# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi pada era digital, terutama teknologi informasi memiliki pengaruh yang signifikan bagi manusia dalam menjalankan kehidupannya sehari-hari, juga dalam bagaimana manusia menyelesaikan masalah-masalah yang timbul dalam kehidupan sehari-hari. Teknologi informasi di era ini dimanfaatkan oleh semua kalangan, baik secara individu, organisasi, atau lembaga untuk meningkatkan efektivitas dan efisiensi dari sebuah proses. Gaya hidup manusia dan pekerjaan-pekerjaan yang dilakukan oleh manusia di era digital ini sudah tidak bisa lagi dipisahkan dari pemanfaatan teknologi. Semua aspek dalam kehidupan manusia di era ini memanfaatkan perkembangan teknologi informasi yang ada. Pemanfaatan teknologi informasi ini terjadi di segala bidang, mulai dari usaha, kesehatan, bisnis, pendidikan, dan lain-lain [1]. Pemanfaatan teknologi informasi yang ada bisa kita jumpai dalam bentuk *website* dan aplikasi (*desktop*/*mobile*). Teknologi informasi seperti *website* dan aplikasi ini banyak dimanfaatkan oleh organisasi atau institusi untuk memajukan organisasi atau institusinya. Perkembangan dari suatu organisasi atau institusi pada era ini sangat dipengaruhi oleh teknologi informasi yang diaplikasikan. Teknologi informasi di era ini, menjadi opsi utama untuk menciptakan sebuah sistem informasi yang berkualitas dan mampu memberikan sebuah organisasi atau institusi keunggulan kompetitif dibandingkan dengan para pesaingnya. Teknologi informasi yang diterapkan dalam organisasi atau institusi ini merubah cara kerja manusia, proses produksi, proses koordinasi, proses berpikir, dan banyak perubahan lainnya di dalam sistem-sistem yang ada di dalam organisasi atau institusi tersebut [2]. Perubahan yang besar dalam organisasi atau institusi ini disebabkan oleh penemuan dan implementasi dari teknologi informasi pada organisasi atau institusi tersebut.

Implementasi teknologi informasi pada organisasi atau institusi tidak bisa terlepas dari data dan informasi. Pengolahan data dahulu masih menggunakan cara konvensional, yaitu dengan menggunakan kertas dan alat-alat konvensional lainnya. Hal ini dinilai tidak efektif dan efisien karena banyaknya peralatan yang harus digunakan, dan banyaknya kekurangan yang dimiliki oleh cara ini seperti dalam proses pencarian dokumen, pencarian data, atau pencarian informasi. Namun, dengan kehadiran teknologi informasi yang sekarang ada, pengolahan data dapat dilakukan dengan sebuah aplikasi *database* yang lebih praktis [3]. Dengan adanya sebuah sistem manajemen *database* yang baik, banyak manfaat yang bisa didapatkan, seperti kemudahan dalam mengorganisir data-data penting suatu organisasi, kemudahan pencarian data atau informasi yang diperlukan, meminimalisir kemungkinan kesalahan pada data, dan banyak lagi. Banyaknya manfaat yang dapat diberikan oleh sistem manajemen *database*, tidak menghindarkan data dari risiko-risiko yang ada, seperti kebocoran data dan pencurian data. Banyak data, seperti data penjualan, data pelanggan, dan lain-lain, dalam sebuah organisasi atau institusi, terutama bagi suatu perusahaan, sangatlah penting dan tidak boleh sampai mengalami kebocoran. Risiko-risiko yang ada ini dapat memunculkan ancaman bagi proses bisnis sebuah perusahaan. Pengelolaan dan manajemen risiko dari data-data milik perusahaan ini menjadi hal yang perlu untuk diperhatikan [4]. Risiko-risiko yang ada menjadi sebuah ancaman bagi perusahaan. Ancaman dapat diartikan sebagai situasi yang secara sengaja maupun tidak sengaja bersifat merugikan dan mempengaruhi sistem terhadap perusahaan yang memiliki sebuah *database*. Keamanan data adalah suatu hal yang harus dimiliki oleh sebuah perusahaan untuk melindungi data mereka dari ancaman-ancaman dan risiko-risiko yang ada, baik secara sengaja maupun tidak [5]. Data-data perusahaan yang disimpan di dalam *database* perusahaan harus diproteksi dengan baik. Banyaknya risiko yang mengancam keamanan data membuat proteksi data diperlukan oleh perusahaan. Proteksi data di dalam *database* perusahaan bisa dilakukan dengan melakukan proteksi pada *database* perusahaan itu sendiri.

Proteksi data dalam *database* diperlukan oleh perusahaan untuk menghindari dan meminimalisir risiko-risiko keamanan pada data seperti kebocoran dan pencurian data. Di Indonesia sendiri, kebocoran data atau *data breach* merupakan sebuah kejadian yang sering terjadi. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2020, jumlah serangan siber naik lebih dari tiga kali lipat [6]. Salah satu kasus terbesar adalah kebocoran data pelanggan dari Perusahaan Listrik Negara (PLN) pada Agustus 2022 yang melibatkan lebih dari 17 juta data pelanggan [7]. Selain itu, pada Juli 2021, terjadi juga sebuah kebocoran data nasabah dari BRI Life yang mengakibatkan lebih dari 2 juta data nasabah bocor, bahkan dijual di internet [8]. Sementara itu, pada akhir tahun 2020, sekitar 1.1 juta data pelanggan Lazada juga diduga bocor ke pasar gelap [9]. Kasus-kasus tersebut menunjukkan bahwa perhatian terhadap keamanan siber dan privasi data perlu untuk diperhatikan. Kasus-kasus tersebut juga menunjukkan bahwa proteksi *database* yang baik diperlukan oleh sebuah perusahaan. Salah satu perusahaan yang membutuhkan proteksi *database* adalah PT ABC. PT ABC adalah salah satu perusahaan yang bergerak di industri teknologi informasi, sebagai penyedia solusi IT. *Database* sebuah perusahaan pasti banyak berisi informasi-informasi sensitif dan rahasia seperti data karyawan, data pelanggan, data keuangan, dan data lainnya [10]. Jika *database* tersebut tidak dilindungi dengan baik, maka perusahaan dapat menghadapi berbagai risiko keamanan seperti kebocoran data, pencurian identitas, dan lain-lain. Ancaman terhadap keamanan *database* perusahaan semakin meningkat karena semakin banyaknya penggunaan teknologi informasi dalam bisnis [11]. Oleh karena itu, perusahaan perlu mengambil tindakan proteksi *database* yang efektif untuk menghindari hal tersebut. Proteksi *database* merupakan hal yang sangat penting bagi perusahaan untuk menghindari risiko keamanan. PT ABC menggunakan sistem manajemen *database* MySQL untuk platform *website*nya. Dengan adanya risiko-risiko yang ada, PT ABC juga membutuhkan proteksi *database* untuk *database* MySQL yang digunakan oleh perusahaan mereka.

Proteksi *database* MySQL menjadi sebuah hal penting yang perlu dilakukan untuk melindungi data perusahaan dari kebocoran data, pencurian data, atau akses tidak sah pada data perusahaan. MySQL merupakan salah satu sistem manajemen *database* yang paling populer digunakan di dunia, dan banyak digunakan oleh perusahaan-perusahaan secara internasional [12]. Proteksi *database* MySQL meliputi berbagai teknik dan strategi untuk melindungi *database* dari serangan atau kehilangan data. Ada beberapa teknik proteksi *database* yang sering digunakan. Pertama, teknik enkripsi merupakan salah satu teknik proteksi *database* yang paling populer. Dalam teknik ini, data dienkripsi sehingga hanya orang yang memiliki kunci enkripsi yang dapat membuka data tersebut. Teknik ini sangat efektif dalam melindungi data yang sensitif. Kedua, teknik pengamanan akses juga merupakan teknik yang penting dalam proteksi *database*. Dalam teknik ini, perusahaan dapat menetapkan aturan akses yang ketat untuk mengontrol siapa saja yang memiliki akses ke *database* tersebut. Hal ini dapat menghindari akses tidak sah dan melindungi data dari serangan *hacker* atau peretas. Ketiga, teknik pemantauan aktivitas *database* juga sangat penting untuk meningkatkan keamanan *database*. Dalam teknik ini, perusahaan dapat menggunakan perangkat lunak khusus yang dapat memantau aktivitas *database* secara *real-time*. Hal ini memungkinkan perusahaan untuk mengidentifikasi aktivitas mencurigakan dan segera mengambil tindakan yang diperlukan [13]. Dari ketiga teknik yang bisa digunakan tersebut, enkripsi menjadi pilihan yang populer untuk melindungi *database* perusahaan dari ancaman kebocoran dan pencurian data.

Enkripsi *database* MySQL adalah salah satu teknik proteksi *database* untuk sistem manajemen *database* MySQL yang dapat dilakukan untuk melindungi data yang tersimpan di dalam *database* dari bentuk-bentuk akses tidak sah. Enkripsi *database* MySQL dapat dilakukan pada level kolom, tabel, atau keseluruhan *database*. Enkripsi dapat mengamankan data-data yang ada ketika data sedang dipindahkan antara *server* dan klien, ataupun saat data sedang disimpan di dalam *database* [14]. Enkripsi pada *database* MySQL menjadi hal yang penting untuk pengamanan data di dalam *database*. Beberapa studi telah

dilakukan untuk meningkatkan keamanan pada enkripsi data di MySQL. Banyak algoritma yang digunakan dalam penelitian-penelitian tersebut. Misal, algoritma enkripsi *vernam chiper*, menunjukkan bahwa algoritma tersebut mampu memberikan proteksi yang baik terhadap *database* dengan minim dampak pada efisiensi kinerja sistem [15]. Adapun teknik enkripsi kolom dinamis dengan menggunakan FHE (*Fully Homomorphic Encryption*) untuk menjaga kerahasiaan data, menunjukkan bahwa teknik tersebut memiliki performa yang baik [16]. Sementara itu ada teknik lain yang pernah diteliti, yaitu teknik enkripsi data dalam SQL Server menggunakan Transparent Data Encryption. Hasil pengujian menunjukkan bahwa teknik tersebut efektif dalam menjaga keamanan data, dengan penurunan performa *database* yang minimum yang diuji dengan menggunakan *load & stress test* [17]. Sementara itu, teknik enkripsi pada *database* dengan menggunakan metode enkripsi Blowfish dan *base* 64, mampu menjaga kerahasiaan data dengan baik namun memiliki kelemahan dalam hal kecepatan *query* [18], sedangkan enkripsi kolom pada MySQL dengan menggunakan algoritma enkripsi homomorfik Paillier mampu menjaga keamanan data dengan baik dan memiliki performa yang cukup cepat [19]. Teknik enkripsi pada *cloud computing* dengan menggunakan algoritma enkripsi homomorfik HEA (*Homomorphic Encryption Algorithm*) juga mampu menjaga kerahasiaan data dengan baik namun memiliki dampak minimum dalam hal kecepatan *query* [20]. MySQL *Transparent Data Encryption* (TDE) adalah solusi enkripsi yang disediakan oleh MySQL Enterprise Edition untuk melindungi data yang disimpan di dalam *database* MySQL. MySQL TDE menggunakan algoritma *Advanced Encryption Standard* (AES) dengan kunci 256-bit untuk melindungi data yang disimpan di dalam *database* MySQL. MySQL TDE juga menyediakan mekanisme manajemen kunci yang aman dan fleksibel. Dari artikel, MySQL TDE dapat meningkatkan keamanan data secara signifikan tanpa mempengaruhi kinerja aplikasi [21]. Dengan menggunakan MySQL TDE, data di dalam *database* dapat terproteksi dari risiko-risiko keamanan yang ada.

Oleh karena itu, dalam penelitian ini, akan dilakukan proteksi *database* MySQL untuk PT ABC menggunakan *tools* MySQL TDE. Penelitian ini akan bertujuan untuk mencari tahu hasil metode proteksi dengan MySQL *Transparent Data Encryption* (TDE) karena masih minimnya penelitian menggunakan metode tersebut. Dalam penelitian ini, *tools* MySQL TDE akan diimplementasikan ke *database* dari PT ABC untuk memberikan proteksi dan meningkatkan keamanan dari *database* PT ABC agar terhindar dari risiko-risiko yang ada.

## 1.2 Rumusan Masalah

Berdasarkan permasalahan yang telah diuraikan pada latar belakang penelitian, berikut adalah rumusan masalah yang ditemukan untuk penelitian:

1. Bagaimana hasil enkripsi *database* yang dilakukan dapat membantu PT ABC dalam memproteksi data-data perusahaan dari kebocoran data dan pencurian data?
2. Bagaimana hasil kinerja enkripsi pada *database* mempengaruhi performa sistem secara keseluruhan?

## 1.3 Batasan Masalah

Dalam penelitian ini, ditentukan beberapa batasan masalah, yaitu:

1. Proteksi *database* dilakukan dengan menggunakan MySQL TDE
2. Sistem DBMS yang digunakan adalah MySQL.
3. Proteksi yang dilakukan akan diimplementasikan sesuai dengan kebutuhan dari PT. ABC.

## 1.4 Tujuan dan Manfaat Penelitian

### 1.4.1 Tujuan Penelitian

1. Mengetahui bagaimana hasil dari enkripsi *database* yang dilakukan dapat membantu PT ABC dalam memproteksi data-data yang ada pada *database* dari PT ABC.
2. Menentukan efisiensi dari hasil enkripsi yang dilakukan.

### 1.4.2 Manfaat Penelitian

1. Memproteksi data di dalam *database* yang dimiliki oleh PT ABC.
2. Meningkatkan kemampuan sistem *database* PT ABC dalam menghadapi ancaman keamanan.
3. Mengetahui cara melakukan enkripsi *database* MySQL menggunakan MySQL *Transparent Data Encryption.*
4. Mengetahui efisiensi dari hasil enkripsi yang dilakukan.

## 1.5 Sistematika Penulisan

BAB I PENDAHULUAN

Dalam bab ini akan dibahas mengenai latar belakang masalah penelitian, rumusan masalah, batasan masalah penelitian, tujuan penelitian, manfaat penelitian, dan sistematika penulisan karya ilmiah.

BAB II LANDASAN TEORI

Dalam bab ini akan dibahas mengenai teori-teori pendukung penelitian, seperti *database,* DBMS, proteksi *database, database availability, database security, database integrity,* enkripsi *database,* enkripsi AES 256, MySQL, MySQL *Transparent Data Encryption.*

BAB III METODOLOGI PENELITIAN

Dalam bab ini akan dibahas mengenai metode-metode yang akan digunakan dalam penelitian, terdiri dari diagram, struktur tabel *database,* dan *flowchart.*

BAB IV HASIL PENELITIAN

Dalam bab ini akan dibahas mengenai hasil dari penelitian yang telah dilakukan.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini akan dibahas mengenai kesimpulan yang didapatkan setelah melakukan penelitian, dan saran untuk penelitian kedepannya.