ABSTRAK

Keamanan menjadi aspek yang sangat penting untuk mengamankan pertukaran data dan meyakinkan bahwa data diterima oleh pengguna yang sah. Beberapa aspek yang harus terpenuhi selama pertukaran informasi adalah otentikasi, kerahasiaan dan integritas. Pada sistem pemilihan elektronik, autentikasi digunakan untuk meyakinkan bahwa pemilih merupakan pemilih yang sah tanpa mengetahui identitasnya, sementara itu pengumpul suara pemilihan memverifikasi bahwa data yang diterima dari pemilih yang sah tanpa menge- tahui identitas pemilih. Sebuah skema otentikasi yang memenuhi persyaratan tersebut adalah skema otentikasi yang dapat disangkal. Otentikasi yang dapat disangkal sebagai otentikasi lanjutan di mana penerima dapat membuktikan sumber pesan dan penerima tidak dapat membuktikan sumber pesan kepada pihak lain. Pada tahun 2013, Li-Takagi et al. [15] mengusulkan skema otentikasi yang dapat disangkal. Kebocoran pada skema Li-Takagi yaitu penerima dapat membuktikan sumber pesan yang diberikan kepada pihak ketiga ketika penerima bekerja sama sepenuhnya dengan pihak ketiga, seperti yang dije- laskan oleh Mashid et al. [20]. Dalam metode yang diusulkan, *zero knowledge proof* diperke- nalkan untuk menjaga anonimitas skema otentikasi yang dapat disangkal ketika penerima sepenuhnya bekerja sama dengan pihak ketiga. Dalam hal ini, pengirim dan penerima menghasilkan bilangan acak yang digunakan untuk membuat kunci rahasia bersama untuk otentikasi bersama. Integritas pesan digunakan untuk memastikan keaslian pesan. Jika penerima meneruskan pesan ke pihak ketiga, pihak ketiga hanya mengetahui penerima sebagai sumber pengirim pesan. Berdasarkan analisis, skema yang diusulkan memenuhi persyaratan skema otentikasi yang dapat ditolak ketika penerima bekerja sama sepenuhnya dengan pihak ketiga. Namun, skema yang diusulkan memiliki biaya komputasi tambahan untuk mengamankan kunci rahasia bersama. Dua skema serangan yang dilakukan pada Li-Takagi dan skema yang diusulkan adalah serangan MITM dan serangan peniruan iden- titas. Probabilitas untuk memecahkan skema yang diusulkan menggunakan MITM attack lebih rendah daripada saat menggunakan skema Li-Takagi, tetapi kemungkinan memc- ahkan skema yang diusulkan menggunakan impersonation attack sama dengan skema Li- Takagi.

Kata kunci: Deniable authentication, fully cooperated, electronic voting system, MITM attack, Impersonation attack.