ABSTRACT

Electronic Medical Records (EMRs) store critical information about patient conditions and require strong protection against risks of manipulation or unauthorized alterations (tampering). This study aims to design and evaluate a private blockchain–based storage system for medical records, focusing on enhancing data integrity and authenticity. The system was developed using a combination of the SHA-256 hashing algorithm, ECDSA digital signatures, and AES encryption, with a Proof of Authority (PoA) consensus mechanism for block validation.

The system design includes role-based user authentication, explicit patient authorization, transaction validation, block formation, as well as synchronization and conflict resolution among nodes. Testing was conducted on a limited-scale prototype by simulating various forms of tampering, including modifications of hash, prev_hash, signature, and transaction content.

The results indicate that the system can detect and reject any manipulation attempts at both data and block levels. Patient authorization proved effective in ensuring that medical records cannot be published without the owner's consent, while the validator mechanism maintained blockchain consistency. Therefore, this study demonstrates that implementing a private blockchain can strengthen protection against tampering and preserve the integrity of electronic medical records, although scalability, interoperability, and large-scale network performance remain areas for further development.

Keywords: Private Blockchain, Tampering, Data Integrity, Digital Signature, Hashing