Notification No: 591/2025

Notification Date: 30-12-2025

Name: Mohd Azeem Faizi Noor

Name of the Supervisor: Prof Khurram Mustafa

Topic: Mitigating Endpoint Vulnerabilities in Blockchain Applications

Department / Faculty: Department of Computer Science, Faculty of Sciences, JMI

Key Findings

Endpoint compromise remains one of the most critical yet under-addressed threats in blockchain ecosystems, even when core blockchain protocols themselves are cryptographically secure. Although blockchain systems provide strong guarantees of integrity and immutability at the network and protocol layers, users' private keys and transaction execution processes remain highly vulnerable at the endpoint level.

A Systematic Literature Review (SLR) conducted in this study indicates that existing research predominantly emphasizes blockchain-layer security mechanisms such as consensus protocols, cryptographic primitives and smart contract verification. In contrast, endpoint security vulnerabilities (EPVs) are insufficiently explored and are often treated as secondary concerns. The SLR highlights a clear research gap due to insufficient solutions for securing blockchain interactions on compromised or untrusted user devices.

The study further examined endpoint breaches and quantified their financial impact. Through the SLR, 28 major endpoint breaches were identified and analysed, resulting in an estimated cryptocurrency loss of approximately USD 1.4 billion. Key contributing factors include the high monetary value of cryptocurrencies, user temptations and lures and the absence of standardized global regulatory frameworks.

Based on evidence gathered from the SLR and empirical investigation, this study developed a comprehensive taxonomy of endpoint security vulnerabilities in blockchain applications. The taxonomy categorizes EPVs into broken authentication, cryptographic failures, security misconfigurations, web-based vulnerabilities, and human vulnerabilities. Human-centric attacks, particularly phishing and social engineering combined with web-based malware,

emerge as the most prevalent and damaging threat vectors, frequently resulting in irreversible private key exposure and financial loss.

Experimental evaluation of the proposed integrated security approach combining blockchain technology with Remote Browser Isolation (RBI) through isolated execution environments confirms its effectiveness in mitigating endpoint-level threats. By executing decentralized application interactions and transaction signing within an isolated environment, the framework prevents direct access to private keys, browser memory, clipboard data and session credentials from compromised endpoints.

In addition to vulnerability identification and mitigation, the study proposes a set of security guidelines and operational protocols for secure blockchain usage. These guidelines emphasize isolation-first execution, strict separation of key management from user endpoints, controlled communication channels and minimal trust assumptions regarding local systems. The proposed protocols define secure procedures for transaction initiation, verification, and signing within isolated environments, ensuring confidentiality, integrity, and non-repudiation without requiring modifications to existing blockchain protocols.

Performance analysis indicates that the RBI-based framework introduces moderate latency overhead; however, the impact remains within acceptable limits for security-critical blockchain applications. The trade-off between enhanced endpoint security and system performance is therefore justified, particularly for financial, governance and enterprise blockchain use cases.

Conclusively, the study establishes that integrating SLR-driven insights, a structured EPV taxonomy and well-defined security guidelines and protocols into an endpoint-centric framework significantly strengthens the security of blockchain applications. The proposed approach addresses a critical gap in current research and offers a practical, deployable solution for mitigating endpoint-based threats in real-world blockchain environments.

Keywords: Blockchain, Cryptocurrency, Endpoints, Vulnerabilities, Taxonomy