ABSTRAK

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES-128) DENGAN MENGGUNAKAN *ONE TIME PASSWORD MOBILE TOKEN* PADA *LOGIN* APLIKASI LENNA PT. SINERGI DIGITAL TEKNOLOGI

Oleh : Agung Santoso (1511502617)

PT. Sinergi Digital Teknologi merupakan Perusahaan IT yang menerapkan teknologi kecerdasan buatan(*Artificial Intelligence*) dan Aplikasi Lenna adalah salah satu produk teknologi informasi berbasis AI (*Artificial Intelligence*) yang di fungsikan sebagai asisten personal berbasis bahasa indonesia. Lenna mengutamakan fitur perintah suara (*Voice Command*) yang dapat memudahkan penggunanya melakukan perintah daripada memerlukan *input* berupa kalimat teks. Selain itu aplikasi lenna bisa memerintahkan untuk menjalankan berbagai hal seperti : membeli pulsa seluler, membeli tiket transportasi atau bioskop. Lenna juga dilengkapi fitur uang *elektronik* atau *e-wallet* untuk memenuhi kebutuhan transaksi. Para pengguna dapat melakukan pengisian saldo *e-wallet* dengan nominal tertentu.Untuk bisa menggunakan aplikasi lenna kita diharuskan memberikan data diri kita agar dapat menggunakan teknologi tersebut. Oleh karena itu keamanan data menjadi aspek yang harus diperhatikan juga, sehingga data diri kita tidak disalahgunakan pihak yang tidak betanggung jawab. Selama ini login aplikasi Lenna hanya menggunakan Metode *One Time Password* (OTP) tanpa adanya enrkipsi data. Hal ini menyebabkan pencurian data, sehingga diperlukannya keamanan data atau informasi untuk mengamankan informasi atau data dari yang tidak berwenang. Metode pembangkit kode *One Time Password* (OTP) pada penelitian ini menggunakan Algoritma kriptografi *Advanced Encryption Standard* dengan jumlah bit 128 (AES-128 Bit) yang digunakan untuk enkripsi data masukan oleh pengguna yang akan diambil 6 digit sebagai kode OTP dan digunakan sebagai validasi Kode OTP yang berada di *database*. Pada Proses enkripsi algoritma AES (*Advancd Encryption Standard*) terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes, Shiftrows, MixColumns,* dan *Addroundkey*. Pada awal enkripsi, input yang telah di *copy* ke dalam *state* akan mengalami transformasi *Subbytes, Shiftrows,MixColumns,* dan *Addroundkey* secara berulang-ulang sebanyak *Nr. penerapan* ini menggunakan algoritma *simetris* yang memiliki *key* pada saat enkripsi dan dekripsi menggunakan kunci yang sama. Selanjutnya *key* tersebut berada pada API dan android dengan mengambil 16 karakter dari proses *md5*. Tujuan penulisan skripsi ini adalah mencoba keamanan tambahan pada aplikasi Lenna berbasis android dengan menambahkan keamanan tersebut pada sebelum menggunakan aplikasi tersebut atau setelah login.

Kata kunci : *One Time Password* (OTP), *Advanced Encryption Standard* (AES-128),Android.

xvii+67 halaman; 52 gambar; 14 tabel; 1 lampiran