IMPLEMENTASI AUTENTIKASI DUAL WALLET MENGGUNAKAN SMART CONTRACT UNTUK TWO-FACTOR AUTHENTICATION

Oleh

Chiko Gita Satria, NIM 2215101053

Program Studi Ilmu Komputer

Jurusan Teknik Informatika

ABSTRAK

Keamanan autentikasi digital menjadi semakin penting seiring meningkatnya serangan siber. Metode Two-Factor Authentication (2FA) konvensional yang mengandalkan One-Time Password (OTP) masih rentan terhadap serangan phishing, SIM swapping, dan man-in-the-middle, serta bergantung pada sistem terpusat. Penelitian ini mengusulkan sistem 2FA terdesentralisasi berbasis blockchain Ethereum dengan mekanisme autentikasi dual wallet menggunakan smart contract. Autentikasi dilakukan melalui verifikasi tanda tangan kriptografis dari dua wallet Ethereum yang terdaftar tanpa melibatkan OTP. Sistem diimplementasikan menggunakan smart contract Solidity pada Ethereum Testnet Sepolia dan diintegrasikan dengan backend Node.js serta frontend React melalui Web3.js. Hasil pengujian menunjukkan bahwa sistem yang diusulkan mampu meningkatkan keamanan autentikasi dan ketahanan terhadap serangan umum pada sistem 2FA tradisional.

Kata Kunci: Two-Factor Authentication, Blockchain, Smart Contract, Dual Wallet, Keamanan Digital

IMPLEMENTING DUAL WALLET AUTHENTICATION USING SMART CONTRACTS FOR TWO-FACTOR AUTHENTICATION

By

Chiko Gita Satria, ***Student ID 2215101053***

Computer Science Program

Department of Informatics Engineering

ABSTRACT

Digital authentication security has become increasingly critical as cyberattacks evolve. Conventional Two-Factor Authentication (2FA) methods based on One-Time Passwords (OTP) remain vulnerable to phishing, SIM swapping, and man-in-the-middle attacks, while relying on centralized infrastructures. This study proposes a decentralized 2FA system based on the Ethereum blockchain using a dual wallet authentication mechanism implemented through smart contracts. Authentication is performed by verifying cryptographic signatures from two registered Ethereum wallets without the use of OTPs. The system is implemented using Solidity smart contracts deployed on the Ethereum Sepolia Testnet and integrated with a Node.js backend and a React frontend via Web3.js. The results indicate that the proposed system provides stronger security and improved resistance to common attack vectors compared to traditional 2FA systems.

Keywords: Two-Factor Authentication, Blockchain, Smart Contract, Dual Wallet Authentication, Digital Security