. The system can differentiate legal and illegitimate ad clicks, at a high degree of precision, with the help of a complementary combination of traditional and advanced architectures such as tree-based architecture, ensemble architecture, sequence-based architecture, and other. The system is implemented on the Flask-based web interface, and it enables the advertisers plus the analysts to access the highly challenging task of fraud detection and enables them to validate inputs, predict the outcomes, and track the performance of ad campaigns effectively. The transparency, scalability, and cost-effectiveness of its design will offer a powerful solution that minimizes the chances of fraudulent clicks and at the same time make it accurate and user-friendly.

VII. FUTURE SCOPE

There are a number of changes that can be made in subsequent versions to ensure the effectiveness, scalability and adaptation of the system. By including explainable AI (XAI) methods (SHAP and LIME, etc.), a user would have information on why certain ad clicks can be viewed as fraudulent, which would boost their trust and transparency. Adding automated information sharing with advertisement sites via API might simplify the process of detecting fraud and in-the-field notification. Further reinforcement of unsupervised methods of anomaly detection would allow identifying new patterns of fraud that were not recognized before. Also, adaptive learning would enable the system to be slowly fixed until it reaches maximum accuracy with the availability of new data. The usability can be improved by increasing multi-language support, and providing sophisticated analytics dashboards to the global audience. And lastly, the system should be implemented as a load-balanced and auto-scaling SaaS solution in the clouds, which would prepare it to be adopted by an enterprise scale. These upgrades would make the system resolute, dynamic, and pertinent in the changing world of digital advertising fraud.

REFERENCES

[1] R. A. Alzahrani, M. Aljabri, and R. A. Mustafa Mohammad, “Ad Click Fraud Detection Using Machine Learning and Deep Learning Algorithms,” *IEEE Access*, vol. 13, pp. 12746–12763, 2025, doi: 10.1109/ACCESS.2025.3532200.

[2] B. Kirkwood, M. Vanamala, and N. Seliya, “Click Fraud Detection of Online Advertising Using Machine Learning Algorithms,” *IEEE International Conference on Electro Information Technology*, pp. 586–590, 2024, doi: 10.1109/EIT60633.2024.10609899.

[3] D. Ma and F. Wan, “Research on Intelligent Recognition of Ad Click Fraud Based on Deep FM Heterogeneous Integration Model,” *ACCESS International Journal of High Speed Electronics and Systems*, vol. 12, 2025, doi: 10.1142/S0129156425407260.

[4] T. A. Khan, J. Tulsi, M. Alam, K. Kadir, K. M. Ali, and M. S. Mazliham, “Analysis and visualization of fraud detection patterns through data mining and classification using MLP and hybrid deep learning model,” *Egyptian Informatics Journal*, vol. 32, p. 100829, Dec. 2025, doi: 10.1016/J.EIJ.2025.100829.

[5] E. A. L. M. Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, “A systematic review of literature on credit card cyber fraud detection using machine and deep learning,” *PeerJ*

Comput. Sci., vol. 9, p. e1278, Apr. 2023, doi: 10.7717/PEERJ-CS.1278/TABLE-7.

[6] V. Chang, B. Ali, L. Golightly, M. A. Ganatra, and M. Mohamed, “Investigating Credit Card Payment Fraud with Detection Methods Using Advanced Machine Learning,” *Information 2024, Vol. 15,* vol. 15, no. 8, Aug. 2024, doi: 10.3390/INFO15080478.

[7] T. Albalawi and S. Dardouri, “Enhancing credit card fraud detection using traditional and deep learning models with class imbalance mitigation,” *Front. Artif. Intell.*, vol. 8, p. 1643292, Oct. 2025, doi: 10.3389/FRAI.2025.1643292/BIBTEX.

[8] A. A. Al-Maari, M. Abdulnabi, Y. Nathan, A. Ali, U. Ali, and M. Khan, “Optimized Credit Card Fraud Detection Leveraging Ensemble Machine Learning Methods,” *Engineering, Technology & Applied Science Research*, vol. 15, no. 3, pp. 22287–22294, Jun. 2025, doi: 10.48084/ETASR.10287.

[9] A. Qayoom *et al.*, “A novel approach for credit card fraud transaction detection using deep reinforcement learning scheme,” *PeerJ Comput. Sci.*, vol. 10, p. e1998, Apr. 2024, doi: 10.7717/PEERJ-CS.1998/SUPP-1.

[10] M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, “Federated learning model for credit card fraud detection with data balancing techniques,” *Neural Computing and Applications 2024 36:11*, vol. 36, no. 11, pp. 6231–6256, Jan. 2024, doi: 10.1007/S00521-023-09410-2.

[11] T. Awosika, R. M. Shukla, and B. Pranggono, “Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection,” *IEEE Access*, vol. 12, pp. 64551–64560, 2024, doi: 10.1109/ACCESS.2024.3394528.

[12] Y. Wu, L. Wang, H. Li, and J. Liu, “A Deep Learning Method of Credit Card Fraud Detection Based on Continuous-Coupled Neural Networks,” *Mathematics 2025, Vol. 13,* vol. 13, no. 5, Feb. 2025, doi: 10.3390/MATH13050819.

[13] N. Damanik and C. M. Liu, “Advanced Fraud Detection: Leveraging K-SMOTEENN and Stacking Ensemble to Tackle Data Imbalance and Extract Insights,” *IEEE Access*, vol. 13, pp. 10356–10370, 2025, doi: 10.1109/ACCESS.2025.3528079.

[14] S. S. Sulaiman, I. Nadher, and S. M. Hameed, “Credit Card Fraud Detection Using Improved Deep Learning Models,” *Computers, Materials & Continua*, vol. 78, no. 1, pp. 1049–1069, Jan. 2024, doi: 10.32604/CMC.2023.046051.

[15] A. Sarker *et al.*, “Credit Card Fraud Detection Using Machine Learning Techniques,” *Journal of Computer and Communications*, vol. 12, no. 6, pp. 1–11, Jun. 2024, doi: 10.4236/JCC.2024.126001.