3.2 BAB II

2.1 TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penulisan penelitian ini akan coba mengaitkan dengan beberapa karya ilmiah terdahulu, sehingga akan didapatkan keterkaitan dengan karya ilmiah diatas. Adapun karya ilmiah yang penulis maksud adalah sebagai berikut :

MD5 adalah metode enkripsi dan dekripsi yang digunakan untuk pengamanan data. "Penerapan Message Diggest Algorithm MD5 untuk Pengamanan Data barang PT. Swifect Berbasis Desktop". Sistem dirancang untuk mengamankan informasi data yang mempunyai tujuan jika data diretas, maka peretas tersebut tidak bias melihat data plaintext dari database yang diretas karna sudah terenkripsi dengan metode MD5 tersebut (Rafiiq Zayana et al., 2022).

Studi terkait juga dilakukan dengan judul "Pemanfaatan Enkripsi MD5 Pada Keamanan Login Sistem Informasi Manufaktur PT.Maruki International Indonesia" diimplementasikan sebagai Enterprise Information Security System untuk keamanan login administrator dengan enkripsi MD5 yang menghasilkan chipertext sepanjang 128 bit (Sambo Layuk et al., n.d.).

Studi terkait selanjutnya juga dilakukan dengan judul "Perancangan Early Warning System
Untuk Mendukung Sistem Persediaan Barang Dagang". Tujuan dari penelitian berikut adalah memudahkan user dalam mengontrol persediaan barang pada perusahaannya (Rizal, n.d.).

Studi terkait berikutnya di lakukan dengan judul "Development of a Hotel Inventory System through Agile Methodology". Pada tahap perancangan sistem dengan menerapkan metode AGILE. Hasil dari penelitian ini menunjukan sistem inventaris hotel dengan menggunakan metode AGILE tersebut menghasilkan rancangan untuk melakukan pencatatan inventaris barang di hotel, serta dapat melakukan validasi data menggunakan system (Diaz et al., 2021).

Berdasar tinjauan pustaka tersebut ditemukan titik persamaan dengan penelitian sebelumnya. Adapun titik persamaannya yaitu membahas tentang pentingnya keamanan data dalam sebuah system dan memberikan peringatan dini agar meminimalisir kekurangan stok terkhusus system inventaris,

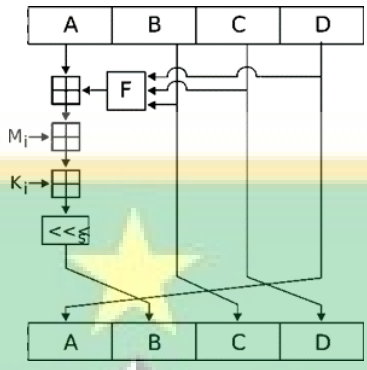
2.2 Inventory System

Sistem inventory barang elektronik adalah sistem yang digunakan untuk melakukan inventarisasi atau pengelolaan stok barang elektronik. Sistem ini biasanya terdiri dari database yang menyimpan informasi tentang jumlah, spesifikasi, dan lokasi barang elektronik, serta menyediakan fasilitas untuk melakukan transaksi penambahan dan penghapusan barang. Sistem inventory barang elektronik dapat membantu meningkatkan efisiensi dan akurasi dalam proses inventarisasi, serta membantu mengurangi resiko kehilangan atau kerusakan barang (Premana Agyztia, 2019).

2.3 MD5

MD5 adalah salah satu dari banyak metode hashing kriptografi dan penerus MD4. Profesor Ronald Rivest mengembangkan metode MD5 pada tahun 1991. Algoritma MD5 bekerja dengan menerima data input dengan ukuran yang tidak ditentukan dan kemudian mengubahnya menjadi metode kompresi pesan hash 128-bit, yang merupakan salah satu dari rangkaian 32 digit heksadesimal.

Proses kerja MD5 adalah memproses data asli dari blok input 512-bit, yang diproses berulang kali (de Guzman et al., 2018).



Gambar 1 Flow MD5

Pada gambar 1 merupakan flow dari MD5 dengan dasar operasi yang dapat dituliskan dengan persamaan berikut :

$$\alpha \leftarrow \boldsymbol{b} + \boldsymbol{CLS_s}\ (\boldsymbol{\alpha} + \boldsymbol{g}(\boldsymbol{b},\boldsymbol{c},\boldsymbol{d}) + \boldsymbol{X}[\boldsymbol{k}] + \boldsymbol{T}[\boldsymbol{i}] \qquad \textbf{(2.1)}$$

Dimana :

a,b,c,d = Merupakan Empat item pengubah penyangga 32-bit (yang akan berisi nilai penyangga A, B, C, D)

g = Salah satu fungsi F, G, H, I

CLS_s = Circular left shift sebanyak s bit.

$X[k]$ = Kelompok 32-bit ke-k dari blok 512bit message ke-q. Nilai k = 0 sampai 15

$T[i]$ = Elemen table T ke-I (32 bit)

+ = Operasi penjumlahan modulo 2^{32}.

MD5 merupakan fungsi hash satu arah yaitu seseorang dapat dengan mudah melakukan enkripsi dengan tujuan untuk mensensor data agar tidak mudah terbaca sehingga plaintext yang diinputkan menjadi chiphertext, namun untuk mengembalikkan chiphertext menjadi plaintext kembali didalam fungsi hash satu arah ini cukup sulit. sehingga masih banyak yang menggunakan algoritma ini untuk enkripsi data.

2.4 Enkripsi & Dekripsi

Enkripsi adalah salah satu teknik enkripsi, yang terjadi dengan kunci dekripsi. Secara umum, enkripsi adalah proses mengubah teks acak atau teks asli (plaintext) menjadi naskah acak (ciphertext) yang sulit dibaca oleh seseorang kecuali mereka memiliki kunci dekripsi. Dengan kata lain, sulit dibaca ada kemungkinan pemulihan skrip asli akan memakan waktu cukup lama dan membutuhkan kombinasi yang tepat sesuai dengan kuncinya. Jika seseorang memiliki kuncinya, tidak butuh waktu lama untuk mendekripsinya.

Enkripsi merupakan sebuah proses penyembunyian informasi asli dalam pesan yang hasil akhirnya akan tetap konsisten setelah di dekripsi. Yang mana enkripsi adalah sebuah proses pengubahan paintext menjadi chiphertext. Tujuan dari enkripsi ialah membuat kriptanalis sesulit mungkin untuk mendekripsi text yang telah di enkripsi (chiphertext) menjadi plaintext Kembali.

Dekripsi merupakan sebuh proses mengubah chiphertext menjadi plaintext. Dalam kata lain dekripsi adalah proses untuk membuka pesan asli dari sebuah enkripsi yang dimana informasi tersebut merupakan informasi asli dari sebuah pesan.

2.5 Early Warning System

Sistem peringatan dini atau Early Warning System merupakan sistem atau prosedur yang dirancang untuk memberikan peringatan terhadap potensi atau masalah yang tidak terdeteksi (Sha et al., 2022)

Sistem peringatan dini, seperti namanya, mengeluarkan peringatan yang dipicu oleh input berdasarkan aturan tertentu. Dalam implementasinya, peringatan yang dikirim dapat berupa message box pada stok barang jika stok tersebut sudah mencapai jumlah batas minimum (Liu et al., 2022).