BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi berkembang dengan sangat cepat di dunia, terutama dibidang aplikasi yang sangat mempengaruhi pekerjaan manusia, aplikasi seperti komputer, ponsel dan lainnya memudahkan pekerjaan dalam mengintegrasikan data yang dikelola. Perusahaan dapat mengakses data yang sangat sensitif seperti informasi keuangan, rincian pengiriman dan juga data pelanggan, untuk mencegah pihak pihak yang tidak bertanggung jawab yang memperoleh keuntungan yang tidak sah dari data ini. Strategi enkripsi yang kuat dan Kebijakan akses yang tepat lah yang diperlukan, selain itu tehnik kriptografi dapat juga digunakan untuk mencegah data pelanggan dilihat oleh orang lain kecuali pengguna itu sendiri atau pengguna yang ditunjuk yang telah disetujui oleh kedua belah pihak (*Aprizald, A., Hasan, M.A., & Setiawan, D, 2023).*

Kebutuhan akan strategi enkripsi yang kuat adalah salah satu cara terbaik untuk melindungi informasi sensitif dari akses yang tidak sah. Dengan menerapkan teknologi enkripsi yang kuat, perusahaan logistik dapat mengamankan informasi mereka dari akses yang tidak diotorisasi, bahkan jika informasi tersebut diretas atau dicuri. Ketika data dienkripsi kunci yang digunakan untuk membuka file sama dengan yang digunakan untuk enkripsi, sehingga orang yang tidak bertanggung jawab tidak dapat membuka file dan membacanya (Feraldi, R., Khairuna, A., Hasan, M. A., Rezky, R., & Ramadhan, H. (2021).

Saat ini peretas bisa menyerang kapanpun dan dimanapun dengan menggunakan akun siapapun untuk mencoba mengakses sistem dan data, untuk itu perusahaan harus melindunginya dengan menghapus akses yang berlebihan yang berkaitan dengan sistem dan data. karyawan pun harus berperan aktif dalam melindungi data, jika menemukan sesuatu hal yang mencurigakan wajib melaporkan kecurigaan kepada management terkait. Teknologi yang digunakan untuk mengumpulkan dan mengirimkan data logistik sering menimbulkan resiko keamanan dan privasi sistem manajemen logistik karena akses yang tidak sah dan kurangnya Privasi (Ugochukwu, N.A.; Goyal, S.B.; Rajawat, A.S.; Islam, S.M.N.; He, J.; Aslam, M. 2022).

Untuk menghentikan kejahatan terutama *cybercrime* diperlukan Tindakan prefentif, detektif dan responsif yang melibatkan pihak terkait seperti Perusahaan, pemerintah dan Lembaga keamanan canggih seperti enkripsi data, *blockchain, firewall* dan monitoring kemanan yang dapat membantu mencegah serangan *cyber (Yuniarti, Dewi Rizka, Hafidz Fauzan Alfarizy, Zifron Siallagan and Moch. Whilky Rizkyanfi, 2023).*

Pada penelitian kali ini penulis akan membahas metode enkripsi yang sering digunakan pada Perusahaan yaitu tehnik AES (*Advanced Encription Standard*) yang diadopsi pertama kali oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001, dan merupakan algoritma kriptografi simetris yang digunakan untuk menjaga data di sistem komputer. AES menggunakan kunci simetris untuk enkripsi dan menjelaskan data berbasis *chipper block,* dengan ukuran mulai dari 128, 192, hingga 256, panjang kunci menentukan seberapa jauh pihak yang tidak berwenang dapat mengakses data dan semakin sulit mendeskripsikan data yang terenkripsi (*Sarce Joel, A., Abdussalaam, F., & Yunengsih, Y. (2023).*

Dengan memahami latar belakang ini, penelitian tentang strategi enkripsi informasi di perusahaan menjadi sangat relevan dan penting untuk dilakukan guna melindungi informasi sensitif dan mengurangi risiko penyalahgunaan informasi. Pada banyak kasus belakangan yaitu terkait penyalahgunaan data yang disebabkan karena minimnya keamanan baik data maupun akses pada sistem yang harus dibatasi penggunaannya. Yang mana pengguna hanya bisa mengakses sistem dan data yang dibutuhkan saja, kecuali pengguna memiliki alasan lain untuk tidak dibatasi dan harus sepengetahuan pihak management terkait.

1.2 Identifikasi Masalah

Penulis menentukan masalah penelitian berdasarkan latar belakang berikut:

1. Data pelanggan yang disimpan dalam bentuk *plaintext* rentan terhadap akses yang tidak sah baik secara *online* maupun *offline.*
2. Kebocoran data dapat terjadi melalui berbagai celah keamanan seperti peretasan, malware atau bahkan bisa terjadi karena kesalahan manusia.
3. Tantangan dalam memastikan sistem keamanan data tidak menghambat operasi bisnis logistik dan mendukung kelangsungan bisnis ditengah ancaman keamanan yang ada.

1.3 Perumusan Masalah

Berikut ini adalah perumusan maslah penelitian ini berdasarkan judul dan latar belakang:

1. Peneliti pada penelitian ini melihat di perusahaan PT Prima Multi Cipta Belum menggunakan metode enkripsi data.
2. Aplikasi yang digunakan oleh PT Prima Multi Cipta belum terintegrasi dengan pelanggan.
3. Kurangnya pemahaman terkait keamanan data dan bagaimana bersikap bijak dalam mengolah data.

1.4 Batasan Masalah

Berdasarkan rumusan masalah diatas maka batasan penelitian ini adalah sebagai berikut:

1. Peneliti akan fokus pada metode AES *(Advanced Encryption Standard)* untuk digunakan pada penelitian ini.
2. Peneliti akan menguji enkripsi pada volume data yang terbatas yaitu data 3 cycle pengiriman untuk simulasi pengujian.
3. Penelitian ini akan fokus pada enkripsi data pelanggan yang terdapat di database dan tidak termasuk enkripsi pada aplikasi.

1.5 Tujuan Penelitian

Tujuan dari penelitian ini dibuat adalah:

1. Mengevaluasi efektifitas penerapan enkripsi data dalam mencegah kebocoran data pada Perusahaan.
2. Mencegah akses ilegal ke data pelanggan baik secara online maupun offline
3. Melindungi data sensitif, mencegah penyalahgunaan dan memastikan sistem keamanan data yang digunakan tidak menghambat operasi bisnis Perusahaan logistik dan dapat mendukung kontinuitas bisnis dalam menghadapi ancaman keamanan.

1.6 Sistematika Penulisan

Sistematika penulisan yang berjudul: PERANCANGAN ENKRIPSI DATA UNTUK MENCEGAH PENYALAHGUNAAN DATA PELANGGAN DENGAN MENGGUNAKAN METODE ADVANCED ENCRYPTION STANDARD, adalah sebagai berikut:

a. BAB I PENDAHULUAN, Pada bab ini menjelaskan latar belakang dilakukannya penulisan ini berdasarkan kejahatan yang belakangan ini banyak terjadi, perumusan

masalah, pembatasan masalah, tujuan yang ingin dicapai pada penulisan ini, dan meng informasikan metodologi apa yang digunakan pada penulisan ini.

b. BAB II Landasan Teori, Pada bab ini akan dibahas mengenai konsep apa yang digunakan, jurnal dan teori yang digunakan untuk menunjang penulisan ini.
c. BAB III Metode Penelitian, Pada bab ini akan dijelaskan metode apa yang digunakan pada penulisan ini, dan bagaimana cara penerapan metode penelitian yang telah ditentukan.
d. BAB IV Pembahasan, Pada bab ini akan dibahas bagaimana Perusahaan bisa menerapkan sistem keamanan data dengan baik, langkah apa saja yang dilakukan untuk pencegahan, dan Kebijakan apa yang sudah diterapkan.
e. BAB V Kesimpulan dan Saran, Pada bab ini berisi kesimpulan dan saran perbaikan yang telah diteliti dan memastikan penulisan dibuat sudah sesuai dengan tujuan.

1.7 Mata Kuliah yang mendasari Penelitian

Adapun mata kuliah yang mendasari penulisan ilmiah ini berkaitan dengan keamanan siber yang berfokus pada perlindungan sistem komputer, perangkat lunak dan data yang berasal dari serangan atau akses yang tidak sah