SmartConSecurity: An SQLite RDBMS with Blockchain Technology Using SHA-256 Hashing Algorithm with a Salting Process

John Anthony E. Torrejas
Department of Computer, Information Sciences, and Mathematics, University of San Carlos, Cebu City, Philippines

Dr. Godwin S. Monserate
Department of Computer, Information Sciences, and Mathematics, University of San Carlos, Cebu City, Philippines

Abstract

Data transparency and integrity remain critical challenges in centralized institutions, where clients often lack visibility into how their data is safeguarded against tampering. To address these challenges, this study presents SmartConSecurity, a framework that combines salted SHA-256 (Secure Hash Algorithm 256-bit) hashing, AES-256-CTR (Advanced Encryption Standard, 256-bit key, in Counter mode) encryption, and blockchain storage to provide verifiable data integrity and transparency. A session-based salting mechanism ensures that even identical files generate unique hashes and ciphertexts, preventing duplication and strengthening tamper resistance. A lightweight web application integrated with MetaMask facilitates BSC (Binance Smart Chain) blockchain interaction, while a watchdog module continuously monitors files in real time to detect unauthorized modifications. To ensure confidentiality, the salted hash also serves as the AES-256- CTR encryption key, with the corresponding nonce stored on-chain for secure verification. Cryptographic validation confirms robustness: salted hashing produced an average 48.2% bit difference (Hamming distance), randomness tests met NIST (National Institute of Standards and Technology) standards, and collision probability remained negligible ($<10^{-54}$ for 10^{12} records). Performance evaluation showed that SmartConSecurity handles files up to 100 MB, maintaining end-to-end encryption and decryption within practical time bounds. These results demonstrate that SmartConSecurity provides a practical, scalable approach for transforming institutional data management from a trust-based to a verifiable model.

Keywords

AES-256 encryption (ctr mode), blockchain technology, data integrity, sha-256 hashing algorithm, verifiable database.