BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah

Perkembangan teknologi *Internet of Things* (IoT) telah memberikan kontribusi besarterhadap kemajuan masyarakat modern dengan menghubungkan berbagai perangkat dan sistem ke jaringan internet [1]. Namun, keuntungan dari konektivitas yang luas ini juga membawa risiko keamanan yang serius, terutama terkait dengan kerentanan data sensitif yang dikirim melalui jaringan yang rentan terhadap serangan penyadapan.

Kebocoran komunikasi data IoT pada *smart home* dapat terjadi karena beberapa faktor. Salah satunya adalah kurangnya keamanan data pada IoT. Data ini berupa text yang merupakan informasi penting yang tidak boleh dilihat oleh siapa pun tanpa izin. Selain itu, kebanyakan perangkat IoT *smart home* mengumpulkan data pribadi pengguna, seperti gaya hidup, perilaku, dan informasi keberadaan. Namun, yang perlu diperhatikan adalah bagaimana data ini diamankan dan dikelola untuk menjaga privasi pengguna. Selain itu, keamanan komunikasi juga menjadi masalah penting dalam IoT. Oleh karena itu, perlu dikembangkan solusi teknologi yang menjaga privasi dan keamanan perangkat IoT untuk mencegah kebocoran komunikasi data IoT pada smart home.

Keamanan data menjadi hal yang sangat penting pada saat ini karena untuk setiap pengambilan keputusan, kebijakan harus berdasarkan data. Banyak data yang bersifat informasi penting dan terbatas untuk diketahui pihak yang terkait saja [2]. Data-data ini dapat digunakan oleh penyerang untuk melakukan kejahatan, seperti pencurian identitas, penipuan, atau penyalahgunaan data. Contoh data pribadi dan sensitif yaitu seperti, data identitas pengguna, data lokasi pengguna, dan data aktivitas pengguna.

Penggunaan steganografi berbasis ZWSP (*Zero Width Space*) *characters* yang memungkinkan penyembunyian data sensitif ke dalam pesan teks/carrier atau komunikasi tanpa menimbulkan kecurigaan, dapat memberikan solusi yang efektif untuk melindungi integritas dan kerahasiaan data yang dikirim melalui jaringan IoT

. Dengan menggunakan teknik ini, informasi rahasia dapat disembunyikan secara tidak terlihat di dalam komunikasi data biasa, sehingga hanya penerima yang dituju yang dapat mendekripsi dan mendapatkan akses ke data asli. Dengan mempertimbangkan kerentanan kebocoran komunikasi data IoT saat ini, perlindungan data sensitif menggunakan steganografi berbasis ZWSP characters menunjukkan potensi yang signifikan dalam mengatasi tantangan keamanan yang terkait dengan pertukaran informasi rahasia di era digital yang terhubung secara luas saat ini. Dengan demikian, penelitian tentang teknik ini diharapkan dapat memberikan kontribusi penting dalam menjaga keamanan dan integritasdata dalam lingkungan IoT yang semakin terkoneksi.

1.1.1 Analisa Masalah

Berikut ini beberapa aspek dalam dalam implementasi Perlindungan Komunikasi Data Sensitif pada IoT:

1.1.1.1 Aspek Keamanan

Perangkat IoT mengirim dan menerima data melalui jaringan. Serangan terhadap komunikasi jaringan dapat mencakup sniffing data, jika perangkat IoT tidak diotentikasi denganbaik, maka dapat mengakibatkan kebocoran data.

1.1.1.2 Aspek Industri

Keamanan IoT sering kali melibatkan berbagai pemangku kepentingan,termasuk produsen perangkat, penyedia jasa, dan pengguna. Kerjasama di seluruh industri untuk mengembangkan standar keamanan dan pembaruan perangkat lunak dapat membantu mengatasi masalah keamanan dengan cara yang lebih ekonomis.

1.1.1.3 Aspek Hukum

Hukum mengatur tanggung jawab hak individu atas data pribadi, hukum privasi datamemberikan hak kepada individu untuk mengakses, mengkoreksi, dan menghapus data olehmereka yang dikumpulkan oleh perusahaan. Dan saat data sensitif yang dikumpulkan oleh perangkat IoT melintasi perbatasan negara, hal ini dapat memunculkan masalah hukum yangkompleks.

1.1.2 Tujuan Capstone

Tujuan dari dibuatnya capstone ini adalah sebagai berikut :

1) Membuat perlindungan komunikasi data menggunakan steganografi.

2) Mengembangkan Algoritma Steganografi Berbasis ZWSP Characters

1.2 Analisa Solusi yang Ada

Dalam penulisan dokumen ini kami telah menganalisa solusi yang sudah ada dalam kasus kebocoran komunikasi data sensitif. Solusi yang ada untuk keamanan komuikasi datasaatini untuk berbagai jenis file adalah dengan menerapkan metode enkripsi dan dekripsi menggunakan algoritma AES 256. Dengan menggunakan teknologi ini, keamanan komunikasi data dari setiap file, termasuk dokumen teks, gambar, video, dan format file lainnya, dapat diamankan secara efektif dan hanya dapat diakses oleh pihak yang berwenangmelalui penggunaan kunci enkripsi yang tepat[3].

Selain itu terdapat metode lainnya yang dapat digunakan yaitu VPN dengan metode Internet Protocol Security (IPSec), Implementasi Metode *Internet Protocol Security* (IPSec) secara efektif dengan memadukan *Virtual Private Network* (VPN) dapat menjadi solusi yangkokoh untuk mengamankan dan melindungi komunikasi data dalam jaringan, menjamin kerahasiaan, integritas, dan otentikasi data secara menyeluruh[4].