Hybrid Deep Learning and Rule-Based Approach for Real-Time Vulnerability Detection in Ethereum Smart Contracts

Shruti Manoj Chavan
M.Tech., Computer Engineering - Data Science, COEP Technological University, Pune, India

Dr. Vinod Pachghare
Project Guide, Department of Computer Science & Engineering, COEP Technological University, Pune, India

Abstract

Ethereum smart contracts underpin critical DeFi and enterprise workflows, but their immutability and financial exposure make them prime targets for exploitation. Vulnerabilities such as unchecked delegatecall usage, arithmetic overflows, reentrancy flaws, and timestamp dependence can lead to serious breaches if undetected before deployment. This research proposes a lightweight, real-time multi-class vulnerability detector that combines a CNN-BiLSTM network for semantic pattern learning with a Solidity-specific rule-based verification layer. The model is trained using custom tokenized Solidity code and leverages focal loss and oversampling techniques to handle class imbalance across four major vulnerability types. Unlike static analysis or binary classifiers, this hybrid system offers nuanced categorization and semantic validation using rules drawn from the Solidity Vulnerability Catalog (SWC). It outputs interpretable, class-specific justifications that aid developers during code audits. Evaluation on a dataset of ethereum smart contracts showed reducuction in false positives, particularly in lower-frequency classes like Dangerous Delegatecall and Timestamp Dependency. Thus, this solution advances the precision, interpretability, and usability of smart contract vulnerability detection tools, making it deployable for real-world blockchain development environments.