ABSTRACT

Data security and integrity are crucial aspects in the digital technology era, especially in digital certificate management. This study develops a digital certificate application using blockchain technology, integrating digital signatures and the Keccak256 hash algorithm to enhance security and integrity. The development method employs a Rapid Application Development (RAD) approach, encompassing three stages: Requirement Planning, Design Workshop, and Implementation. Tests on digital certificates ensure resilience against various modifications such as compression, data alteration, image addition, and rotation, demonstrating that the system can detect even the smallest changes. The average time to generate a signature decreased from 3.23 seconds without blockchain to 2.11 seconds with blockchain, and signature validation time decreased from 2.11 seconds to 0.22 seconds with blockchain. These results indicate a significant improvement in speed and efficiency. The application effectively enhances digital certificate security by ensuring that any change to the digital certificate affects the signature, thus maintaining its integrity. Future research is recommended to evaluate the performance of various hash algorithms in the context of blockchain.

Keywords: Blockchain, Digital Certificate, Digital Signature, Keccak256 Hash