Roll: 22011DA802

Course: M. Tech [CFIS] { 2022-24 }

Particulars: Abstract and title proposal for Mini Project/Technical Seminar

Proposed Title:

- Blockchain Contract Fortification: Bytecode Analysis to Check for Smart Contract Vulnerabilities

Abstract: Smart contracts and blockchain platforms have revolutionized various industries, offering decentralized and transparent execution of agreements. However, they are not immune to security lapses, and the presence of vulnerabilities has led to security issues. This fieldwork will leverage bytecode analysis, focusing on security implications by using bytecode analysis along with EVM opcodes to determine the potential vulnerabilities in a smart contract. By delving into the low-level instructions of smart contracts, we intend to present a detailed analysis of the vulnerabilities detected and provide essential insights wherever required to improve smart contract. To accomplish this, we will explore the case study that uses smart contract as a decentralized approach to electoral integrity. The approach combines automated analysis through tools and manual examination for inspection of bytecode. Overall, the key focus is inclined to have a concise view of what and how the vulnerabilities in smart contract can be checked through bytecode analysis.

Keywords: *Smart Contracts, Blockchain, Bytecode Analysis, Vulnerability, EVM opcode.*