BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Ada banyak sistem keamanan data telah dikembangkan dan dituangkan dalam penelitian dengan berbagai macam method yang digunakan. Referensi ini digunakan sebagai daasar dalam penyusunan penelitian ini yang memiliki keterkaitan dengan objek maupun metode penelitian yang diangkat. Ada berbagai macam penelitian yang mengangkat topik sistem keamanan *database* sejauh ini.

Hafid Rosianto (2017) pada penelitianya dalam penelitiannya mengimplementasikan adonan menurut 2 metode prosedur pemecahan yg tidak sinkron yaitu *Data Encryption Standard* serta *Blowfish* sebagai proses *encryption* dan *decryption* data. encripsi & dekripsi ini memakai data berekstensi, *.jpeg, .gif, .mp3, .mp4, .avi, .txt, .doc, .pdf*. Sistem ini dibangun menggunakan cara mengacak rambang bit menurut arsip orisinil tadi yg membentuk proses enkripsi yang tidak sinkron-beda. Dengan memakai perangkat lunak *Visual Studio* 2012 dengan bahasa pemrograman *Virtual Box.NET* [6].

Dalam Penelitian Oris Krianto Sulaiman tahun 2019 bertujuan untuk mengamankan pesan digital dengan memnggunakan methode *XOR Cipher* dan *Merkle-Hellman Knapsack*. Pengujian dilakukan pada text SRIE dan key ORIS dilakukanya *Xor Chipher* dan Enkripsi dengan *Merkle-hellman Knapsack* [7].

Dalam penelitian Purwadi(2021) Algoritma Markel Hellman digunakan sebagai sistem keamanan data terhadap penyalahgunaan data dari nilai siswa serta dapat lebih mengoptimalkan data untuk melindungi data nilai siswa. [8]

Dalam penelitian Muklas Adik P. menjelaskan Aplikasi berbasis web yang dibuat peneliti menggunakan setidaknya 4 bahasa yaitu *HTML ,CSS ,PHP* dan *JS*. Aplikasi ini membutuhkan web yang merupakan sebuah server dan juga menggunakan *browser* Untuk menyambungkan aplikasi web dan perangkat komputer dibutuhkan koneksi internet. [9]

Dalam penelitian Mahadi W., Sinar S., Taronisokhi Z. (2018) melakukan encripsi mengubah nilai piksel citra digital yang mengakibatkan nilai piksel tidak sama dengan citra yang asli. Dalam penelitiannya peneliti mengungkapkan bahwa peneliti menggunakan metode 128-bit *Advanced Encription System* serta *Triple Data Encryption Standard* sebagai enkripsi serta dekripsi citra digital terhadap aplikasi client-server. Hasil enkripsi dari algoritma *Advanced Encription System* dienkripsi lagi dengan menggunakan *Triple Data Encryption Standard* yang menghasilkan nilai dari piksel yang berbeda sekali dengan nilai piksel asli. [10]

Penelitian yang dilakukan Ahmad-Loay S., Dalia Y., dan M. Joudi (2020) secara luas didukung dan diadopsi oleh perangkat lunak dan perangkat keras. seperti yang dinyatakan di seluruh Apa yang membuat metode ini istimewa adalah Anda dapat menggunakan ukuran kunci berbeda, seperti 128-bit, 192-bit atau 256-bit dengan *cipher block* 128-bit. Sorotan lain dari AES Algoritmanya adalah bahwa proses enkripsi dan dekripsi sangat mirip dengan beberapa pengecualian. Variasi dan perbedaan urutan. Menjelaskan beberapa fitur kunci dari algoritma AES. Kinerja dievaluasi berdasarkan penelitian dan hasil sebelumnya. Korespondensi Penelitian telah menunjukkan bahwa AES dapat memberikan keamanan yang jauh lebih tinggi daripada yang lain. Algoritma seperti DES, 3DES. Algoritma AES tentunya memiliki beberapa kekurangan, Minimal dibandingkan dengan kekuatan. Akhirnya, kami tidak mengharapkan perubahan peneliti akan menggunakan algoritma ini dalam waktu dekat kecuali kuantum/superkomputer menyelesaikannya dengan baik kata sandi. [11]

Tabel 2.1 Penelitian Terdahulu

No	Judul Penelitian	Penulis	Ringkasan
1.	Implementasi Algoritma Data Encyption Standard Berbasis Blowfish Untuk Enkrip Dan Dekrip Data [6]	Anifah L. dan Rosianto H.	Penelitian ini mengimplementasikan adonan menurut 2 metode prosedur pemecahan yang tidak sinkron yaitu *Data encryption standard* dan *blowfish* buat enkripsi dan dekripsi data. Untuk proses enkripsi serta dekripsi ini memakai *.jpeg, .gif, .mp3, .mp4, .avi .txt, .doc, .pdf* . System ini dibangun menggunakan cara mengacak rambang bit menurut arsip orisinil tadi yg membentuk proses enkripsi yg tidak sinkron-beda. Dengan memakai bahasa pemrograman VB.NET dengan *visual studio* tahun 2012
2.	Hybrid Cryptosystem Menggunakan Xor Cipher Dan *Merkle–Hellman Knapsack* Untuk Menjaga Kerahasiaan Pesan Digital [7]	Sulaiman,Oris K.	Penelitian ini bertujuan untuk mengamankan pesan digital dengan menggunakan methode m*erkle-hellman knapsack serta XOR cipher*. Pengujian dilakukan pada text SRIE dan key ORIS dilakukanya Xor *Cipher* dan enkripsi dengan *Merkle-hellman Knapsack*

No	Judul Penelitian	Penulis	Ringkasan
3.	Implementasi Kriptografi Merkle-Hellman Dalam Mengamankan Data Nilai Siswa SMK Wira Kesuma Jaya Kec. Namo Rambe [8]	Tahun 2021 oleh Purwadi	Algoritma Markel Hellman digunakan sebagai sistem keamanan data terhadap penyalahgunaan terhadap data dari nilai siswa serta dapat mengoptimalkannya data untuk melindungi data dari nilai siswa.
4.	Perancangan Aplikasi Enkripsi & Dekripsi Pada Dokumen File Dengan Algoritma Triple Des Berbasis Web [9]	Muklas A. P., Dadang I. M., Runi A. A., Mirsandi	Aplikasi berbasis web ini menggunakan CSS, PHP, HTML dan JS. sebagai bahasa pemrogramanya. Aplikasi ini membutuhkan web server dan juga menggunakan *browser*. Untuk menyambungkan aplikasi web dan perangkat komputer dibutuhkan koneksi internet.
5.	Implementasi Algoritma *AES* Dan *Triple DES* Untuk Mengamankan Citra Digital [10]	Taronisokhi Z. ,Mahadi W., Sinar S.,	Dalam penelitian ini melakukan enkripsi dengan cara memodifikasi nilai piksel citra sedemikian rupa untuk menghasilkan nilai piksel yang tidak sama dari nilai citra aslinya untuk keamanan. . proses enkripsi algoritma AES memiliki hasi yang nantinya akan dienkripsi ulang dengan menggunakan Triple DES

No	Judul Penelitian	Penulis	Ringkasan
			untuk setidaknya menghasilkan nilai piksel yang tidak sama dengan nilai dari piksel asli.
6.	*Advance Encryption Standard Encryption*: *Study & Evaluation* [11]	Ahmad L. S., Dalia Y., dan Mohamad J.	Algoritma AES adalah salah satu algoritma yang paling efektif dan efisien. Ini secara luas didukung dan diadopsi oleh perangkat lunak dan perangkat keras. seperti yang dinyatakan di seluruh Apa yang membuat metode ini istimewa adalah Anda dapat menggunakan ukuran kunci setidaknya tidak sama, seperti 128-bit, 192-bit, dan 256-bit dengan *cipher block* 128-bit. Sorotan lain dari AES Algoritmanya adalah bahwa proses enkripsi dan dekripsi sangat mirip dengan beberapa pengecualian. Variasi dan perbedaan urutan. Menjelaskan beberapa fitur kunci dari algoritma AES. Kinerja dievaluasi berdasarkan penelitian dan hasil sebelumnya. Korespondensi Penelitian telah menunjukkan

No	Judul Penelitian	Penulis	Ringkasan
			bahwa AES dapat memberikan keamanan yang jauh lebih tinggi daripada yang lain. Algoritma seperti DES, 3DES. Algoritma AES tentunya memiliki beberapa kekurangan, Minimal dibandingkan dengan kekuatan. Akhirnya, kami tidak mengharapkan perubahan peneliti akan menggunakan algoritma ini dalam waktu dekat kecuali kuantum/superkomputer menyelesaikannya dengan baik kata sandi.

Setelah ditinjau terlihat bahwa penelitian terdahulu yang dijadikan acuan penelitian ini menunjukkan perbedaan dengan penelitian-penelitian yang telah dilakukan peneliti yaitu menggunakan algoritma kriptografi *Merkle-hellman Knapsack* serta *Advanced Encryption Standard (AES)* Sebagai keamanan dari data yang ada didalamnya. Sementara instrumen objek penelitian ini nantinya adalah admin, password, dan Data pada website yang dirancang sendiri oleh peneliti. Dalam perancanganya data yang dibaca oleh public adalah yang dienkripsi.

2.2 Dasar Teori

2.2.1 Data

Data merupakan bagian penting dari sistem informasi perusahaan dan menjadi acuan dalam pengambilan keputusan. Tidak dapat dipungkiri bahwa perkembangan teknologi informasi di negara ini semakin pesat. Hal ini tentunya akan berdampak positif bagi semua orang [12]. Dari pernyataan tersebut dapat

disimpulkan bahwa itu adalah database atau yang lebih dikenal database tempat untuk menyimpan, mengelola dan manajemen data yang besar dimana basis data ini dapat digunakan oleh banyak pengguna secara bersamaan [13]. Pada umumnya, basis data terdiri dari beberapa tabel yang tersusun berisikan informasi dari suatu aplikasi atau program yang diakses sesuai kebutuhan [14]. *Database* tentunya sangat dibutuhkan dalam sistem informasi yang dimana data disimpan dan diolah menjadi sebuah informasi yang cukup penting bagi perusahaan organisasi [15].

Pada praktiknya, ada beberapa aplikasi manajemen basis data yang umum digunakan seperti Oracle, MySQL, MariaDB, PostgreSQL dan masih banyak lagi. Proses manajemen pada *database* umumnya dikenal dengan *Create, Read, Update, Delete*. Sesuai dengan istilah tersebut, di dalam *database*, kita dapat melakukan proses manipulasi seperti membuat/merancang, membaca, melakukan pembaruan dan juga penghapusan. Sistem tersebut juga mempermudah seorang administrator basis data dalam melakukan pengelolaan dan manajemen dari basis data itu sendiri.

2.2.2 Merkle-Hellman Knapsack

Knapsack digunakan dengan menggunakan logika XOR.*Knapsack* juga memiliki Panjang kunci antara 8-bit sampai 72-bit. Misalnya pada operasi perkalian antara dua bilangan 9 digit, bilangan yang panjangnya 18 dimasukkan ke dalam tipe *long double*, setelah itu dengan menggunakan fungsi modulus akan menghasilkan bilangan dengan panjang 9-bilangan. *Cipher Merkle-Hellman Knapsack* terdiri dari lima komponen: data murni, data kriptografi, kunci kriptografi, fungsi konversi enkripsi, dan fungsi konversi dekripsi. [16].

Merkle-hellman Knapsack memiliki 3 proses yaitu pembuatan kunci, *encryption* dan *decryption* berikut adalah proses perhitunganya : [17]

1. Pembuatan Kunci

1. Pilih ukuran blok n. Bilangan bulat hingga n bit panjangnya dapat dienkripsi dengan kunci ini.
2. Pilih urutan superincreasing acak dari n bilangan bulat positif.
   $W = (w_1, w_2, w_3 \dots , w_n)$ (2.1)

Syarat (2.1) diketahui persyaratan superincreasing berarti $w_k > \sum_{i=1}^{k-1} w_i$, for 1 <k≤n.

3. Pilih bilangan bulat acak q sedemikian rupa sehingga

$$q > \sum_{i-1}^{n} w_i \text{ (2.2)}$$

4. Pilih bilangan bulat acak r sehingga gcd(r,q)=1 (yaitu, r dan q adalah coprime).
5. Hitung urutannya

   $B = (b_1, b_2, \ldots b_n)$(2.3)

   Dimana $b_i = rw_i \ mod \ q$ (2.4)

   Kunci publik adalah B dan kunci pribadi adalah (W,q,r).

2. Encryption

Biarkan m menjadi pesan, n-bit yang terdiri dari bit $m_1m_2 \ldots m_n$, dengan m_1 urutan tertinggi sedikit. Pilih setiap b_1 yang m_i bukan nol, dan tambahkan bersama-sama. Secara ekuivalen, hitung .

$$c = \sum_{i=1}^{n} m_i b_i \text{ (2.5)}$$

Teks sandinya adalah c.

3. Decription

Untuk mendekripsi ciphertext c kita harus menemukan subset dari B yang berjumlah c. Kami melakukan ini dengan mengubah masalah menjadi salah satu pencarian subset dari W. Masalah tersebut dapat diselesaikan dalam waktu polinomial karena W semakin meningkat.

1) Hitung invers modular dari r modulo q menggunakan algoritma Extended Euclidean. Kebalikannya akan ada karena r koprime dengan q.

$$r' \coloneqq r^{-1} \ (mod \ q) \text{(2.6)}$$

Perhitungan r' tidak bergantung pada pesan, dan dapat dilakukan hanya sekali ketika kunci privat dibuat.

2) Hitung

$$c' \coloneqq cr' \ mod \ q (2.7)$$

3) Selesaikan masalah jumlah subset untuk c' menggunakan deret superincreasing W, dengan algoritma serakah sederhana yang dijelaskan di bawah ini. Misalkan $X = (x_1, x_2, \dots, x_k)$ menjadi daftar indeks yang dihasilkan dari elemen :
   W yang berjumlah $c'. (itu \ adalah \ c = \sum_{i=1}^{k} w_{xii})$(2.8)

4) Buat pesan m dengan 1 di setiap posisi bit x_i dan 0 di semua posisi bit lainnya:

$$m = \sum_{i=1}^{k} 2^{n-xi} \ (2.9)$$

2.2.3 *Advanced Encryption Standard*

AES *(Advanced Encryption Standard)* merupakan kelanjutan enkripsi DES *(Data Encryption Standard)* yang memiliki masa berlaku telah dianggap kadaluwarsa dengan alasan keamanan. Algoritma ini bertipe simetris atau menggunakan kunci yang sama untuk dekripsi dan enkripsinya.[7] *Advanced Encryption Standard* menggunakan symmetric key block cipher memiliki ukuran kunci yang berbeda yaitu 128-bit, 192-bit, dan 256-bit. Pemerintahan Amerika Serikat telah menggunakan AES untuk standar dari enkripsi. Untuk ini mencakup 3-cipher blok ada *Advanced Encryption Standard*-128, *Advanced Encryption Standard*-192 dan *Advanced Encryption Standard*-256, dari koleksi yang lebih besar dan dirilis di tahun 200l dengan nama rijndael.[8] *Advanced Encryption Standard* dianalisis dengan menyeluruh, sekarang telah digunakan di dunia. [9]. Proses algoritma enkripsi *Advanced Encryption Standard* (AES) mencakup 4 fungsi konversi yaitu; *MixColumns*, *SubByte*, *ShiftRows,* dan *AddRoundKey* [18]. Di dalam AES kecepatan waktu dari enkripsi serta dekripsinya sama sekali tidak dipengaruhi oleh jenis file, tetapi dapat dipengaruhi oleh ukuran filenya. Untuk waktu dari proses dipengaruhi oleh besaran dari plainteks(file asli) . [19].

2.2.4 Web Server

Internet atau lebih kita kenal dengan Web memiliki berbagai jenis layanan yang umum kita gunakan, salah satunya adalah *Web Server*. *Server web* adalah server yang menyediakan layanan data dan media melalui jaringan komputer atau Internet menggunakan protokol HTTP dan HTTPS, dan mengirimkannya sebagai halaman web dalam bentuk file HTML [20]. Bentuk komunikasinya sendiri searah antara *client* dengan *Server* dan bersifat *Connection Less*, karena pada saat itu server hanya merespon request client dan tidak mempertahankan koneksi yang persisten. Fungsi utama server web adalah mengirimkan file yang diminta klien melalui protokol HTTP dan HTTPS (jenis layanan web dengan fitur *secure*/keamanan*)* [21].

web server sendiri dapat diakses oleh pengguna/*client* menggunakan aplikasi *web browser*. Proses permintaan yang dilakukan oleh pengguna akan dibaca oleh web browser sebagai request untuk kemudian request tersebut dikirimkan lagi oleh web server kepada client melalui web browser [22]. Untuk platformnya sendiri, web server memiliki banyak jenis seperti Apache, Nginx, Lighttpd dan masih banyak lagi dengan Apache merupakan yang paling umum digunakan hingga saat ini.