ABSTRAK

Pemungutan suara elektronik adalah teknik pemungutan suara di mana suara direkam atau dihitung menggunakan peralatan elektronik. Sistem pemilihan sering menghadapi tantangan serius terkait keamanan dan kepercayaan. Ancaman seperti pemalsuan suara dan kurangnya transparansi dalam penghitungan suara telah menggoyahkan integritas pemilihan di berbagai negara. Untuk mengatasi masalah ini, penggunaan teknologi blockchain dalam e-voting telah diusulkan sebagai solusi menarik. Beberapa studi menggunakan blockchain untuk keamanan sistem pemungutan suara elektronik, seperti penelitian oleh Wu & Yang [1]. Dalam penelitian ini, terdapat kelemahan dalam memverifikasi pengirim. Kelemahan ini membuat potensi impersonation attack dan man in the middle attack terhadap pengirim menjadi mungkin. Penelitian ini mengusulkan skema baru untuk memperkuat sistem e-voting berbasis blockchain, skema yang diusulkan menggunakan The Goldreich-Goldwasser-Halevi (GGH) signature scheme. Tanda tangan yang dihasilkan menggunakan Goldreich-Goldwasser-Halevi (GGH) dapat memperkuat identitas pengirim pesan sehingga musuh tidak dapat meniru seseorang. Pada penelitian ini tetap menggunakan kunci public dari voter dan hanya menggunakan anonymous ID yang kemudian digunakan oleh pemilih dapat menjaga anonimitas dari voter. Sedangkan pada penelitian Wu & Yang memberikan sepasang kunci baru yang dihasilkan dan digunakan oleh pemilih untuk menjaga anonimitas dari pemilih. Berdasarkan hasil percobaan dapat disimpulkan bahwa skema yang diusulkan lebih kuat dari skema sebelumnya karena probabilitas sukses untuk meniru pengirim dengan skema yang diusulkan menggunakan impersonation attack dan man in the middle attack lebih kecil daripada skema Wu & Yang.

Kata Kunci: Impersonation Attack, Man-in-the-middle Attack, Goldreich-Goldwasser-Halevi (GGH) Signature scheme, Anonymous ID, Voter Anonymity.