BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi telah membawa perubahan besar dalam cara organisasi mengelola data, khususnya melalui sistem digital. Berbagai sektor seperti pemerintahan, pendidikan, keuangan, dan kesehatan semakin bergantung pada sistem informasi yang terhubung secara daring. Namun, seiring dengan meningkatnya pemanfaatan teknologi tersebut, risiko kebocoran dan manipulasi data juga semakin besar. Hal ini menjadikan keamanan data sebagai aspek yang sangat penting untuk diperhatikan, terutama pada sistem berbasis web yang rentan terhadap berbagai jenis serangan.

Salah satu bentuk serangan yang paling sering terjadi adalah SQL Injection, yaitu teknik yang memanfaatkan celah input untuk menyisipkan perintah SQL berbahaya. Serangan ini memungkinkan pelaku untuk mengakses, memodifikasi, atau bahkan menghapus data dalam basis data tanpa otorisasi. Studi yang dilakukan oleh Widianti dan Waluyo menyatakan bahwa sistem yang tidak dilengkapi validasi input yang ketat sangat rentan terhadap serangan jenis ini (SNTIK, 2015).

Beberapa kejadian kebocoran data berskala besar yang terjadi dalam beberapa tahun terakhir menunjukkan lemahnya sistem pengamanan data di berbagai institusi. Misalnya, pada tahun 2021, sebanyak 297 juta data pribadi milik peserta BPJS Kesehatan dilaporkan bocor dan diperjualbelikan secara daring (CNN Indonesia, 2021). Di tahun yang sama, kelompok peretas LockBit mengklaim telah mencuri 1,5 TB data milik Bank Syariah Indonesia. Selanjutnya, pada Maret 2023, sekitar 19,56 juta data peserta BPJS Ketenagakerjaan dilaporkan tersebar ke publik, mencakup informasi seperti NIK, nama, dan alamat. Bahkan Bank Kalteng pun dikabarkan sempat mengalami kebocoran data, meskipun pihak bank membantah adanya pelanggaran keamanan.

Dalam mengatasi ancaman kebocoran data, penggunaan kriptografi menjadi salah satu solusi utama yang banyak diadopsi. Kriptografi merupakan teknik untuk menyamarkan informasi agar hanya pihak yang memiliki kunci tertentu yang dapat mengakses data aslinya. Secara umum, kriptografi dibagi menjadi dua jenis, yaitu

kriptografi simetris yang menggunakan satu kunci untuk proses enkripsi dan dekripsi, serta kriptografi asimetris yang menggunakan pasangan kunci publik dan privat (Ardana, 2021).

Penelitian ini mengembangkan pendekatan *super encryption*, yaitu metode pengamanan data yang menggabungkan dua algoritma kriptografi yang berbeda. Algoritma Diffie Hellman digunakan sebagai mekanisme pertukaran kunci, sedangkan Blowfish digunakan untuk proses enkripsi dan dekripsi data (Hamni et al., 2022). Diffie Hellman dipilih karena mampu membentuk kunci bersama tanpa perlu mengirimkan kunci secara langsung, sementara Blowfish dikenal sebagai algoritma yang efisien dalam kriptografi blok (Rizka, 2021).

Salah satu penelitian terdahulu yang juga menerapkan kombinasi algoritma Diffie Hellman dan Blowfish adalah penelitian oleh Rizka, (2021), yang menggunakan pendekatan tersebut pada sistem pengamanan dokumen berbasis desktop dengan fokus pada efisiensi proses enkripsi. Penelitian ini berbeda dari pendekatan Rizka karena diarahkan pada implementasi langsung dalam konteks pengamanan *database* berbasis web, dengan penekanan pada integrasi algoritma secara manual serta pengujian terhadap ketahanan data melalui simulasi serangan.

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada perancangan sistem keamanan basis data menggunakan metode *super encryption*, yakni kombinasi algoritma Diffie Hellman untuk pertukaran kunci secara aman dan Blowfish untuk proses enkripsi dan dekripsi data. Data yang diamankan mencakup tempat dan tanggal lahir, NIM, nomor rekening, dan nomor handphone, yang mewakili informasi pribadi pengguna. Sistem ini dibangun dalam lingkungan web berbasis PHP Native dan MySQL, dan diuji melalui simulasi serangan SQL Injection serta evaluasi keberhasilan proses dekripsi untuk memastikan integrasi algoritma berjalan dengan baik.

Penelitian ini bertujuan untuk menguji efektivitas metode *super encryption* sebagai solusi perlindungan data sensitif pada basis data berbasis web. Sistem yang dikembangkan bersifat *proof of concept,* yang menunjukkan bahwa kombinasi algoritma kriptografi klasik seperti Diffie Hellman dan Blowfish tetap relevan dan potensial untuk diimplementasikan secara modern. Diharapkan, penelitian ini dapat memberikan kontribusi dalam pengembangan sistem keamanan data yang efisien,

ringan, dan terstruktur, khususnya di lingkungan sistem terbatas atau pengembangan manual tanpa *library* eksternal.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini dapat dijabarkan sebagai berikut:

1. Maraknya kasus kebocoran data seperti yang dialami oleh BPJS Kesehatan dan Bank Syariah Indonesia menunjukkan bahwa banyak data penting disimpan dalam bentuk teks terbuka (plaintext) di dalam database, sehingga apabila terjadi pelanggaran keamanan, data tersebut mudah diakses dan disalahgunakan oleh pihak yang tidak bertanggung jawab.
2. Sistem pengamanan database umumnya belum mengimplementasikan kombinasi algoritma kriptografi secara manual, terutama dalam hal pertukaran kunci dan enkripsi data secara terintegrasi.
3. Diperlukan evaluasi terhadap efektivitas metode super encryption yang mengombinasikan algoritma Diffie Hellman dan Blowfish dalam menjaga kerahasiaan informasi penting pada sistem database berbasis web, khususnya saat menghadapi ancaman serangan.

1.3 Batasan Masalah

Berdasarkan latar belakang dan rumusan masalah yang telah diuraikan sebelumnya, maka batasan masalah yang digunakan pada penelitian ini, yaitu :

1. Penelitian ini hanya berfokus pada perancangan sistem keamanan data melalui proses enkripsi dan dekripsi yang dirancang dengan menerapkan algoritma kriptografi.
2. Algoritma kriptografi yang digunakan adalah Diffie Hellman dan Blowfish.
3. Proses enkripsi dan dekripsi akan dilakukan menggunakan Blowfish dengan Kunci yang dihasilkan oleh Diffie Hellman
4. Sistem yang dikembangkan tidak menggunakan *library* eksternal untuk kriptografi.
5. Pengujian dilakukan pada website uji coba dalam kondisi tanpa perlindungan tambahan, yaitu dengan menonaktifkan mekanisme keamanan seperti SSL/TLS, protokol HTTPS, dan *firewall* pada situs web.

1.4 Tujuan dan Manfaat

1. Tujuan Penelitian
    a. Merancang model enkripsi dengan implementasi kombinasi algoritma Diffie Hellman dan Blowfish untuk pengamanan data pada *database*.
    b. Untuk mengetahui efektivitas dan kinerja metode *super encryption* yang menggunakan kombinasi algoritma Diffie Hellman dan Blowfish dalam proses pengamanan data teks pada kolom *database* melalui simulasi sistem berbasis web.
2. Manfaat Penelitian
    a. Memberikan referensi teknis dan akademis mengenai penerapan *super encryption* dalam sistem pengelolaan data.
    b. Menunjukkan potensi algoritma klasik dalam konteks keamanan *database.*
    c. Memberikan simulasi nyata penggunaan algoritma kriptografi dalam menghadapi ancaman umum pada *database*.