BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dewasa ini, teknologi merupakan salah satu hal yang tidak terlepaskan dalam kehidupan masyarakat. Salah satu bentuk dari perkembangan teknologi adalah *word processor* yang merupakan alternatif modern terhadap mesin tik yang hanya memiliki penyimpanan menggunakan *magnetic tape* [1]. *Word processor* merupakan program atau perangkat lunak pada komputer yang mampu membuat, menyimpan, dan menyetak sebuah dokumen teks [2]. Umumnya, *word processor* menawarkan *graphical user interface* yaitu *"what you see is what you get"* atau apa yang anda lihat adalah apa yang anda dapat [3].

Sejalan dengan pernyataan sebelumnya, *word processor* pada mulanya hanya dapat bekerja secara *offline* dan berkembang hingga menjadi *online word processor*. Salah satu contoh dari *online word processor* adalah Google Docs. Google Docs merupakan *online word processor* yang dikembangkan oleh Google yang memungkinkan pengguna untuk membuat atau memformat dokumen serta dapat bekerja atau berkolaborasi dengan orang lain [4]. Google Docs sendiri dapat diakses melalui *website* dan *smartphone* melalui aplikasi dengan sistem operasi berbasis Android maupun IOS.

Berdasarkan pernyataan sebelumnya, Google Docs dapat diakses melalui teknologi dari perkembangan internet yaitu *website*. *Website* merupakan kumpulan halaman yang menampilkan berbagai macam informasi seperti teks, gambar, video, animasi, dan lainnya baik bersifat statis atau dinamis yang terangkum menjadi satu domain atau subdomain [5]. Dengan terhubungnya *website* dengan internet diperlukan penjagaan keamanan informasi dari sebuah *website*. Hal ini didukung dengan maraknya pencurian data atau dokumen pribadi yang ditunjukkan pada tahun 2023 telah diduga terjadi lebih dari 400 juta pencurian data pribadi oleh *hacker* [6]. Salah satu tindakan untuk menjaga keamanan data pribadi adalah dengan pemberian kata sandi atau *password* [7]. *Password* atau kata sandi merupakan serangkaian karakter yang terdiri dari huruf maupun angka untuk melakukan otentikasi ke dalam sistem komputer [8]. Perusahaan sekuritas digital milik Inggris yaitu LockLizard mengatakan Google Docs tidak disarankan untuk digunakan untuk menyimpan data yang bersifat sensitif salah satu faktornya

dikarenakan Google Docs saat ini tidak memiliki alat *built-in password* [9].

Sejalan dengan pernyataan sebelumnya, Adelson et al. menyebutkan bahwa pemberian *password* diperlukan namun pemberian *password* saja tidak cukup dikarenakan cukup rentan untuk disadap dengan berbagai cara [10]. Berdasarkan hal tersebut, diperlukan keamanan berlapis setelah pengguna memasukkan *password* yaitu *two factor authentication* [11]. *Two factor authenticaton* (2FA) adalah metode keamanan yang memerlukan 2 langkah otentikasi yang berbeda untuk melakukan verifikasi pengguna sebelum diberikan akses ke dalam sistem [12]. Dalam 2FA, terdapat beragam metode yang dapat digunakan salah satunya adalah *one time password* (OTP) dan *Security Question* [12]. Pada penerapannya *security question* dalam menangani pembobolan penyerang memiliki peluang sebesar 6.9 persen hingga 14.6 persen [13]. Dibandingkan dengan *security question*, *One time password* dengan 6 buah karakter yang mengandung huruf dan angka jika dilakukan serangan *brute force* memiliki probabilitas sebesar 0.000000991 untuk dapat dibobol [14].

One time password (OTP) merupakan proses otentikasi dari server yang menggunakan kode dinamis yang akan berubah pada rentang waktu tertentu [15]. Selain 2FA terdapat algoritma kriptografi yang membantu dalam melakukan enkripsi data. Salah satu algoritma kriptografi yaitu *Advanced Encryption Standard* (AES). Dalam jurnalnya yang berjudul "*A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security*", Sivakumar dkk menyimpulkan bahwa AES unggul dibandingkan *Data Encryption Standard* (DES) dan *Triple Data Encryption Standard* (3DES) dalam segi kecepatan, *throughput*, panjang kunci, putaran dan ukuran blok [16]. Sejalan dengan pernyataan sebelumnya, Youssouf dkk menyebutkan bahwa algoritma AES unggul dalam hal keamanan dibandingkan dengan DES, Carlisle Adams and Stafford Tavares (CAST-128), dan Blowfish setelah dilakukan beberapa percobaan *attack* [17]. Penggabungan metode OTP dan algoritma AES memiliki waktu enkripsi dan dekripsi yang lebih cepat serta memiliki tingkat perbedaan yang signifikan dari pengujian Avalanche Effect dibandingkan dengan penggabungan OTP dengan algoritma Blowfish [18].

Berdasarkan permasalahan yang telah diuraikan sebelumnya, penggabungan metode OTP dan enkripsi AES dapat menjaga keamanan dari isi milik dokumen pengguna. Dengan hal tersebut maka diimplementasikan metode Two Factor Authentication berupa OTP dan algoritma AES ke dalam *online word processor* yang dibangun. Program yang diimplementasikan dibangun dengan menggunakan bahasa pemrograman JavaScript dan PHP serta menggunakan *framework* React dan

Laravel serta berbagai *library* yang dibutuhkan.

1.2 Rumusan Masalah

Berdasarkan permasalahan yang telah dijelaskan sebelumnya pada latar belakang, berikut adalah beberapa rumusan masalah yang ingin dipecahkan dalam penelitian ini,

1. Bagaimana mengimplementasikan *Two Factor Authentication* dan algoritma *Advanced Encryption System* (AES) dalam menjaga keamanan *online word processor* yang dibangun?
2. Bagaimana hasil dari percobaan *brute force attack* dan pengujian Avalanche Effect pada hasil implementasi yang dilakukan?

1.3 Batasan Permasalahan

Pada penelitian ini terdapat beberapa batasan masalah dalam pengembangan sistem, beberapa diantaranya:

1. Metode 2FA yang digunakan adalah OTP melalui *email*.
2. *Online word processor* hanya bisa menerima *alphanumeric* (huruf dan angka).

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah yang telah dirumuskan sebelumnya terdapat beberapa tujuan yang diharapkan untuk memecahkan berbagai permasalahan tersebut, yaitu:

1. Mengimplementasikan *Two Factor Authentication* dan algoritma *Advanced Encryption Standard* (AES) pada *online word processor* yang dibangun.
2. Mendapatkan hasil *brute force* dan pengujian Avalanche Effect yang maksimal untuk memastikan tingkat keamanan dari hasil implementasi yang dilakukan.

1.5 Manfaat Penelitian

Dari penelitian yang dilakukan dapat memberikan manfaat bagi beberapa pihak, yaitu:

1. Bagi pengguna, antara lain.
   (a) Isi pada dokumen pengguna yang disimpan dilindungi oleh 2FA dan juga terenkripsi menggunakan AES.
   (b) Risiko kebocoran data berkurang.
2. Bagi pengelola, antara lain.
   (a) Mendapatkan kepercayaan pengguna dikarenakan data dokumen dapat terjaga dengan baik.

1.6 Sistematika Penulisan

Berikut merupakan sistematika penulisan yang digunakan dalam proses penyajian laporan skripsi atau tesis ini.

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Bab ini merupakan Bab pendahuluan yang berisi Latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian, serta sistematika penulisan.
- Bab 2 LANDASAN TEORI
  Bab ini berisi terkait penjelasan teori-teori algoritma dan teknologi serta konsep dasar yang digunakan dalam mendukung penelitian terkait permasalahan yang ingin dipecahkan, meliputi penjelasan terkait *Advanced Encryption Standard* (AES), *Two Factor Authentication* (2FA), dan *Web socket*.
- Bab 3 METODOLOGI PENELITIAN
  Bab ini meliputi metodologi penelitian yang digunakan dan percangan sistem yang terdiri dari *requirements*, *flowchart*, *database schema*, struktur tabel pada *database*, dan *rancangan UI yang ingin dibangun*.

- Bab 4 HASIL DAN DISKUSI

  Bab ini berisi tentang hasil implementasi algoritma dan metode yang diimplementasikan ke dalam sistem yang dibangun menggunakan algoritma *Advanced Encryption Standard* (AES) dan *Two Factor Authentication* (2FA) yang digunakan untuk memperkuat keamanan sistem pada sistem yang dibangun.

- Bab 5 KESIMPULAN DAN SARAN

  Pada bab ini berisi tentang hasil penelitian atau analisis terhadap sistem yang dibangun untuk mencapai tujuan penelitian yang dituju serta saran terhadap hal yang dapat dikembangkan di masa yang akan datang.