BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan ilmu pengetahuan dan teknologi di Indonesia telah secara signifikan memengaruhi kehidupan Masyarakat khususnya dalam bidang keamanan siber[1]. Keamanan siber memiliki peran sentral dalam melindungi system computer, jaringan, perangkat, dan data dari ancaman serta upaya akses ilegal. Hal ini sangat penting untuk menjaga kerahasiaan data pribadi, memastikan keamanan bisnis, dan menjaga stabilitas infrastruktur kritis seperti transportasi data[2]. Selain itu, keamanan siber juga menjadi fondasi bagi pengembangan teknologi yang lebih canggih, sambil membantu meningkatkan kesadaran Masyarakat akan pentingnya menjaga keamanan data pribadi. Masalah keamanan data menjadi focus utama, terutama di era teknologi informasi di mana hamper semua data disimpan secara daring dan dapat diakses oleh siapa saja, yang menimbulkan kekhawatiran akan kemungkinan kebocoran data pelanggan dan penjualan, terutama bagi bisnis dan organisasi yang mengandalkan platform digital untuk operasional[3].

Kebocoran data menjadi permasalahan krusial yang sering terjadi di Indonesia[4]. Menurut data dari Perusahaaan keamanan siber *Surfshark*, Indonesia menempati peringkat ketiga dalam jumlah kasus kebocoran data terbanyak di dunia pada tahun 2022, dengan lebih dari 12 juta akun yang terkena dampak. Salah satu contohnya yaitu insiden kebocoran data pribadi pengguna Tokopedia pada 20 Maret 2020, yang dilaporkan oleh CNN Indonesia. Dalam insiden tersebut, seorang peretas dengan nama *whysodank* berhasil mencuri data sekitar 91 juta pengguna Tokopedia. Data tersebut meliputi nomor telepon, email dengan *hash password*, dan nama pengguna telah diretas dan dijual oleh seorang peretas dengan harga 74 juta di *dark web*[5]. Kejadian serupa juga terjadi di sektor perbankan khususnya pada Bank Syariah Indonesia (BSI) yang diretas oleh seorang *hacker* asal Rusia pada 8 Mei 2023. *Hacker* tersebut berhasil mencuri dan mengambil alih sekitar 1,5 *gigabyte* informasi pribadi pengguna yang meliputi nama lengkap, nomor telepon, lokasi, saldo rekening,

riwayat transaksi, serta detail pembukaan rekening detail pekerjaan, dan beberapa data lainnya. Kemudian data nasabah BSI di jual pada pasar gelap internet atau *dark web*[6]. Semua kejadian tersebut menunjukkan adanya kerentanan yang signifikan terhadap privasi dan keamanan data pribadi serta lembaga-lembaga yang terkena dampaknya. Kerentanan ini muncul saat sistem keamanan data yang digunakan masih belum aman dan cepat dan mudah dialihkan oleh pihak-pihak yang tidak bertanggung jawab.

Dampak dari kebocoran data berpotensi mengarah pada pencurian identitas, manipulasi mata uang, atau bahkan penggunaan data untuk tujuan kriminal. Selain itu, data pelanggan yang tidak akurat dapat merugikan reputasi perusahaan atau organisasi yang mengumpulkan data tersebut karena pelanggan tidak lagi memiliki kepercayaan terhadap perusahaan atau organisasi tersebut. Oleh karena itu, perlindungan privasi menjadi semakin penting di era digital saat ini.[7]

Untuk mengatasi permasalahan kebocoran data yang telah dijelaskan sebelumnya, langkah yang diambil adalah menerapkan enkripsi pada tingkat database dengan melakukan proses pengenkripsian pada tabel yang ada dalam database tersebut. Langkah ini sesuai dengan upaya meningkatkan keamanan data pelanggan, terutama mengingat rentannya keamanan saat berbagi informasi dan menyimpan data. Pada penelitian ini akan mengamankan data pelanggan di toko kelontong Pak Nurhadi yang terletak di Jl. Endro Bajang Mlarak Ponorogo. Toko kelontong Pak Nurhadi merupakan usaha kecil menengah (UKM) yang bergerak dibidang ritel dengan menjual sembilan bahan pokok dan kebutuhan sehari-hari telah berkembang pesat seiring waktu. Toko kelontong Pak Nurhadi telah mengalami perkembangan signifikan dengan mengadopsi sistem informasi untuk mengelola berbagai aspek operasionalnya. Usaha kecil menengah (UKM) seperti toko kelontong Pak Nurhadi belum memiliki sistem keamanan database pelanggan, dan sering diabaikan dalam hal keamanan data. Sistem ini dirancang untuk mengelola dan melindungi data pribadi pelanggan seperti NIK,nama, alamat, nomor telepon, dan riwayat pembelian dengan keamanan tinggi. Dengan volume transaksi harian, sistem ini

juga harus memiliki skala untuk menangani pertumbuhan jumlah data seiring dengan peningkatan jumlah pelanggan.

Oleh karena itu, di Toko Kelontong Pak Nurhadi, diterapkan sistem keamanan database pelanggan yang mengandalkan algoritma kriptografi dan teknik enkripsi, khususnya menggunakan Algoritma RSA *(Rivest-Shamir-Adleman)*, untuk melindungi kerahasiaan dan integritas data pelanggan. Algoritma RSA *(Rivest-Shamir-Adleman)* dipilih karena memiliki keamanan tinggi, ketahanan terhadap serangan, skalabilitas, dan penggunaan yang luas, menjadikannya pilihan yang kuat untuk melindungi kerahasiaan dan integritas data[8]. Implementasi ini memberikan Usaha Kecil Menengah (UKM) dapat memanfaatkan teknologi kriptografi modern untuk meningkatkan keamanan data mereka.

Proses enkripsi dengan menggunakan algoritma RSA (*Rivest-Shamir-Adleman*) dilakukan pada data pelanggan sebelum data tersebut disimpan ke dalam database. Selama proses enkripsi, informasi pribadi yang bersifat sensitif seperti Nomer Induk Kependudukan, nama, alamat, nomor telepon, tanggal lahir, dan riwayat pembelian sebelumnya dienkripsi. Proses pengkodean diawali dengan pemisahan dua kunci yaitu public dan private. Kunci publik digunakan untuk mengenkripsi data, sedangkan kunci privat digunakan untuk mendekripsi data yang dienkripsi sebelumnya. Informasi sensitif diubah ke dalam format yang disebut terenkripsi menggunakan kunci publik sebelum disimpan dalam database. Ketika data tersebut dibutuhkan kembali, proses dekripsi dilakukan dengan menggunakan kunci pribadi yang sesuai sehingga data sensitif dapat dipulihkan ke dalam bentuk aslinya. Dengan menerapkan pendekatan ini, risiko terhadap kemungkinan bocornya data pelanggan dapat dikurangi, menjaga keamanan data pelanggan, memastikan privasi tetap terjaga, dan mengurangi potensi akses yang tidak sah. Berdasarkan latar belakang yang telah diuraikan diatas, maka peneliti melakukan penelitian dengan judul "Impelemtasi Algoritma *Rivest Shamir Adleman* (RSA) Untuk Keamanan Database Pelanggan di Toko Kelontong".

1.2 Rumusan Masalah

Berdasarkan permasalahn dari latar belakang yang telah diuraikan diatas, maka rumusan masalah pada penelitian ini bagaimana mengamankan data pelanggan menggunakan Algoritma RSA (*Rivest-Shamir-Adleman*) pada *database* pelanggan di Toko Kelontong Pak Nurhadi ?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini yaitu untuk mengetahui cara mengamankan data pelanggan menggunakan algoritma RSA (*Rivest-Shamir-Adleman*) pada database pelanggan di Toko Kelontong Pak Nurhadi.

1.4 Batasan Masalah

Berdasarkan penjelasan tersebut diatas diperlukan adanya batasan masalah sehingga penelitian ini dapat lebih terarah dan sesuai yang diharapkan, Batasan masalah pada penelitian ini, sebagai berikut :

1. Penelitian ini hanya membahas tentang keamanan database pelanggan di Toko Kelontong Pak Nurhadi.
2. Penelitian ini tidak membahas implementasi atau evaluasi teknologi enkripsi lainnya selain Algoritma RSA (*Rivest-Shamir-Adleman*).
3. Penelitian ini hanya mempertimbangkan aspek teknis dalam menerapkan Algoritma RSA (*Rivest-Shamir-Adleman*) pada keamanan database pelanggan.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah melindungi data pelanggan dan mengurangi potensi risiko kebocoran data pada database pelanggan khususnya pada Sistem Informasi Penjualan di Toko Kelontong Pak Nurhadi.