BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada masa modern sekarang, teknologi informasi juga mengalami kemajuan yang signifikan, dan salah satu bentuk kemajuan teknologi informasi ialah *website* yang terhubung oleh *web service*. *Web service* atau layanan *web* merupakan sistem yang terdiri dari berbagai fungsi dan metode yang tersimpan pada suatu *server* dan dapat diakses oleh pengguna dengan sistem arsitektur aplikasi yang berbeda secara *remote* (Ardiansyah dkk., 2023).

Dengan terus majunya perkembangan teknologi, tidak selalu menghasilkan sesuatu yang positif. Dengan pesatnya perluasan pada bidang teknologi informasi di seluruh dunia juga diiringi oleh tingginya faktor risiko penyalahgunaan dan serangan terkait keamanan informasi yang dapat dilakukan oleh berbagai cara dan dilakukan oleh peretas (Amalia dan Nasution, 2024). Keamanan informasi di bidang informasi digital yang terus berkembang memerlukan sistem keamanan yang kuat dan tidak bisa diabaikan, dan kerentanannya memerlukan perhatian kritis (Setyowardhani dkk., 2024). Tujuan dari dibentuknya proses keamanan data adalah untuk melindungi suatu informasi yang telah disimpan, diterima, dikirim, atau dikumpulkan yang mana setiap proses tersebut suatu data atau informasi itu harus dilindungi (Wulandari dan Hwihanus, 2023).

Urgensi keamanan data atau informasi pada suatu *web service* menjadi hal yang perlu diberikan perhatian khusus. Faktor keamanan dalam suatu hubungan antara *client* atau pengguna dengan *server web service* itu belum tentu tejamin keamanannya, yang mana aspek keamanan ini sangat penting agar informasi data yang tersimpan tidak disalahgunakan atau diakses oleh sembarang pihak (Muzakir, 2013). Salah satu urgensi keamanan yang perlu diperhatikan pada *web service* yaitu serangan XSS, SQL *Injection*, *Brute Force Attack*, dan *Man In The Middle* jenis *Sniffing*. Beberapa serangan tersebut memberikan serangan dengan tingkat bahaya yang berbeda dimana *Man In The Middle* memiliki tingkat persentase serangan

tertinggi sebesar 85%, sedangkan XSS 45%, SQL *Injection* 75% dan *Brute Force Attack* 80% (Arnaldy dan Perdana, 2019). Hal inilah yang membuat penelitian ini akan berfokus pada serangan *web service* yaitu *Man In The Middle*.

Serangan *Man In The Middle Attack* (MITM) ini adalah kegiatan atau aktivitas dengan teknik melakukan penyerangan pada sisi keamanan, yang mana penyerang ini merupakan orang yang berada di tengah-tengah komunikasi yang dapat dengan bebas mendengarkan bahkan mengubah suatu pesan yang disampaikan (Zulkarnain, 2020). Ada beberapa teknik MITM salah satunya yaitu *Sniffing*. *Sniffing* merupakan suatu teknik yang digunakan oleh pihak tak berwenang, dimana mereka melakukan tindakan kejahatan berupa pencurian dan pengambilan suatu data sensitif dengan pemantauan pertukaran *packets* dalam suatu jaringan (Manguling dan Parenreng, 2023).

Terdapat beberapa cara pencegahan yang dapat dilakukan terkait penyerangan pada *web service Man In The Middle Attack* (MITM). Proses pencegahan yang disarankan diantara lain dengan proses enkripsi. Enkripsi adalah kegiatan yang merubah bentuk informasi yang dapat dipahami dengan mudah oleh seseorang ke bentuk kode yang akan sulit dipahami. Terdapat beberapa penerapan enkripsi yang dapat digunakan antara lain penggunaan SSL, penggunaan SSH, dan *End To End Encryption* (E2EE) untuk mencegah serangan MITM (Wulandari dan Hwihanus, 2023).

Dengan menerapkan *End To End Encryption* merupakan cara yang sangat efektif pada kasus melindungi transmisi pesan digital, kerahasiaan informasi, perlindungan dan privasi suatu informasi. Dari beberapa penerapan yang dapat digunakan, penelitian ini akan menitikberatkan pada *End To End Encryption* (E2EE) yang merupakan proses pertukaran informasi yang dilakukan dengan aman dari pengirim ke penerima dengan melakukan proses enkripsi selama proses pertukarannya yang menyebabkan informasi tidak dapat diakses dan diubah oleh pihak ketiga yang tidak berwenang (Maharani dkk., 2023).

Karena penelitian ini ingin menggunakan E2EE, maka perlu menetapkan suatu algoritma untuk enkripsinya. Terdapat beberapa algoritma enkripsi yang dikenal antara lain, DES (*Data Encryption Standard*), *Blowfish*, IDEA

(*International Data Encryption Algorithm*), dan AES (*Advanced Encryption Standard*). Dimana dari berbagai algoritma enkripsi tersebut menunjukkan bahwa AES merupakan algoritma terbaik dari kecepatan melakukan proses enkripsi dan proses dekripsinya dimana urutan kecepatan algoritma tersebut dari tercepat yaitu AES, *Blowfish*, DES, dan IDEA (Meko, 2018). Oleh karenanya, penelitian ini akan menggunakan algoritma AES sebagai algoritma enkripsi pada sistem *End To End Encryption* yang ingin diterapkan.

Berdasarkan pemilihan algoritma yang telah dipilih, *Advanced Encryption Standard* (AES) terdapat beberapa jenis yang dibedakan berdasarkan jumlah bit yang digunakan yaitu 128 bit, 192 bit dan 256 bit. AES adalah suatu algoritma dalam Kriptografi yang dikerjakan pada *blok cipher* yang menggunakan berbagai teknik seperti substitusi, permutasi dan rotasi pada setiap putaran di setiap blok yang akan dilakukan enkripsi dan dekripsi. AES 128 bit ini akan memiliki panjang kunci sebanyak 128 bit dengan jumlah proses sebanyak 10 putaran (Luqman dkk., 2022). AES 128 merupakan salah satu algoritma untuk mengamankan data yang teraman dengan percobaan serangan secara *Brute Force Attack* maka memerlukan sekitar 1 milliar tahun untuk memecahkan kode enkripsi nya (Basatwar, 2023).

Berdasarkan beberapa fenomena yang telah dijelaskan pada paragraph-paragraf sebelumnya, maka diperlukan suatu sistem keamanan yang mendukung dalam mengatasi urgensi keamanan data dari serangan MITM pada *web service*. Menurut Yaomulfurqqan dan Pramusinto (2023) juga menyatakan jika penerapan AES pada keamanan data suatu *website* sangat tepat karena penggunaannya yang fleksibel dalam pengaksesan dan penggunaannya.

Oleh karena itu, maka penulis penelitian ingin melakukan penelitian pada pencegahan serangan keamanan yang dapat terjadi pada *website* terutama pada *service* mendapatkan seluruh data pasien untuk diterapkan enkripsi dengan *End To End Encryption* pada sisi *Web Service* (*Server Backend*) dan *Web Client* (Server Frontend).

1.2 Rumusan Masalah

Setelah memuat beberapa fenomena pada latar belakang yang telah dijelaskan pada subbab sebelumnya, maka pada penelitian ini merumuskan dan memfokuskan pokok masalah yang akan dikerjakan selama kegiatan penelitian ini berlangsung, yaitu bagaimana efektivitas penerapan *End To End Encryption* dengan AES 128 bit dalam mengatasi serangan keamanan *Man In The Middle Attack* dengan serangan *Sniffing*?

1.3 Batasan Masalah

Agar penelitian lebih terfokus sesuai dengan apa yang ingin dicapai, maka perlu ditetapkan batasan masalah pada penelitian ini yang mana batasan masalah bertujuan untuk membatasi bidang dan cakupan penelitian yang akan diteliti. Berikut beberapa batasan masalah pada penelitian ini :

1. Kegiatan penelitian ini hanya memfokuskan pada salah satu jenis serangan *Man In The Middle Attack* yaitu *Sniffing*.
2. Penelitian ini membatasi *service* dari *web* yang ingin diterapkan yaitu pada *service* pengambilan data.
3. Penelitian ini akan menggunakan *website dummy* yang dibuat untuk melakukan simulasi serangan.
4. Penelitian ini tidak mencakup evaluasi performa sistem secara umum.
5. Implementasi atau penerapan sistem akan dibuat dengan bahasa pemrograman Javascript dan beberapa library seperti Burp Suite, ExpressJS, CryptoJS, Prisma.io, dan PostgreSQL.

1.4 Tujuan Penelitian

Dilakukannya penelitian ini bertujuan untuk menganalisis, meneliti dan mengimplementasikan mekanisme atau sistem dalam pencegahan serangan keamanan pada *web service* yaitu *Man In The Middle Attack* dengan jenis *Sniffing* menggunakan *End To End Encryption* yang menerapkan Algoritma *Advanced Encryption Standard* (AES) dengan 128 bit dalam proses pertukaran data atau

informasi dari *Web Service* (*Server Backend*) dan *Web Client* (*Server Frontend*) yang ada pada *website*.

1.5 Manfaat Penelitian

Mengenai manfaat penelitian yang menjadi nilai dalam penelitian yang dilakukan ini baik untuk peneliti, dan pembaca baik itu dalam segi teoritis ataupun praktis, berikut kajian manfaat penelitian yang dihasilkan dari penelitian ini :

1. Manfaat secara Teoritis
   a. Berkontribusi terhadap ilmu pengetahuan dalam penerapan sistem keamanan untuk pencegahan serangan yang dapat terjadi pada pertukaran informasi atau data.
   b. Menambah wawasan literatur bagi peneliti maupun pembaca penelitian ini terkait pentingnya keamanan data dan bagaimana cara mengamankan data informasi tersebut.
   c. Membantu mendalami kajian ilmu terkait pencegahan serangan pada *web service* dengan penerapan sistem keamanan dan metode enkripsi.

2. Manfaat secara Praktis
   a. Memberikan wawasan cara mengimplementasikan keamanan informasi atau data pada saat pertukaran informasi antara *web service* dan *client*.
   b. Menambah pengetahuan terkait kegiatan penyerangan yang dilakukan dengan metode MITM dengan jenis *Sniffing* untuk mendapatkan suatu informasi atau data dari *web service*.
   c. Mengetahui cara penerapan AES 128 sebagai metode enkripsi suatu informasi atau data.

1.6 Sistematika Penulisan

Proses penulisan tugas akhir ini dilakukan secara sistematis. Berikut adalah langkah-langkah yang diikuti dalam menyusun skripsi ini:

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II KAJIAN LITERATUR

Pada bab ini menjelaskan tentang penelitian-penelitian terdahulu, konsep, dan teori yang pernah digunakan dalam studi kasus dan metode yang sama.

BAB III METODE PENELITIAN

Pada bab ini menjelaskan tentang fokus dan lama penelitian bahan atau materi penelitian, jenis data yang digunakan, alat pengumpulan data, alat atau instrumen penelitian, kerangka penelitian, pengumpulan data, serta analisa dan perancangan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini membahas tentang pengujian dan pembahasan dari apliksai yang akan dibangun.

BAB V PENUTUP

Pada bab ini membahas mengenai kesimpulan dan saran dari hasil penelitian.

DAFTAR PUSTAKA

Pada bagian ini berisikan sumber-sumber yang digunakan untuk pendukung pada kajian literatur.