BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir, popularitas *cloud* telah meningkat secara signifikan, menarik perhatian sejumlah besar pengguna internet. *Cloud computing* adalah sebuah model yang memungkinkan akses yang nyaman dan *on-demand* ke sumber daya komputasi yang dapat dikonfigurasi dan diandalkan. Hal ini juga dapat diartikan sebagai sebuah jaringan *real-time* yang dapat terhubung ke berbagai perangkat, seperti komputer, ponsel pintar, atau tablet, termasuk setiap perangkat yang memiliki alamat *MAC* yang valid dari adapter jaringan yang telah terintegrasi. (Pitchay et al., 2016). *Cloud* dapat diimplementasikan dalam berbagai arsitektur dan layanan dengan menggunakan pendekatan desain perangkat lunak yang beragam. Model layanan yang diterapkan pada *cloud* mencakup *infrastructure as a service* (IAAS), *platform as a service* (PAAS), dan *software as a service* (SAAS).

Menurut (Pitchay et al., 2016) Salah satu keunggulan utama dari *cloud* terletak pada kemampuannya untuk menyediakan aplikasi dan ruang penyimpanan sebagai layanan melalui internet dengan biaya yang rendah atau bahkan tanpa biaya. Pengguna tidak perlu menggunakan mesin berkinerja tinggi, karena aplikasi *dihosting* di *cloud*, dan komputer hanya perlu menampilkan *output* dari apa yang dihasilkan oleh aplikasi tersebut. Dan jika disimpulkan, Seluruh faktor ini menyediakan solusi yang sangat menguntungkan bagi pengguna perorangan maupun pemilik bisnis, baik yang berskala kecil maupun besar. Pengguna juga memiliki kontrol penuh terhadap aplikasi dan data mereka, yang dapat diakses dari mana saja dan kapan saja melalui koneksi internet.

Namun, Akibat dari intensitas penggunaan layanan *cloud* yang tinggi, tantangan keamanan terhadap data pengguna semakin kompleks. Dalam konteks jaringan yang luas seperti ini, terdapat potensi tinggi terjadinya kehilangan data

atau serangan ke dalam jaringan langsung, yang dapat meningkatkan risiko terhadap kehilangan, eksploitasi dan kerusakan data

Dalam laporan keamanan siber oleh *palo alto networks* yang memberikan gambaran lengkap tentang situasi keamanan dalam *cloud computing*. Terdapat laporan "*Alerts by MITRE Tactic*" yang mengelompokkan peringatan berdasarkan taktik MITRE, seperti *"Initial Access*", "*Discovery*", dan "*Credential Access*". Hal ini memberikan wawasan tentang metode umum yang digunakan oleh penyerang. Terdapat juga diagram lingkaran "*Open Incidents by Severity*" yang menunjukkan jumlah insiden terbuka dalam 30 hari terakhir, dikategorikan berdasarkan tingkat keparahan (tinggi, sedang, rendah). Yang dapat disimpulkan bahwa ada berbagai serangan terhadap komunikasi data yang melibatkan taktik akses awal, pengembangan sumber daya, pengelakan pertahanan, dan eskalasi hak istimewa. Tren ini menunjukkan bahwa penyerang terus mengeksploitasi kelemahan dalam jaringan untuk mendapatkan akses dan melakukan serangan lebih lanjut.

Upaya untuk melindungi data pengguna juga melibatkan aspek keamanan selama proses transfer data dan penyimpanan data. Skema keamanan yang sudah ada biasanya terbatas pada aspek keamanan penyimpanan data dan kurang mempertimbangkan potensi penetrasi yang dapat terjadi selama transfer data. (Hidayat & Mahardiko, 2020)., Selain itu, dalam sistem yang sudah ada, terkadang pihak auditor ketiga diberikan akses untuk melihat data pengguna. Hal ini yang dapat menimbulkan ancaman yang signifikan karena potensi bagi hacker untuk menyamar sebagai pihak ketiga. (Akhil et al., 2018).

Pada akhirnya, model *cloud* belum dapat dianggap sebagai model yang sepenuhnya aman karena adanya berbagai isu dan tantangan didepan untuk melindungi data yang disimpan di *cloud* (Surv et al., 2015). Untuk itu diperlukan sebuah mekanisme yang cukup terbukti ampuh dalam mengatasi permasalahan diatas. Menurut (Fajrin, 2014) selain pengamanan pada level aplikasi dibutuhkan juga pengamanan pada level jaringan, selain data yang sedang ditransfer berhasil diamankan melalui proses enkripsi, perlu adanya perlindungan pada jalur komunikasi data. Komunikasi data dalam jaringan komputer terjadi pada lapisan

TCP/IP, dan untuk mengamankan jalur ini, *Transport Layer Security* atau *TLS* dapat digunakan. Yang mana *TLS* beroperasi melalui tiga tahap, dimulai dengan tahap pertama di mana server dan klien berkomunikasi untuk menentukan sistem enkripsi yang akan digunakan. Selanjutnya, pada tahap kedua, terjadi pertukaran kunci data untuk proses enkripsi, di mana kunci yang digunakan adalah kunci publik. Tahap terakhir melibatkan pengiriman pesan dengan menggunakan kunci enkripsi yang telah ditetapkan sebelumnya.

Lalu menapa perlu sebuah model pengamana pada *level transport di layer OSI* atau pada proses transmisi data sebagai bahan pertimbangan usulan? Merujuk pada penelitian (Rani & Jethi, 2020) Sebuah *Private Tunnel* adalah bentuk jaringan yang menciptakan jalur aman di atas jaringan yang kurang aman, seperti internet. Melalui jalur pribadi ini, data dapat ditransfer dan komunikasi dapat terjadi melalui jaringan publik, memungkinkan pengguna untuk mengirim dan menerima data melalui jaringan yang kurang aman atau jaringan publik. *Private Tunnel* dibuat dengan memelihara koneksi *virtual* dari satu titik ke titik lainnya (dari sumber ke tujuan) dengan menggunakan sirkuit dedikasi atau dengan menerapkan protokol *tunneling* melalui jaringan yang telah dijaga sebelumnya.

Terakhir kenapa memerlukan *AES*-128 sebagai metode enkripsi yang diusulkan? Berdasarkan *literatur review* yang penulis lakukan pada proses penulisan usulan penelitian ini, cukup banyak topik bahasan mengenai keandalan *AES*-128 jika diimplementasikan pada keamanan data disebuah sistem. Bahkan pada rujukan penelitian. (Hidayat & Mahardiko, 2020) yang merupakan sebuah penelitian dengan metode *SLR (Semantic Literatur Review)* menarik sebuah keseimpulan bahwasanya Algoritma *AES* sering digunakan untuk melindungi data dengan melakukan proses enkripsi. Pemilihan algoritma ini didasarkan pada tingkat keamanannya yang lebih tinggi dibandingkan dengan algoritma lain. *AES* sendiri dapat dijelaskan sebagai suatu metode enkripsi blok simetris, yang seluruh operasi dalam algoritma ini beroperasi pada data dengan panjang 8-bit atau lebih. Dengan blok *cipher* yang akan mengambil teks biasa (*plaintext*) dengan ukuran 128-bit, 192-bit, dan 256-bit, dan kunci yang digunakan untuk melakukan enkripsi

dan dekripsi diilustrasikan sebagai matriks persegi *byte* melalui 10 iterasi kunci yang berbeda. Sehingga kecil sekali kemungkinan untuk dapat dilakukan *bruteforce*.

Oleh karena itu, penelitian ini bertujuan untuk dapat mengidentifikasi dan mengatasi isu-isu keamanan tersebut melalui pengembangan mekanisme keamanan yang efektif, serta melibatkan enkripsi data dan pengamanan komunikasi dengan menggunakan saran pengembangan *tunnel* aman, pemanfaatan *TLS*, protokol *FTP* dan algoritma *AES* 128.

1.2 Rumusan Masalah

Dari latar belakang yang telah dipaparkan diatas, maka bisa di tarik beberapa rumasan masalah yang akan menjadi tujuan pada proposal penelitian ini:

1. Bagaimana sebuah mekanisme *private tunnel* dapat mengamankan transmisi data pada *cloud Storage*?
2. Bagaimana sebuah algoritma *AES*-128 dapat menjadi solusi dalam keamanan dan integritas data pada saat transmisi data terjadi?

1.3 Batasan Masalah

Dari konteks latar belakang proposal dan perumusan masalah, sejumlah batasan penelitian dapat diidentifikasi untuk membatasi cakupan penelitian. Beberapa di antaranya adalah:

1. Penelitian ini menggunakan data berbasis teks sebagai bahan uji.
2. Penelitian ini menggabungkan beberapa teknologi sebagai pengamanan ekstra, hal ini merujuk pada sebuah skema dasar dari sistem dan standar keamanan internasional.
3. Penelitian ini akan menggunakan data sampel sebagai bahan uji, dikarenakan data yang bersifat rahasia tidak dapat dijabarkan secara gamblang pada penelitian ini.
4. Penelitian ini tidak melibatkan beberapa hal sebagai acuan hasil, diantaranya adalah layanan *cloud* komersil.

1.4 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang telah dijabarkan, terdapat dua tujuan utama dalam penelitian ini:

1. Mengimplementasikan algoritma *AES*-128 sebagai solusi untuk meningkatkan tingkat keamanan dan integritas data pada saat transmisi data terjadi dalam proses pertukaran data.
2. Menganalisis dan mengevaluasi kinerja mekanisme *tunnel* aman serta implementasi algoritma *AES*-128 dalam konteks keamanan data pada layanan *cloud*.

1.5 Manfaat Penelitian

Berikut adalah beberapa manfaat dari hasil penelitian yang diharapkan oleh penulis:

1. Manfaat untuk Penulis, diharapkan memperoleh pemahaman yang lebih mendalam mengenai keamanan data dalam konteks *Private cloud Storage*, serta keterampilan dalam merancang dan mengimplementasikan solusi keamanan yang efektif.
2. Manfaat untuk Pembaca, diharapkann pembaca dapat mengaplikasikan pengetahuan ini dalam lingkup kerja atau penelitian mereka sendiri dan menyempurnakan rancangan ini terkait keamanan data dan *Private cloud Storage*.