Abstrak

Authentikasi pengguna adalah suatu metode untuk mengauthentikasi pengguna yang dilakukan oleh pihak lain yang berkomunikasi dengan pengguna. Authentikasi biasanya dapat dilakukan dengan menggunakan verifikasi username, password, dan biometrik pengguna. Pada studi Seung .et.al., authentikasi pengguna dilakukan dengan menggunakan biometrik (sidik jari) dan password. Akan tetapi, authentikasi selesai dilakukan dengan mengirimkan biometric dan password yang telah dienkripsi. Selanjutnya pengguna dapat memindai sidik jari dan password dengan menggunakan perangkat authentikasi palsu karena pada metode tersebut tidak ada authentikasi yang diterapkan untuk melakukan authentikasi perangkat. Metode yang diajukan untuk mengatasi masalah tersebut menggunakan elliptic curve dan fungsi hash keccak. *Elliptic curve* digunakan untuk melakukan authentikasi perangkat sehingga pengguna dapat membuktikan bahwa perangkat yang digunakan adalah perangkat sah sedangkan fungsi hash keccak digunakan untuk melakukan authentikasi pengguna. Berdasarkan percobaan, waktu proses authentikasi mengalami penurunan menjadi 35.06 ms - 41.6 ms dibandingkan dengan metode yang diajukan oleh Seung .et.al., sedangkan kemungkinan untuk mendapatkan fingerprint dan password menggunakan metode yang diajukan lebih kecil kemungkinannya dari pada metode sebelumnya yaitu 2^{-57}. Selanjutnya, metode yang diajukan dapat mencegah dari perangkat palsu dalam pencurian informasi biometrik dan password.

Keywords: Authentikasi, *Elliptic Curve*, *Keccak Hash Function.*