**IDENTIFICATION OF CREDIT CARD FRAUDS USING MACHINE LEARNING AND DEEP LEARNING**

**Aravind.M1, a)**, **CS Abhinay 2, b) DS Prathamesh3, c) K. Naveen Kumar 4, d) Sheetal Kundra 5, e)**

**1,2,3Student, Department of Artificial Intelligence and Data Science, GNIT Ibrahimpatnam, Ranga Reddy ,501506,**

**4Assistant Professor, Department of Artificial Intelligence and Data Science, GNIT, Ibrahimpatnam, Ranga Reddy ,501506**

**5Professor & HOD, Department of Artificial Intelligence and Data Science, GNIT, Ibrahimpatnam , Ranga Reddy ,501506,**

**Corresponding Authors:**

**a)l**[**Aravindm726@gmail.com**](mailto:Aravindm726@gmail.com),b)[**Abhinaycs01@gmail.com**](mailto:Abhinaycs01@gmail.com),c)[**ds.prathamesh03@gmail.com**](mailto:ds.prathamesh03@gmail.com),d)[**kommalapatin@gmail.com**](mailto:kommalapatin@gmail.com)

**ABSTRACT**

The rise in digital financial transactions has increased credit card fraud risks, demanding advanced detection methods. Traditional machine learning models struggle with imbalanced datasets and evolving fraud patterns, leading to high false positives and reduced accuracy. This research introduces a fraud detection framework combining deep learning with ensemble models like Gradient Boosting, Random Forest, and Logistic Regression. To tackle data imbalance, SMOTE and under-sampling are applied to enhance model performance. The system, developed using TensorFlow and Keras, employs a sequential deep learning model for fraud detection. Feature engineering techniques, such as temporal transaction analysis, further improve detection capabilities. Hyperparameter tuning optimizes performance and mitigates overfitting. This study also evaluates bidirectional Long Short-Term Memory (BiLSTM) and bidirectional Gated Recurrent Unit (BiGRU) models. The BiLSTM-MaxPooling-BiGRU-MaxPooling model outperforms traditional classifiers like Naive Bayes, AdaBoost, Logistic Regression, and Decision Tree. A deep autoencoder framework further enhances accuracy. Comparative analysis across multiple financial datasets confirms deep learning models' superiority. For real-time detection, the Deep Ensemble Algorithm framework (DEAL) is proposed to identify fraudulent transactions in streaming data. Stochastic Gradient Descent (SGD) is used for efficient parameter updates, reducing computation time. Given the need for rapid fraud detection, SGD enhances real-time capabilities. The proposed system achieves 99.59% accuracy, surpassing conventional methods. These findings highlight deep learning's potential in financial security applications, including banking, e-commerce, and insurance. By integrating deep learning with ensemble techniques, this research offers a scalable, effective fraud detection solution.

**Keywords:** Credit card fraud, fraud detection, deep learning, ensemble learning, Gradient Boosting, Random Forest, Logistic Regression, SMOTE, TensorFlow, Keras, BiLSTM, BiGRU, autoencoder, real-time detection, SGD, financial security.