Abstract

Ransomware attacks have become a major cybersecurity concern, resulting in data breaches, financial losses, and disruptions to operations. This project introduces a Blockchain-Powered Ransomware Protection System that leverages the decentralized and unchangeable nature of blockchain to prevent unauthorized file encryption and detect malicious activities in real time. The system maintains data integrity by creating a SHA-256 hash of file contents and recording it on a private blockchain along with a timestamp. Any attempt to encrypt or alter the file is identified by comparing the current hash with the stored hash, allowing for early detection of ransomware activity. The project employs a Proof of Authority (PoA) consensus mechanism to enable quicker validation with a select group of trusted validators. Each organization can set up its own validators to retain independent control while still participating in the shared blockchain framework. The blockchain is developed from the ground up using Java for core logic and Go for the peer-to-peer (P2P) network, which supports efficient block propagation via WebSockets. Furthermore, the integration of the Inter Planetary File System (IPFS) provides secure decentralized storage, minimizing dependence on centralized data repositories. This architecture not only offers strong protection against ransomware but also improves transparency, auditability, and data resilience. The system aims to create an open, scalable platform for organizations to safeguard critical digital assets against evolving cyber threats.