# Literature Review

Credit card fraud detection has been an extensively researched area, particularly in the domain of machine learning due to its ability to identify patterns in large, complex datasets. Traditional rule-based systems, which rely on predefined thresholds and manual intervention, have proven inadequate in detecting evolving fraud patterns (Abdallah et al., 2016). Machine learning models, such as logistic regression, decision trees, random forests, and deep learning techniques, have demonstrated significant potential in improving fraud detection accuracy (Nguyen et al., 2020).

A key challenge in fraud detection is handling highly imbalanced datasets, where fraudulent transactions constitute only a small fraction of the data. Standard machine learning models tend to be biased towards the majority class, leading to poor fraud detection performance. Several techniques have been proposed to address this issue, including oversampling the minority class (e.g., SMOTE), undersampling the majority class, and using cost-sensitive learning methods (Wei et al., 2019). Ensemble methods, such as boosting and bagging, have also been applied to improve fraud detection by combining multiple weak classifiers into a stronger predictive model (Zareapoor & Shamsolmoali, 2015).

Feature engineering and feature selection play a crucial role in enhancing the accuracy and interpretability of fraud detection models. Researchers have explored domain-specific feature extraction methods, such as transaction frequency, spending patterns, and geolocation-based behaviors, to improve fraud identification (Dal Pozzolo et al., 2017). Automated feature selection techniques, including recursive feature elimination and mutual information-based approaches, have been used to optimize model performance while reducing computational complexity (Carcillo et al., 2021).

Recent advancements focus on hybrid models that integrate deep learning with traditional machine learning techniques, such as combining convolutional neural networks (CNNs) with recurrent neural networks (RNNs) to capture both spatial and temporal fraud patterns (Zhao et al., 2022). Additionally, explainable AI (XAI) methods are being explored to enhance model transparency, allowing financial institutions to better understand fraud detection decisions (Li et al., 2023).

While significant progress has been made, future research can explore adaptive models that dynamically adjust to new fraud patterns in real-time, as well as blockchain-based fraud detection frameworks to enhance transaction security.  
  
Implementation:

Most fraud detection models use static machine learning algorithms that require retraining periodically. Instead, **Reinforcement Learning (RL)** can adapt dynamically by learning from new fraudulent patterns in real-time.  
  
How to Implement?

Use a Deep Q-Network (DQN) or Proximal Policy Optimization (PPO) to train an agent that continuously updates its fraud detection strategy.

By Defining rewards based on transaction legitimacy, minimizing false positives and false negatives.

Implement online learning, where the model updates with each transaction instead of periodic retraining.

Benefits

Real-time fraud detection with adaptive learning.

Reduces manual retraining, saving computation time.

Handles evolving fraud tactics dynamically instead of relying on static historical patterns.