ABSTRAK

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pemilihan umum elektronik berbasis *Public Key Infrastructure* (PKI) yang sesuai dengan alur kerja Kelompok Penyelenggara Pemungutan Suara (KPPS) di Indonesia. Sistem dibangun dengan arsitektur tiga server terpisah, yaitu server autentikasi, voting, dan tabulasi, menggunakan Java socket server sebagai *backend* dan Flask sebagai antarmuka pengguna. Untuk menjamin keamanan dan integritas data suara, digunakan algoritma kriptografi RSA dan SHA-256 serta mekanisme tanda tangan digital. Penelitian ini menerapkan prinsip *zero-knowledge* dengan menyimpan kunci privat secara lokal oleh pemilih dan kunci publik pada server. Hasil pengujian menunjukkan bahwa sistem mampu menjalankan seluruh fungsi dengan baik, mulai dari registrasi pemilih, verifikasi kunci, pemungutan suara, hingga tabulasi hasil secara otomatis dan terenkripsi. Sistem ini terbukti memenuhi aspek kerahasiaan, autentikasi, integritas, dan non-repudiasi, sehingga dapat dijadikan sebagai solusi awal dalam penerapan *e-voting* yang aman dan efisien di Indonesia.

Kata Kunci: *e-voting*, *Public Key Infrastructure*, RSA, SHA-256, keamanan data, Java socket.

ABSTRACT

This study aims to design and implement an electronic voting system based on Public Key Infrastructure (PKI) that aligns with the workflow of the Voting Organizing Group (KPPS) in Indonesia. The system is built using a three-server architecture consisting of authentication, voting, and tabulation servers, with a Java socket server as the backend and Flask as the user interface. To ensure the security and integrity of voting data, the system employs RSA and SHA-256 cryptographic algorithms along with a digital signature mechanism. The study adopts a zero-knowledge principle by storing private keys locally on the voter's device and public keys on the server. Testing results demonstrate that the system successfully performs all essential functions, including voter registration, key verification, vote casting, and encrypted automatic tabulation. The system has been proven to fulfill the key security principles of confidentiality, authentication, integrity, and non-repudiation, making it a viable preliminary solution for secure and efficient e-voting implementation in Indonesia.

Keywords: e-voting, Public Key Infrastructure, RSA, SHA-256, data security, Java socket.