**CREDIT CARD FRAUD DETECTION**

**TITLE OF THE PAPER:**

Credit Card Fraud Detection

**Authors:**

S. Varusha (210701304)

G. Udhaya Kumar (210701293)

**Abstract With Keywords:**

Credit card fraud is a significant issue in financial transactions, leading to financial losses for individuals and institutions worldwide. These models are crucial for minimizing these losses and maintaining trust in financial systems. In this project we collected the dataset then by preprocessing it and then trained machine learning models to classify transactions as fraudulent or not. These fraudulent activities helps the bank side in smooth and by the customer side. Our models were evaluated on the basis of accuracy, precision, and F1 score. The results show the fraudulent activities in real time data using the model prediction.

Keywords: Data preprocessing, Feature engineering, Classification, Performance evaluation.

**Introduction:**

Credit card fraud poses a significant threat to financial institutions and consumers. Detecting and preventing fraudulent transactions is very crucial and important for maintaining trust and security in the financial system. In this project, we explore a machine learning model to identify and eliminate credit card fraud, by undergoing various technologies and various procedures.in the fast-paced world credit cards have to be cut off and our goal is to develop a credit card fraud detection system capable of accurately determining fraudulent activities in the real time world.

**LITERATURE SURVEY:**

|  |  |  |
| --- | --- | --- |
| Advantages | Disadvantages | Outcomes |
| * Enhanced Accuracy: Suitable machine learning algorithm which can handle large data which in turns gives accuracy over the model. | * Class Imbalance: Datasets that are imbalanced cannot be predicted rightly and shows biassed output. | * Improved Detection Accuracy: More detailed research will help to find suitable algorithms and therefore the accuracy of detection is improved. |
| * Real-time Detection: Machine learning models can operate in real-time, which will detect and prevent fraudulent transactions.. | * Interpretability: Some deep learning models will be making it challenging to understand the contributing factors to fraud detection controls and decisions. | * Enhanced Efficiency: Machine learning algorithms give efficient fraud detection processes, allowing the bank side smoothing the process. |
| * Adaptability: Machine learning systems can adapt and evolve over time and by learning itself. | * Scalability: Building and deploying machine learning models for large industries or in real time detection is difficult as it needs government bases. | * Advanced Techniques: enabling machine learning and deep learning algorithms will help to create hybrid algorithms. |
| * Efficient Algorithms: Hybrid algorithms between machine and deep learning will give an efficient model. | * Deploying: Deploying the model which has low accuracy will collapse the entire banking process. | * Live Detection: The model developed will give an efficient record in the real time live detection. |

**RESEARCH GAPS:**

* Class Imbalance Mitigation

Even Though the advancements in the machine learning field is significant the proper predicting algorithms has to show increase in accuracies in the output.

* Explainable AI and Model Interpretability

The lack of interpretability in many machine learning models poses a bridge between the fraudulent activities. Future research should focus on developing the decision making part in the model..

* Transferability and Generalization

Machine learning models trained on one dataset may not be classified generally. Research is needed to investigate techniques for improving the generalising the domain activities.

* Incorporating Contextual Information

Current fraud detection models often rely completely on transactional data, neglecting valuable contextual information that could enhance fraud detection accuracy. Research gaps exist in the methods should include other determining activities to enhance the accuracy.

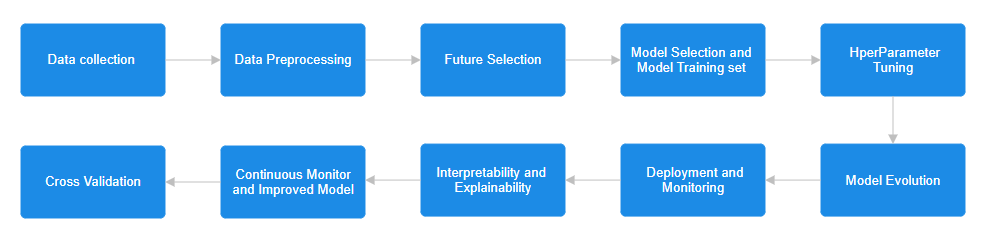
* Adversarial Attacks and Model Robustness

Adversarial attacks pose a threat to the maintenance of machine learning models for credit card fraud detection. Research gaps exist in developing maintainable models that are resistant to manipulations that are less susceptible to adversarial perturbations.

* Privacy-Preserving Techniques

Maintaining data privacy and confidentiality is crucial in credit card fraud detection, particularly with sensitive customer information. Research gaps exist in exploring privacy-preserving techniques, to enable collaborative model training without leaving the privacy of customer data.

**PROPOSED METHODOLOGY:**



**RESULT & DISCUSSION:**

**COMPARATIVE ANALYSIS:**

**CONCLUSION:**

**REFERENCES:**