BAB II

KAJIAN PUSTAKA

2.2 Teori Dasar

2.2.1 Keamanan Jaringan

Keamanan jaringan adalah suatu proses untuk pencegahan dan identifikasi dari aktifitas penggunaan yang tidak sesuai serta dari jaringan komputer tersebut. Selain itu, keamanan jaringan berupaya untuk mengamankan bahaya dan ancaman berupa ancaman fisik dan logis sehingga mengganggu secara langsung dan tidak tidak langsung (Amarudin, 2018).

Dibawah ini adalah tiga konsep umum yang ada di dalam keamanan jaringan.

1. *Risk*

   Risiko atau tingkat bahaya untuk menunjukkan kemungkinan penyusup dapat menyusup ke jaringan komputer ditunjukkan dengan risiko atau tingkat bahaya.

2. *Threat*

   untuk menyampaikan ancaman dari mereka yang mencoba mendapatkan akses tidak sah ke sistem jaringan komputer pengguna.

3. *Vulnerability*

   Untuk menunjukkan kekuatan dan ketahanan sistem keamanan terhadap potensi ancaman dan bahaya eksternal.

2.2.2 Keamanan Data

Salah satu komponen penting dari suatu sistem informasi adalah keamanan. Sayangnya, tidak banyak perhatian yang diberikan terhadap kerentanan

keamanan ini. Masalah keamanan sering kali menempati urutan kedua atau bahkan terakhir dalam daftar prioritas. Jika masalah keamanan ini memengaruhi fungsionalitas sistem, masalah ini biasanya diminimalkan atau dihilangkan sama sekali (Sari et al., 2021).

Kemampuan mengakses sebuah penyedia informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berbentuk organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan maupun individual (pribadi). Kemajuan pesat dalam teknologi komputer dan telekomunikasi memungkinkan hal ini. Data sensitif tidak disimpan di komputer di masa lalu karena jumlahnya sangat sedikit. Komputer hanya digunakan untuk menyimpan data rahasia sejak tahun 1950an (Mukthar, 2018).

Karena pentingnya dan berharganya suatu informasi, terkadang individu tertentu diminta untuk memiliki akses eksklusif terhadap informasi tersebut. Kepemilikan informasi dapat mengalami kerugian jika informasi tersebut berada di tangan pihak ketiga, seperti pihak komersial. Misalnya, banyak informasi perusahaan bersifat rahasia dan hanya tersedia untuk orang tertentu. termasuk rincian tentang item yang sedang dikembangkan dan algoritma serta proses produksi yang digunakan untuk membuatnya. Oleh karena itu, keamanan sistem informasi perlu dijamin dalam batas wajar (Putri et al., 2020).

Informasi dapat dikirim dengan cepat berkat jaringan komputer seperti internet dan jaringan area lokal (LAN). Hal inilah yang menjadi pembenaran utama mengapa perusahaan atau organisasi mulai membangun *Local Area Network (LAN)* dan menghubungkannya ke internet untuk sistem informasi mereka. Potensi lubang

keamanan disebabkan oleh komputer yang terhubung ke jaringan area lokal (LAN), dan lubang ini dapat ditutup dengan menggunakan langkah-langkah keamanan fisik. Hal ini sesuai dengan gagasan bahwa tingkat keamanan suatu sistem informasi berbanding terbalik dengan kemudahan aksesnya. Semakin sulit mengakses informasi (tidak memuaskan), semakin tinggi ambang sensitivitasnya (Prasetyo & Wirawan, 2018).

Keamanan data mengacu pada menjaga informasi dalam sistem dari akses ilegal, perubahan, atau penghapusan, serta menjaga sistem komputer dari penggunaan atau modifikasi yang tidak sah (Irma Listiani et al., 2022).

Keamanan data dan informasi memiliki tiga komponen utama, yaitu

1. *Privacy/Confidentiality* yaitu yang mengacu pada tindakan yang diambil untuk menamankan keamanan data milik pribadi dari akses yang tidak sah.
2. *Integrity* yaitu upaya untuk menghambat pihak yang tidak berkepentingan mengubah data atau informasi.
3. *Authentication* adalah suatu upaya atau teknik untuk memastikan keabsahan data, seperti apakah informasi yang dikirim benar-benar dilihat oleh penerima yang dituju atau apakah server yang menerima layanan tersebut benar-benar tersumber dari server data yang bersangkutan. Ketersediaan sistem dan data (informasi) bila diperlukan berkorelasi dengan ketersediaan data.

Keamanan fisik dan keamanan sistem adalah dua kategori keamanan data. Keamanan fisik mencakup segalanya mulai dari pemasangan kabel hingga server, terminal, dan router klien. Keamanan sistem, di sisi lain, mengacu pada keamanan dalam sistem operasi, atau lebih tepatnya, perangkat lunak, yang menggunakan

teknik seperti steganografi dan kriptografi. Dalam studi ini, kita akan membahas tentang bagaimana keamanan data dicapai dengan menggabungkan steganografi dan kriptografi.

2.2.3 Jenis Serangan

1. Serangan DDoS (*Distributed Denial of Service)*

   Serangan ini ditujukan untuk mengganggu layanan online dengan mengalirkan lalu lintas internet berlebih ke server atau situs web tertentu, sehingga membuatnya tidak dapat diakses oleh pengguna yang sah (Akhriana & Irmayana, 2019).

2. Serangan Malware:

   kategori terdiri dari malware seperti trojan, worm, dan virus yang bertujuan untuk merusak, mencuri, atau mengambil alih perangkat.

3. Serangan *Phishing*:

   Serangan ini melibatkan upaya untuk memperoleh informasi pribadi atau keuangan dengan menggunakan situs web atau komunikasi palsu untuk berpura-pura sebagai sumber yang dapat dipercaya..

4. Serangan *Man-in-the-Middle (MITM*)

   Ketika seseorang mencuri atau merusak data antara dua pihak yang berkomunikasi tanpa sepengetahuan korban, hal itu disebut penyerangan.

5. Serangan *SQL Injection*

   Hal ini memerlukan penggunaan input yang salah untuk mengeksekusi pernyataan SQL berbahaya pada database, yang dapat mengakibatkan pencurian atau kerusakan data.

6. Serangan *Cross-Site Scripting (XSS)*

   Penyerang menyisipkan kode skrip berbahaya ke dalam aplikasi web atau halaman web yang akan dijalankan oleh pengguna yang mengunjungi situs tersebut.

7. Serangan *Ransomware*

   Jenis serangan ini mencakup enkripsi data korban dan penuntutan tebusan untuk mendekripsi data tersebut.

8. Serangan *Insider Threat*

   Terjadi ketika seseorang yang memiliki akses ke sistem atau data organisasi dengan sengaja atau tidak sengaja merusak atau mencuri informasi.

9. Serangan *Zero-Day*

   Serangan ini menge exploit kerentanan perangkat lunak yang belum diketahui oleh pihak yang mengembangkan perangkat lunak tersebut.

10. Serangan *Social Engineering*

    Serangan ini melibatkan manipulasi atau penipuan orang untuk mengungkapkan informasi rahasia atau melakukan tindakan yang merugikan organisasi (Akhriana & Irmayana, 2019).

2.2.4 Model Deteksi Serangan

Salah satu cara untuk mendefinisikan keamanan jaringan adalah kemampuan komputer yang terhubung ke beberapa jaringan untuk memberikan risiko keamanan yang lebih besar dibandingkan komputer yang tidak terhubung ke jaringan apa pun (Pramono et al., 2021). Ancaman keamanan jaringan yang tidak

diinginkan dapat dihindari melalui deteksi dan pengendalian. Pengguna jaringan komputer juga berharap bahwa pesan yang mereka kirim akan sampai ke penerima yang dituju tanpa perubahan atau cacat apa pun ketika mereka menerimanya, mengingat keadaan keamanan jaringan saat ini (Constantin Menteng et al., 2023). Keamanan suatu jaringan dapat dianggap kurang aman dan lebih rentan terhadap serangan jika jaringan tersebut mudah diakses. Sebaliknya, jika sulit mendapatkan akses ke suatu jaringan, maka tindakan keamanan jaringan akan lebih efektif. Keamanan jaringan terancam karena sejumlah elemen yang ada dalam jaringan komputer. Misalnya, semua jenis serangan, baik logis maupun fisik, merupakan masalah umum dalam jaringan komputer. Aktivitas apa pun di jaringan dapat terganggu oleh serangan langsung atau tidak langsung. Di antara banyak elemen penentunya adalah: Masalah pada perangkat keras komputer, sistem operasi jaringan, sistem jaringan komputer, dan kelemahan pengguna komputer (Constantin Menteng et al., 2023).

2.2.5 *Megitation IDS*

Perangkat yang dapat mendeteksi aktivitas mencurigakan pada jaringan atau sistem komputer yang tidak biasa bagi sistem atau jaringan tersebut disebut sistem deteksi intrusi, atau IDS. Ini bisa berbasis perangkat keras atau berbasis perangkat lunak (Tama et al., 2019).

Menurut (Eric & Jurcut, 2022), Tujuan dari *sistem deteksi intrusi* (IDS) adalah untuk mengidentifikasi beberapa lalu lintas paket yang tidak tepat atau tidak terduga di jaringan. Perangkat lunak yang diinstal pada perangkat dapat digunakan untuk membangun sistem deteksi intrusi (IDS). IDS memiliki kemampuan untuk

memantau dan mengidentifikasi beberapa paket mencurigakan yang dapat membahayakan keamanan jaringan selama pengoperasiannya.

Sistem deteksi intrusi, atau IDS, pada dasarnya adalah sistem yang dapat mencatat log, memblokir serangan, dan menganalisis serta mendeteksi serangan secara real time. Salah satu cara untuk menggambarkan sistem deteksi intrusi (IDS) adalah sebagai alat keamanan yang membantu menangani aktivitas mencurigakan dari peretas (Swapna et al., 2018).

IDS terdiri dari beberapa komponen, yaitu sebagai berikut:

a. *Security events* yang dapat dikenali oleh sensor
b. Pengelola kontrol sensor dan mengawasi kejadian atau peringatan dilakukan oleh *Console*
c. Sensor mencatat peristiwa dan menyimpannya dalam database dengan memanfaatkan aturan keamanan *Central Engine*. Namun demikian, jika intrusi (serangan) atau infiltrasi terjadi dalam jaringan di mana terdapat perilaku yang meragukan, sistem deteksi intrusi (IDS) tidak selalu efektif dalam mencegahnya. IDS terbatas pada deteksi; itu tidak bisa dicegah. Meskipun demikian, IDS memainkan sejumlah tanggung jawab penting dalam keamanan jaringan. Ini adalah beberapa peran penting yang dimainkan IDS. (Swapna et al., 2018).

a. Awasi secara aktif aktivitas apa pun yang mencurigakan.
b. Lakukan secara teliti pemeriksaan di audit logs.
c. Memberitahu administrator melalui SMS atau peringatan jika Anda melihat adanya perilaku yang mencurigakan.

d. Lakukan pemberian symbol atau tanda jika semisal ada kerentanan.

IDS dapat dibagi menjadi dua kelompok berdasarkan seberapa baik IDS dapat mengidentifikasi intrusi atau serangan pada jaringan:

Pemeriksaan seluruh lalu lintas jaringan dilakukan oleh sistem deteksi intrusi berbasis jaringan, atau NDS, untuk menentukan apakah telah terjadi intrusi atau serangan. Intinya, segmen jaringan yang penting dan yang mirip dengan pintu masuk jaringan adalah rumah bagi sistem deteksi intrusi jaringan (NIDS). Sementara itu, kelemahan NIDS adalah memerlukan lebih banyak pekerjaan untuk menyiapkannya pada jaringan Ethernet-switched. Namun, untuk memantau koneksi port, sejumlah produsen switch Ethernet telah menambahkan fitur IDS ke switch produksi mereka (Swapna et al., 2018).

Sistem Deteksi Intrusi Berbasis Host (HIDS) adalah suatu sistem yang mendeteksi intrusi yang kemampuannya terbatas untuk mengidentifikasi intrusi pada host tempatnya diinstal. Apakah ada aktivitas mencurigakan atau upaya penyusupan, HIDS mengawasi dan mencatat semua aktivitas di satu host jaringan. Lebih sering daripada tidak, HIDS diinstal pada sejumlah server penting, seperti firewall, server web, atau server yang sedang online.

2.2 Teori Khusus

2.2.1 Algoritma

Algoritme adalah teknik berguna yang muncul sebagai kumpulan perintah yang dinyatakan untuk menghitung suatu fungsi. Saat mengatasi suatu masalah, ada persyaratan keadaan pertama yang harus dipenuhi sebelum algoritma dijalankan. Untuk semua permulaan yang memenuhi persyaratan, algoritma akan selalu

berakhir. Diawali dari nilai awal, serangkaian perintah akan dijalankan untuk memproses kondisi yang ditentukan guna menghasilkan keluaran, setelah itu kondisi akhir akan dipastikan (Sulistiyawati & Supriyanto, 2021).

Algoritme adalah penjelasan langsung tentang logika yang ditulis oleh pengembang perangkat lunak untuk sistem komputer guna meningkatkan efektivitas perangkat lunak dalam mencapai tujuannya dan menghasilkan hasil dari masukan yang diberikan (terkadang nol).

Menurut (Rahmanto et al., 2021), Sebuah algoritma harus memiliki lima sifat penting berikut: keterbatasan, kepastian, masukan, keluaran, dan kemanjuran. Suatu algoritma diharus berhenti untuk semua keadaan dan memproses ke sejumlah langkah yang telah ditentukan agar dianggap terbatas. Sesuai dengan konsep ketetapan, setiap langkah harus diungkapkan secara tepat (tidak jelas atau ambigu).

Masukan : Suatu algoritma mungkin menerima satu atau lebih masukan, atau tidak menerima masukan sama sekali. Besaran yang dimasukkan pada awal sebelum algoritma dijalankan disebut masukan. Setiap algoritma menghasilkan beberapa jenis keluaran, yang bisa berupa satu atau beberapa keluaran. Besaran yang berhubungan atau terhubung dengan masukan disebut keluaran. Efektivitas: Setiap algoritma harus mendasar dan mampu menyelesaikan semua tugas dalam jangka waktu yang wajar agar dianggap efektif.

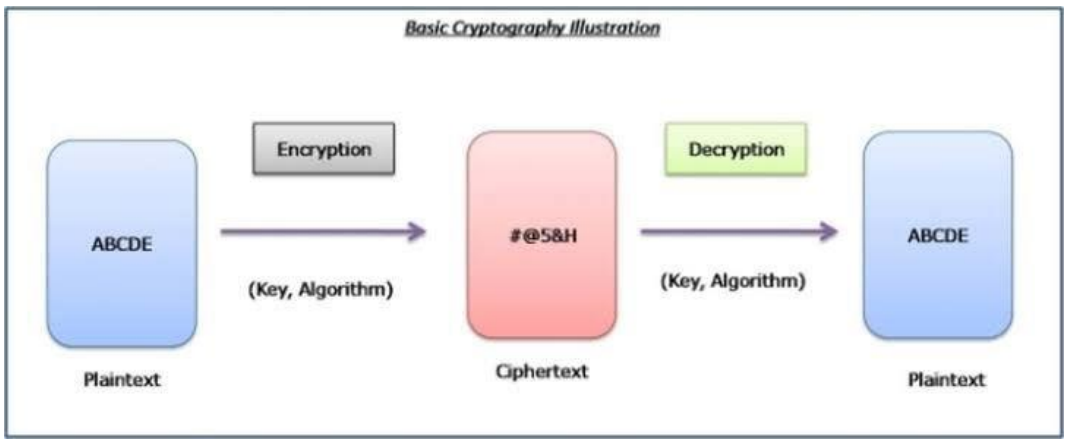
Ambang batas kerumitan suatu algoritma adalah jumlah langkah yang harus diambil algoritma tersebut untuk menyelesaikan suatu masalah tertentu. Dengan kata lain, algoritma dengan kompleksitas tinggi adalah algoritma yang dapat menyelesaikan suatu masalah dengan cepat, sedangkan algoritma dengan

kompleksitas rendah memerlukan waktu yang lebih lama untuk menyelesaikan suatu masalah.

2.2.2 Kriptografi

Studi tentang penulisan rahasia, atau kriptografi, bertujuan untuk mengkodekan data dan komunikasi sedemikian rupa sehingga dapat didekripsi dan kemudian didekodekan sekali lagi, menjaga isinya tetap tersembunyi dari mata-mata. Kata kriptografi berasal dari kata Yunani "*kryptos"* yang berarti tersembunyi. Studi tentang transformasi data, informasi, dan dokumen menjadi bentuk yang unik dan menantang untuk dipahami dikenal sebagai kriptografi. Ini juga dapat dipahami sebagai tulisan terselubung (Sutejo, 2021).

Enkripsi, juga dikenal sebagai *decipherment*, adalah proses mengubah teks biasa menjadi teks tersandi dekripsi, juga dikenal sebagai decipherment, adalah proses mengembalikan ciphertext ke *plaintext*. Parameter konversi yang dikendalikan oleh satu atau lebih kunci digunakan dalam kriptografi. Saat ini, kriptografi memainkan peran penting dalam keamanan teknologi informasi, terutama ketika berkomunikasi secara rahasia (Assyamiri & Hardinanto, 2022).



Gambar 2. 1 Ilustrasi kriptografi

Beberapa istilah yang harus kita ketahui adalah:

1. Pesan,*Plainteks*, dan*Cipherteks*

Data atau informasi yang dapat dibaca dan dipahami disebut pesan. Pesan dapat ditangkap pada media atau dikirimkan sebagai data atau informasi melalui telepon atau melalui metode lain. Tidak hanya pesan teks yang dapat disimpan, file biner, suara atau suara lainnya (audio), dan gambar (mage) juga dapat disimpan. Untuk mencegah orang lain memahami substansi komunikasi, maka harus dikodekan ke dalam format lain yang tidak dapat dipahami (Matondang et al., 2018).

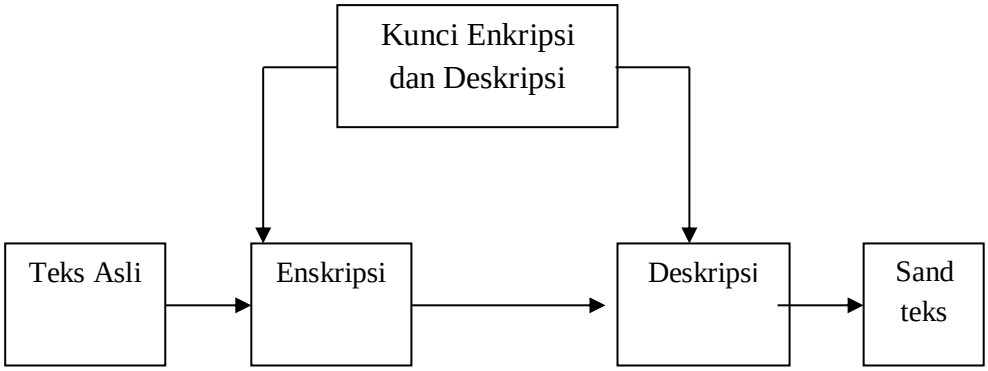
2. *Enkripsi* dan *Dekripsi*

Enkripsi adalah proses mengubah plaintext menjadi ciphertext. Dekripsi, di sisi lain, adalah proses mengubah ciphertext kembali ke plaintext asli.

3. *Ciphe*r dan Kunci

Algoritma kriptografi, yang merupakan difungsikan dari matematika yang di pergunakan untuk enkripsi dan dekripsi, juga dikenal sebagai cipher. Cipher adalah aturan untuk pengkodean dan penguraian kode. Tautan antara dua himpunan - himpunan yang berisi potongan teks biasa dan himpunan berisi teks tersandi merupakan gagasan matematis yang mendasari teknik kriptografi. Fungsi enkripsi dan dekripsi dalam kriptografi kontemporer memetakan komponen antara kedua kelompok ini. Dalam hal ini, algoritme tidak lagi bersifat rahasia, namun kuncinya tetap perlu dipertahankan seperti itu. Kunci adalah parameter yang digunakan dalam pengkodean dan penguraian transformasi. Seberapa aman suatu algoritma dapat ditentukan oleh seberapa besar usaha yang diperlukan untuk menerjemahkan

ciphertext menjadi plaintext tanpa mengetahui kunci rahasianya (Matondang et al., 2018).



Gambar 2. 2 Skema Enskripsidan Deskripsi

4. Sistem Kriptografi

Suatu sistem yang terdiri dari kriptografi dikenal sebagai sistem kriptografi. Kumpulan kunci, ciphertext dan plaintext yang dapat dibuat, dan suatu algoritma kriptografi disebut kriptosistem. Sistem kriptografi terdiri dari lebih dari sekedar sandi (Suhandinata et al., 2019).

5. Penyadap

Seseorang yang mencoba untuk mencegat pesan saat sedang dikirim dikenal sebagai penyadap. Untuk memecahkan ciphertext, penyadap ingin belajar sebanyak mungkin tentang protokol kriptografi yang digunakan untuk komunikasi.. Nama lainpeyadap: *enemi, adversary, intruder, interceptor, bad guy*. (Matondang et al., 2018).

6. Kriptanalisis dan Kriptologi

Bidang kriptanalisis lahir dari arah yang berlawanan dengan perkembangan kriptografi. Ilmu dan keterampilan menguraikan ciphertext menjadi plaintext tanpa mengetahui kuncinya dikenal dengan istilah kriptoanalisis. Kami menyebut

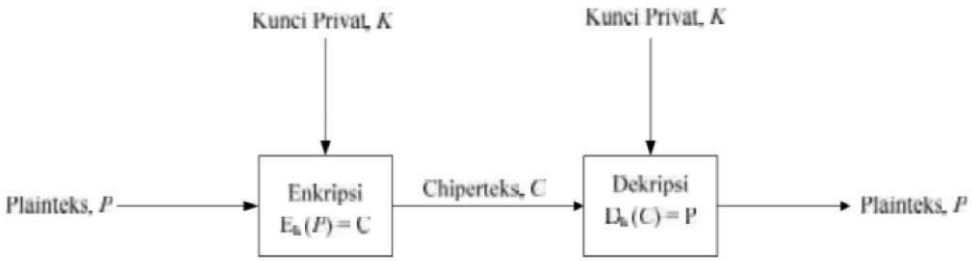
pelakunya sebagai kriptanalisis. Jika suatu algoritma dan kunci digunakan oleh seorang kriptografer untuk mengubah teks biasa menjadi teks tersandi, seorang kriptanalis mencoba menguraikan teks tersandi untuk mendapatkan teks biasa atau kunci. Ilmu yang mempelajari kriptografi dan kriptanalisis dikenal dengan istilah kriptologi (cryptology). Ada hubungan antara kriptografi dan kriptanalisis. (Matondang et al., 2018).

1. Jenis-jenis Algoritma Krptografi

Berdasarkan kunci yang digunakannya, algoritma kriptografi dapat diklasifikasikan menjadi tiga kategori (Azhari et al., 2022) :

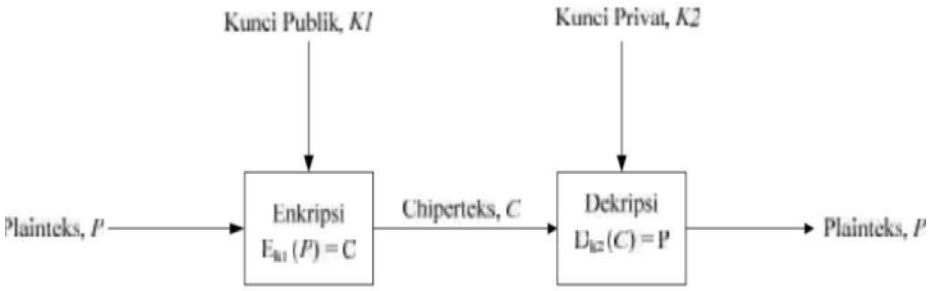
1. Algoritma *Simetri* (enkripsi dan dekripsi dengan satu kunci). Jenis kriptografi yang paling sering digunakan adalah kriptografi ini. Pesan terenkripsi dapat dibuka kuncinya dengan kunci yang sama yang digunakan untuk membuatnya. Oleh karena itu, pengirim dan penerima pesan harus memiliki kunci yang sama persis. Rahasia ciphertext dapat dibuat dan diungkapkan oleh siapa saja yang mempunyai kunci, termasuk oleh orang yang tidak berkepentingan. Terkadang masalahnya di sini bukan pada pengiriman ciphertext melainkan mencari cara agar pihak yang dituju menerima kunci simetris.. *DES (Data Encryption* Standard), blowfish, twofish, MARS, IDEA, 3DES (DES diterapkan tiga

kali),dan *AES (Advanced Encryption Standard),* yang nama aslinya adalah Rijndael, adalah beberapa contoh algoritma kunci simetris.



Gambar 2. 3 Proses Endskrip Algoritma Simetri

2. Algoritma asimetris yang pemakaiannya kunci yang beda untuk mengenkripsi dan mendekripsi data. Algoritme asimetris kadang-kadang dikenal sebagai algoritma kunci publik karena menggunakan kata kunci yang berbeda untuk enkripsi dan dekripsi. Kunci algoritma asimetris terdiri dari dua bagian, yaitu:
   a. Kunci umun (*publickey*): kunci yang mampu diakses oleh siapa saja (dipublikasikan).
   b. Kunci rahasia (*privatekey*): kode tersembunyi yang hanya diketahui oleh satu orang saja. Kunci-kunci ini saling berhubungan satu sama lain. Pesan dapat dienkripsi dengan kunci publik, namun tidak dapat didekripsi. Hanya pemilik kunci rahasia yang mampu mendekripsi komunikasi. Contoh algoritma asimetris yaitu *RSA*, Rabin dan El Gamal. Skema kriptografi algoritma asimetris dapat dilihat pada gambar (Azhari et al., 2022).



Gambar 2. 4 Algoritma Simetris

Algoritma simetri digunakan dalam aplikasi ini pada gambar di atas, untuk *enkripsi plaintext* dan *dekripsiciphertext* mengguunakan *algoritma Vernamcipher* dan RC4, maka kunci yang sama perlu digunakan untuk *enkripsi* dan *dekrip*.

2. Secure Hash Algorithm (SHA)

SHA merupakan salah satu dari algoritma dari fungsi hash satu-arah(*one-way Algorithm*) yang dibuatoleh NSA dan dipublikasikan oleh NIST. *SHA* adalah perpanjangan dari MD5, yang dianggap tidak aman pada tahun 2005 karena kesalahan algoritmik yang menyebabkan kunci publik berbeda menghasilkan intisari pesan yang identik. Secara komputasi sulit bagi metode *SHA* ini untuk menemukan pesan yang cocok dengan intisari pesan yang disediakan. Dengan demikian, algoritma ini aman. Enam algoritma *SHA* yang telah dipublikasikan adalah *SHA-0, SHA-1, SHA-224, SHA-256, SHA-384,* dan *SHA-512* (Silalahi & Sindar, 2020). Tabel dengan beberapa algoritma *SHA* disediakan di bawah ini:

Tabel 2. 1 Algoritma SHA

Algoritma	**Ukuran messegedigest (bit)**	**Ukuran Blok pesan (bit)**	**Ukuran maksimal pesan (bit)**
SHA-0	160	512	2^{64}-1
SHA-1	160	512	2^{64}-1
SHA-256/224	256/224	512	2^{64}-1
SHA-512/384	512/384	1024	2^{128}-1

3. Cara Kerja Algoritma SHA

Algoritma ini bertujuan untuk menciptakan hak akses dari database berupa admin, author dan user yang diperbolehkan dalam mengakses sistemagar hak akses tersebut masuk dan dicek, terlebih dahulu Algoritma *Secure Hash Algorithm (SHA)* dirancang untuk menghasilkan nilai hash tetap panjang dari data input (Mary. et al., 2021). *SHA* bekerja dengan beberapa langkah pengolahan blok data, termasuk pengubahan bit, pergeseran bit, dan operasi logika. Proses ini dilakukan secara berulang hingga blok-blok data selesai diproses, menghasilkan nilai hash yang unik untuk setiap input. *SHA* memiliki beberapa varian, seperti *SHA-1, SHA-256, SHA-3,* yang berbeda dalam panjang hash dan kompleksitas algoritmanya (Syahputra et al., 2023).

Berdasarkan hasil penelitian (Aryasa & Paulus, 2015), mengatakan bahwa cara kerja algoritma *SHA* adalah sebagai berikut:

1. *Padding*: Pesan masukan dibagi menjadi blok-blok dengan ukuran tetap. Sebelum diproses, pesan sering kali diberi bantalan untuk memastikan pesan tersebut sesuai dengan persyaratan ukuran blok. Padding biasanya mencakup 1 bit diikuti dengan serangkaian angka nol dan panjang pesan asli dalam biner.

2. Nilai Hash Awal: Algoritme *SHA* menggunakan sekumpulan konstanta awal, yang sering disebut sebagai "IV" (Vektor Inisialisasi). IV ini telah ditentukan sebelumnya dan memberikan status awal untuk komputasi hash.
3. Perhitungan Intisari Pesan: Perhitungan hash berlangsung dalam serangkaian putaran. Setiap putaran melibatkan serangkaian fungsi logika dan operasi bitwise, termasuk bitwise AND, OR, XOR, dan bit yang berputar.
4. Komponen utama dari setiap putaran adalah: Ekspansi Pesan: Blok saat ini diperluas menjadi kumpulan kata yang akan digunakan dalam operasi selanjutnya.
5. Fungsi Kompresi: Kata-kata yang diperluas digabungkan dengan nilai hash saat ini dan diproses melalui serangkaian operasi bitwise.
6. Nilai *Hash* Akhir: Nilai hash yang dihasilkan dari pemrosesan setiap blok diperoleh. Nilai ini adalah string bit dengan panjang tetap, sering kali direpresentasikan sebagai angka heksadesimal.

Fungsi hash *SHA* dirancang dengan mempertimbangkan properti tertentu:

1. Deterministik: Untuk input yang sama, fungsi hash akan selalu menghasilkan nilai hash yang sama.
2. Komputasi Cepat: Algoritme *SHA* dirancang agar efisien secara komputasi sekaligus memberikan keamanan yang kuat.
3. Resistensi Preimage: Mengingat nilai hash, secara komputasi tidak mungkin untuk menentukan input asli.
4. Ketahanan Tabrakan: Tidak mungkin menemukan dua masukan terpisah yang menghasilkan nilai hash yang sama secara komputasi.

5. Efek Longsoran: Perubahan kecil pada input akan menghasilkan nilai hash yang berbeda secara signifikan.

SHA-1, SHA-256, SHA-384, SHA-512, dan varian lainnya merupakan bagian darii keluarga *SHA*. Meskipun *SHA-1* banyak digunakan di masa lalu, namun kini dianggap lemah karena kerentanannya, dan *SHA-256* serta variannya lebih aman dan umum digunakan untuk berbagai tujuan kriptografi, seperti tanda tangan digital dan verifikasi integritas data (Aryasa & Paulus, 2015).

2.3 Penelitian Terdahulu

Sejumlah sumber bahan analisis atau perbandingan tentunya harus dicantumkan di penelitian. berikut adalah beberapa jurnal penelitian sebelumnya:

1. Penelitian yang diselesaikan oleh Antika Lorient, Theophilus Wellem, di Universitas Kristen Satya Wacana tahun (2019) dengan judul "**Implementasi Sistem Otentikasi Dokumen Berbasis *Quick Response* (QR) *Code* dan *Digital Signature*"** (ISSN 2580-0760). Sebagai contoh, kertas sertifikat siswa diautentikasi menggunakan sistem otentikasi dokumen yang diterapkan. Dalam menghasilkan tanda tangan digital, diperlukan fungsi hash untuk menyusun inti pesan dari dokumen yang akan ditandatangani. Selain itu, pembuatan tanda tangan digital memerlukan suatu algoritma yang dapat mengenkripsi dan dekripsi serta menghasilkan kunci publik bisa juga privat. Pada penelitian ini, algoritma *Rivest-Shamir-Adleman* (RSA) digunakan untuk proses enkripsi/dekripsi dan pembuatan kunci publik dan privat. *Algoritma Hash Aman-256 (SHA-256)* digunakan sebagai fungsi hash. Tiga puluh sertifikat menjalani pengujian sistem (Lorien & Wellem, 2021).

2. Penelitian Hendra Handoko Syahputra Pasaribu, Sarbjit Singh Dhilon, Panji Dinata Galingging, Surya Syaputra, Somantri dengan judul "**IMPLEMENTATION SHA 512 BIT ON ROUTINGURL"** (ISSN/E-ISSN 1979-9292 / 2460-5611). Tujuan dari penelitian ini adalah untuk memastikan bahwa keamanan dan integritas data dapat ditingkatkan dalam sistem informasi dengan menggunakan *SHA-512* dalam perutean URL. Dengan menggunakan teknik hashing *SHA-512*, data pengguna yang disediakan melalui URL perutean pada dasarnya dienkripsi, sehingga mengurangi bahaya gangguan dan peretasan data. Analisis statistik yang melibatkan pengumpulan data dari sistem informasi sebelum dan sesudah *SHA-512* diimplementasikan pada URL perutean mendukung temuan ini. Informasi yang dikumpulkan mencakup serangan yang teridentifikasi, percobaan serangan siber, entri yang tidak disetujui, dan data yang diubah. Setelah itu, data ini diperiksa menggunakan teknik statistik terkait untuk menemukan perubahan penting pada sistem keamanan (Handoko et al., 2023).
3. Penelitian Andi Setiawan, Ade Irma Purnamasari, di STMIK IKMI Cirebon, dengan **"Implementasi *JSON Web Token* Berbasis Algoritma *SHA-512* untuk Otentikasi Aplikasi BatikKita"** (ISSN 2580-0760), Penelitian ini menggunakan pendekatan pengembangan perangkat lunak *Rapid Application Development (RAD)* dan teknik JSON Web Token (JWT) menggunakan HMAC SHA-512. Pengujian dilakukan pada dua arsitektur web service yaitu aplikasi BatikKita yang dikembangkan menggunakan platform web dan Android, serta Simple *Object Access Protocol (SOAP)* dan *Representational State Transfer*

(REST). JSON Web Token (JWT) dengan algoritma *HMAC SHA-512* digunakan untuk otentikasi. Dalam studi ini, dua arsitektur layanan web Simple *Object Access Protocol (SOAP)* dan *Representational State Transfer (REST)* diuji menggunakan *JSON Web Tokens (JWT)* dengan *HMAC SHA-256* dan *JSON Web Tokens (JWT)* dengan *HMAC SHA -384* algoritma sebagai perbandingan Hasil evaluasi (Setiawan & Purnamasari, 2020).

4. Penelitian Emanual A. Adeniyi, dkk pada tahun 2022 dengan judul "***Secure Sensitive Data Sharing Using RSA and Elgamal Cryptographic Algoritms With Has Function"*** Penelitian ini menggunakan algoritma kriptografi RSA dan ElGamal dengan penerapan *SHA-256* untuk formulasi tanda tangan digital guna meningkatkan keamanan dan memvalidasi pembagian informasi sensitif. Keamanan semakin menjadi tugas yang kompleks untuk dicapai. Tujuan dari penelitian ini adalah untuk mengaktifkan autentikasi data bersama dengan penerapan fungsi *SHA-256* pada algoritma kriptografi. Metodologi yang digunakan melibatkan penggunaan bahasa pemrograman C# untuk implementasi algoritma kriptografi RSA dan ElGamal menggunakan fungsi hash *SHA-256* untuk tanda tangan digital. Hasil percobaan menunjukkan bahwa algoritma RSA memiliki kinerja lebih baik dibandingkan ElGamal pada proses enkripsi dan verifikasi tanda tangan, sedangkan ElGamal memiliki kinerja lebih baik dibandingkan RSA pada proses dekripsi dan pembuatan tanda tangan (Adeniyi et al., 2022).
5. Penelitian Velmurugadas, S, Dhana Sekaran, S. Shasi Anan (2020) dengan judul "***Enhanching Blockhain Security In Cloud Computing With Lot Environment***

Using Ecies and Chryptografy Hash Algorithm" (E-ISSN 2214-7853). Hasil penelitian ini telah mengembangkan kerangka kerja baru yang akan memantau aktivitas yang terjadi pada bukti data tertentu, dengan membuat *Software Defined Network* (SDN) berbasis Cloud, yang terdiri dari 100 - Node seluler (perangkat IOT), saklar aliran terbuka dan pengontrol berbasis *Blockchain, server cloud, Server Otentikasi* (AS) dan penyelidik. Awalnya semua pengguna terdaftar di AS dan mendapatkan kunci rahasianya dari AS berdasarkan *Harmony Search Optimization* (HSO). Di node seluler, paket dienkripsi menggunakan algoritma *Elliptic Curve Integrated Encryption Scheme* (ECIES) dan ditransfer ke *server cloud*. Pengontrol SDN memelihara *blockchain* untuk menyimpan bukti yang dikumpulkan dari data dan tanda tangan pengguna berdasarkan Algoritma *Hash* Kriptografi *SHA-256*. Penyelidik yang berwenang melakukan proses berikut: identifikasi, pengumpulan bukti, analisis bukti, dan pembuatan laporan berdasarkan Grafik Logis Bukti (LGoE). kami memplot grafik yang dihasilkan untuk Waktu respons versus Jumlah pengguna, Waktu penyisipan bukti versus jumlah pengguna, Waktu verifikasi bukti versus Jumlah pengguna, *Overhead* komputasi versus jumlah pengguna, Tingkat perubahan total versus Jumlah pengguna, Waktu komputasi hash versus jumlah pengguna pengguna, Waktu pembuatan kunci versus jumlah pengguna, Waktu enkripsi versus jumlah pengguna dan Waktu dekripsi versus jumlah pengguna. Terakhir, investor atau badan hukum lainnya dapat memperoleh bukti dari pengontrol dan dikonstruksikan sebagai Grafik Bukti Logis (LGoE). Analisis eksperimental mengungkapkan fakta bahwa sistem yang diusulkan memperoleh kinerja yang

lebih baik dalam hal waktu respons, akurasi, peningkatan throughput, dan perubahan total parameter keamanan (Velmurugadass et al., 2020).

6. Penelitian Ferza Putra Utama, Gusman Wijaya, Revita Faurina, Arie Vatresia pada tahun 2019 dengan judul **"Implementasi Algoritma *AES 256 CBC, Base 64,* dan *SHA 256* Dalam Pengamanan dan Validasi Data Ujian Online "**(ISSN 2355-7699). Pengenkripsian data ujian dengan menggunakan teknik kriptografi merupakan salah satu cara untuk menjaga keutuhan hasil yang diperoleh dari ujian online. Dalam upaya menjaga dan menjamin keaslian data ujian online, penelitian ini menyarankan penggunaan sejumlah teknik kriptografi, antara lain algoritma *AES 256 CBC, Base 64*, dan *SHA 256*. Hasil penelitian ini adalah aplikasi ujian online berbasis web yang dikembangkan dengan teknologi *MERN Stack*. Nilai hash pada hasil pengujian validasi data ujian online yang dienkripsi dengan sistem dan *OpenSSL* adalah sama. Hal ini menunjukkan bahwa sistem berhasil mengenkripsi, mendekode, dan memvalidasi data ujian yang diperoleh secara online (Algoritma et al., 2023).

2.4 Kerangka Pemikiran

Tata cara penentuan kerangka pemikiran untuk analisis data dan menciptakan keamanan data teks menggunakan algoritma kriptograf SHA (*Secure Hash Algorithm*) dari pihak yang bersangkutan namun kurang efektif dan perlu adanya terobosan baru. Dari kerangka pemikiran berikut uraiannya:

Gambar 2. 5 Kerangka Pemikiran
Sumber: (Data penelitian, 2023)