

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini sangat pesat memengaruhi kehidupan masyarakat terutama pada bidang kemanan. Kebutuhan akan akses informasi cepat menuntut kita untuk memanfaatkan teknologi yang ada pada saat ini. Sejak adanya internet, masyarakat tidak dibatasi untuk mencari berbagai informasi apaun di berbagai penjuru dunia, dan penggunaan teknologi informasi sekarang menjadi transmisi informasi yang efisien dan efektif [1]. Keamanan data merupakan masalah yang sangat serius dan krusial dalam melindungi sistem komputer, data, jaringan serta perangkat lainnya dari ancaman akses ilegal. Hal ini sangat penting untuk menjaga privasi data diri untuk memastikan dan menjaga stabilitas transportasi data [2]. Selain itu keamanan juga menjadi dasar bagi pengembangan teknologi yang lebih baik lagi, dan sebagai peringatan untuk masyarakat akan pentingnya keamanan data. Sistem keamanan menjadi fokus utama pada era 5.0 dimana semua data disimpan melalui perangkat yang bisa diakses oleh semua orang, sehingga bisa menimbulkan serangan siber dan kemungkinan kebocoran data terutama pada kelangsungan keamanan di lembaga pendidikan khususnya pondok pesantren [3].

Negara Indonesia saat ini tengah menghadapi permasalahan serius terkait dengan kebocoran data. Berdasarkan informasi dari perusahaan Surfshark, Indonesia termasuk dalam salah satu negara dengan tingkat kebocoran data tertinggi di dunia pada tahun 2022, dengan jutaan akun pengguna yang menjadi korban peretasan. Salah satu contohnya adalah insiden kebocoran data pribadi pengguna platform *e-commerce* Tokopedia pada tanggal 20 Maret 2020, seperti yang dilaporkan oleh CNN Indonesia. Dalam kasus ini, seorang peretas dengan nama samaran *whysodank* berhasil menembus sistem keamanan Tokopedia dan mencuri data pribadi milik puluhan juta pengguna[4]. Informasi penting seperti nomor telepon dan rincian

akun Tokopedia kemudian diperjual belikan secara ilegal di pasar gelap setelah berhasil diretas. Insiden serupa juga terjadi pada sektor perbankan, tepatnya di Bank Syariah Indonesia (BSI), yang mengalami serangan siber oleh peretas asal Rusia pada 8 Mei 2023. Dalam serangan ini, pelaku berhasil mengakses serta mencuri data pribadi nasabah BSI, termasuk informasi keuangan yang sangat sensitif. Data tersebut kemudian diperjual belikan di internet gelap atau *dark web*[5]. Banyaknya kejadian ini menegaskan bahwa adanya kelemahan serius dalam perlindungan data pribadi serta sistem keamanan institusi yang menjadi sasaran. Kekurangan dalam sistem keamanan memberikan celah bagi peretas untuk dengan mudah mengakses dan mencuri informasi penting.

Banyaknya kasus kebocoran data di Indonesia turut berdampak pada keamanan data. Kebocoran data berpotensi menyebabkan penyalahgunaan informasi seperti penipuan dan manipulasi, yang dapat menimbulkan kerugian finansial. Selain itu, lemahnya perlindungan data dapat menurunkan tingkat kepercayaan pengguna terhadap sistem yang digunakan. Oleh karena itu, penerapan sistem keamanan data transaksi yang andal menjadi kebutuhan untuk menjamin kerahasiaan dan integritas data. [6]

Solusi diperlukan untuk menangani permasalahan kebocoran data di Indonesia. Salah satu langkah krusial adalah meningkatkan pemahaman mengenai pentingnya keamanan data, baik di tingkat individu maupun lembaga. Langkah yang tepat pada kasus kebocoran data yang sudah dibahas diatas adalah penerapan enkripsi database dengan melakukan pengenkripsian pada tabel-tabel yang ada pada database tersebut [7]. Cara ini sesuai dengan langkah strategis untuk meningkatkan keamanan data transaksi santri, terutama mengingat berpotensi tinggi terjadi kebocoran data saat berbagi informasi data. Dalam penelitian ini, fokus diarahkan pada pengamanan database pada Sistem Pembayaran di DT Mart yang berlokasi di Desa Pintu, Kecamatan Jenangan, Kabupaten Ponorogo. DT Mart merupakan unit layanan di lingkungan pondok pesantren yang memanfaatkan sistem pembayaran berbasis teknologi informasi. Saat ini, DT Mart belum memiliki sistem yang memadai untuk menjaga kerahasiaan data pribadi dan data transaksi para santri. Informasi

penting santri masih sangat rentan terhadap resiko kebocoran, oleh karena itu perlu dikembangkan suatu sistem yang mampu memberikan perlindungan data santri secara efisien dan maksimal, serta memiliki kemampuan skalabilitas untuk menyesuaikan dengan peningkatan jumlah data santri di masa yang akan datang.[8]

Penerapan algoritma kriptografi yang kuat seperti RSA (*Rivest Shamir Adleman*) merupakan langkah tepat untuk melindungi data santri. RSA (*Rivest Shamir Adleman*) dipilih karena memiliki sistem keamanan yang tinggi dan memiliki kelebihan dalam menjaga kerahasiaan data melalui penggunaan dua kunci berbeda (*public key* dan *private key*) RSA dinilai cocok untuk sistem dengan kebutuhan keamanan tinggi karena sulit untuk memfaktorkan bilangan besar.[9] Penerapan algoritma ini memungkinkan lembaga untuk memanfaatkan teknologi kriptografi dan metode enkripsi modern dalam rangka meningkatkan perlindungan terhadap data yang mereka miliki.

1.2 Rumusan Masalah

Bedasarkan masalah yang diuraikan pada latar belakang, maka rumusan masalah pada penelitian ini bagaimana cara mengamankan data transaksi menggunakan Algoritma RSA (*Rivest Shamir Adleman*) di DT Mart Pondok Pesantren Darut Taqwa?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini untuk mengetahui cara mengamankan data transaksi menggunakan algoritma RSA (*Rivest Shamir Adleman*) di Pondok Pesantren Darut Taqwa terutama pada database sistem pembayaran DT Mart berbasis RFID.

1.4 Batasan Masalah

Bedasarkan penjelasan diatas adanya batasan masalah agar penelitian ini lebih terarah, maka batasan masalah pada penelitian ini sebagai berikut :

1. Penelitian hanya membahas tentang sistem keamanan detail transaksi santri di Pondok Pesantren Darut Taqwa.
2. Penelitian ini tidak membahas penerapan atau evaluasi enkripsi lainnya selain Algoritma RSA (*Rivest Shamir Adleman*).

3. Penelitian ini mempertimbangkan aspek teknis dalam penerapan algoritma RSA (*Rivest Shamir Adleman*) pada keamanan data transaksi santri di Pondok Pesantren Darut Taqwa.

1.5 Manfaat Penelitian

Dari penelitian ini diharap dapat memberikan manfaat, yaitu menghasilkan sistem yang mampu menjaga keamanan data dan transaksi melalui penerapan enkripsi pada database menggunakan algoritma RSA khususnya pada sistem pembayaran berbasis RFID di DT Mart Pondok Darut Taqwa.

