BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan siber telah menjadi isu utama semua negara di seluruh dunia sejak teknologi informasi dan komunikasi mulai digunakan dalam berbagai aspek kehidupan, termasuk sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan, dan lain-lain [1]. Penggunaan teknologi di semua aspek ini menghasilkan banyak data yang perlu dikelola. Jika tidak dikelola dengan baik, data tersebut dapat menimbulkan masalah besar karena berisiko mengalami kebocoran. Kebocoran data adalah masalah serius yang mengkhawatirkan individu, perusahaan, dan pemerintah di seluruh dunia. Kebocoran ini terjadi ketika data yang seharusnya bersifat rahasia atau pribadi, seperti informasi pribadi, bisnis, atau pemerintah, terungkap kepada pihak yang tidak berwenang. Dampak dari kebocoran data termasuk hilangnya privasi individu, penyalahgunaan data, dan berbagai konsekuensi serius lainnya. Keamanan data sangat penting karena setiap individu memiliki hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan aset yang mereka miliki, serta hak untuk merasa aman dan terlindungi dari ancaman yang bisa menghalangi mereka melakukan atau tidak melakukan sesuatu yang menjadi hak asasi mereka [2].

Kebocoran data merupakan masalah serius yang mengkhawatirkan, dan banyak faktor yang dapat menyebabkannya, termasuk lemahnya system keamanan data yang digunakan dan serangan dari pihak yang tidak berwenang, seperti para *hacker* [3]. Dalam dunia siber, serangan *SQL Injection* merupakan salah satu bentuk serangan yang sangat berdampak pada kebocoran data. Di Indonesia, BSSN (Badan Siber dan Sandi Negara) mencatat bahwa selama tahun 2022 Insiden kebocoran data memasuki top 3 insiden siber dengan jumlah total 399 dugaan [4].

Kebocoran data telah menjadi masalah yang mendesak dalam dunia digital yang terus berkembang. Mencegah, mendeteksi, dan menangani pelanggaran data menjadi prioritas utama bagi organisasi dan pemerintah. Untuk mengatasi resiko kebocoran data, organisasi perlu menerapkan strategi keamanan data yang komprehensif. Salah satu pendekatan yang efektif adalah melalui enkripsi data, khususnya dalam *database*. Dengan menerapkan enkripsi pada *database*, data sensitif di dalamnya dapat dilindungi dengan baik, bahkan jika peretas berhasil memasukkan perintah *SQL* berbahaya. Enkripsi memastikan bahwa data yang tersimpan hanya dapat diakses dengan kunci dekripsi yang tepat, menjaga kerahasiaan dan integritas informasi. Enkripsi adalah proses untuk mengamankan pesan (*plain text*) yang diubah sedemikian rupa menjadi pesan tersembunyi (*ciphertext*) [5]. Selain itu, memiliki rencana tanggap insiden yang efisien menjadi penting, karena ini memungkinkan organisasi untuk segera menangani dan melaporkan kebocoran data jika terjadi, sehingga dapat mengurangi dampak negatif yang mungkin timbul.

Berpijak pada Penelitian yang dilakukan oleh Sourav Mukherjee dengan judul "Popular *SQL Server Database Encryption Choices*" mengungkapkan fakta yang mengkhawatirkan: pelanggaran keamanan hampir pasti terjadi pada sebagian besar organisasi saat ini [6]. Hal ini menunjukkan bahwa tantangan keamanan siber semakin kompleks dan organisasi perlu mengambil langkah-langkah proaktif untuk melindungi data mereka. Salah satu solusi yang semakin diakui adalah penggunaan enkripsi pada *database*, khususnya dalam konteks *SQL Server*.

Meskipun sudah banyak para ahli yang membahas penelitian seputar Enkripsi *database* dan tentunya penelitian ini memeliki kesamaan dengan penelitian terdahulu seperti , Teknik enkripsi, metode enkripsi, dan juga *database*. Namun penulis akan menegaskan sisi perbedaan penelitiaan ini dengan penelitian sebelumnya. Pertama, perbedaan dari Teknik enkripsi yang menggunakan *Transparent Data Encryption* . Keamanan data saat disimpan (*data at rest*) pada *database* merupakan tujuan utama dari system

Transparent Data Encryption . Kedua, penelitian ini akan diimplementasikan pada *database* yang akan dikelola oleh *Microsoft SQL Server* [7].

Dengan mengambil beratnya problematika kebocoran data dan kompleksitas tantangan keamanan siber saat ini, penulis bertujuan untuk lebih memfokuskan penelitian ini pada "Enkripsi pada *Database SQL Server* menggunakan Metode Enkripsi *Database* Transparan." Simulasi dari implementasi enkripsi ini diharapkan nantinya, dapat memberikan kontribusi signifikan dalam peningkatan keamanan data yang terdapat dalam *database* tanpa mengganggu kinerja yang berlebihan dari *database*. Oleh karena itu, penelitian ini aberfokus dalam pembahasan lebih lanjut tentang implementasi enkripsi *database* transparan pada *SQL Server* serta dampaknya terhadap integritas dan keamanan data.

1.2. Rumusan Masalah

Ancaman atas kerahasiaan data dapat terjadi melalui serangan terhadap *database* yang menyimpan banyak data dan informasi sensitif sehingga mengancam kerahasiaan dari data tersebut.

1.3. Pertanyaan penelitian

Berdasarkan rumusan masalah diatas, maka pertanyaan peneliti dalam melakukan penelitian ini yaitu:

1. Bagaimana penerapan enkripsi *database* transparan pada *SQL Server* berdampak pada peningkatan keamanan data dalam *database*?
2. Apa dampak dari penggunaan *Transparent Data Encryption* terhadap integritas dan keamanan data dalam *SQL Server*, khususnya dalam melindungi data saat disimpan (*data at rest*)?
3. Bagaimana penggunaan *Transparent Data Encryption* memengaruhi kinerja *database* dalam konteks keamanan data, dan sejauh mana kompromi antara keamanan dan kinerja dapat diidentifikasi?

1.4. Batasan masalah

Penelitian ini memiliki batasan-batasan tertentu yang membimbing fokus penelitian terhadap implementasi *Transparent Data Encryption* pada *Microsoft SQL Server*:

1. Fokus Analisis Keamanan Data:
    - Penelitian ini difokuskan pada analisis dampak *Transparent Data Encryption* terhadap keamanan data di dalam *database*.
    - Penekanan pada perlindungan data saat disimpan (*data at rest*).
2. Pembatasan pada Aspek Kinerja:
    - Penelitian ini tidak mencakup aspek kinerja atau efisiensi *Transparent Data Encryption* terhadap operasi *database* yang tidak secara langsung terkait dengan keamanan data.
    - Fokus utama penelitian ini adalah pada aspek keamanan *Transparent Data Encryption* .
    - Dampak *Transparent Data Encryption* terhadap kinerja umum *database* yang mungkin tidak relevan dengan tujuan utama penelitian ini tidak akan dievaluasi.

1.5. Tujuan

Berdasarkan rumusan masalah. Dapat dijabarkan tujuan penelitian sebagai berikut:

1. Menganalisis dan mengidentifikasi manfaat dari penggunaan *Transparent Data Encryption* dalam meningkatkan keamanan data dalam *database SQL Server*.
2. Mempelajari dampak implementasi *Transparent Data Encryption* terhadap integritas dan keamanan data dalam *SQL Server*.
3. Menilai pengaruh penggunaan *Transparent Data Encryption* terhadap kinerja *database* dalam konteks keamanan data.

1.6. Manfaat Penelitian

Beradasarkan tujuan dari penelitian ini. Dapat dijabarkan manfaat dari penelitian ini adalah:

1. Memberikan pemahaman yang lebih mendalam tentang pentingnya dan manfaat penggunaan *Transparent Data Encryption* dalam melindungi data sensitif dalam *database SQL Server*.
2. Menyediakan wawasan tentang dampak penggunaan *Transparent Data Encryption* terhadap integritas dan keamanan data, serta kinerja *database*, yang dapat membantu organisasi merancang strategi keamanan data yang lebih efisien.
3. Menyumbangkan pengetahuan tambahan dalam bidang keamanan data, khususnya dalam konteks *SQL Server*, yang dapat digunakan sebagai referensi oleh peneliti dan praktisi keamanan siber