Abstrak

Kartu Tanda Penduduk (KTP) merupakan hal yang sangat penting bagi masyarakat Indonesia. KTP memuat informasi pribadi, seperti Nomor Induk Kependudukan (NIK), Nama, Alamat, Jenis Kelamin, dll. Karena KTP memiliki data penting dan masih dicetak secara konvensional, maka rawan terhadap pencurian data jika KTP hilang. Jika KTP ditemukan oleh orang yang tidak bertanggung jawab, maka data dari pemilik KTP dapat digunakan orang tersebut untuk menyamar sebagai pemiliknya. Dalam metode sebelumnya yang dikemukakan oleh Haque et al., [1], data disimpan dalam Kode QR. Namun, tidak ada metode verifikasi untuk melegitimasi pemilik aslinya, dan sistem tidak memiliki fitur login. Untuk mengatasi kelemahan Haque et al., metode[1], NIK pemilik dienkripsi menggunakan Elliptic Curve El-Gamal (ECEG) dan selanjutnya ditandatangani menggunakan ECDSA oleh pemilik sebelum disimpan dalam QR Code. Untuk mendapatkan data pemilik di database, proses verifikasi harus dilakukan setelah QR Code dipindai. Dengan menggunakan metode yang diusulkan, probabilitas keberhasilan serangan tebakan adalah 1 / (*n* - 1). Sedangkan probabilitas keberhasilan serangan peniruan identitas adalah 1 / (*q1 * q2 * l*).

Kata kunci: qr code, kartu identitas, KTP, ECDSA, elliptic curve el-gamal