BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan meningkatnya pemanfaatan teknologi informasi, keamanan data dan privasi menjadi salah satu aspek yang sangat diperhatikan [1]. Sistem digital umumnya menyimpan dan memproses data dalam jumlah besar, termasuk data yang bersifat pribadi dan sensitif. Tanpa mekanisme perlindungan yang memadai, data tersebut berisiko mengalami kebocoran, akses tidak sah maupun penyalahgunaan oleh pihak yang tidak bertanggung jawab [2]. Risiko tersebut dapat berasal dari berbagai ancaman, baik yang bersifat teknis seperti serangan siber, maupun non-teknis seperti kesalahan konfigurasi dan kelalaian pengguna. Menurut data Kementerian Koordinator Bidang Politik dan Keamanan, terdapat sebanyak 370 juta anomali yang terdeteksi dalam lalu lintas siber Indonesia pada periode Mei hingga Juni 2025 [3]. Tingginya jumlah anomali tersebut menunjukkan bahwa aktivitas siber masih dihadapkan pada berbagai ancaman seperti *phishing*, *malware*, dan *Distributed Denial of Service* (DDoS) [4] [5] [6]. Kondisi ini mengindikasikan bahwa sistem informasi yang digunakan oleh berbagai institusi memerlukan mekanisme perlindungan yang memadai untuk menjaga kerahasiaan, integritas, dan ketersediaan data [7]. Oleh karena itu, penerapan prinsip-prinsip keamanan informasi diperlukan untuk memastikan bahwa data dapat dilindungi dari ancaman yang dapat mengganggu kerahasiaan, keutuhan dan ketersediaannya selama siklus pengelolaan data berlangsung.

Bidang kesehatan merupakan salah satu sektor yang memiliki tingkat sensitivitas data yang tinggi [8]. Informasi seperti identitas pasien, riwayat medis, hasil diagnosis dan tindakan medis termasuk dalam kategori data pribadi yang harus dijaga kerahasiaannya [9]. Data tersebut tidak hanya mencerminkan kondisi kesehatan seseorang tetapi juga dapat memengaruhi aspek sosial dan psikologis apabila disalahgunakan. Beberapa kasus kebocoran data kesehatan yang pernah terjadi mencakup bocornya data BPJS pada tahun 2021 [10], kebocoran data *Electronic Health Alert Card* (E-HAC) milik Kementerian Kesehatan [11] serta

kebocoran data PeduliLindungi pada tahun 2022 lalu [12]. Hal ini menunjukkan bahwa lemahnya sistem keamanan dapat menimbulkan pelanggaran privasi serta menurunkan kepercayaan masyarakat terhadap institusi kesehatan [13]. Kondisi tersebut menunjukkan bahwa sistem informasi berbasis digital, khususnya di sektor kesehatan, memerlukan mekanisme perlindungan data yang memadai. Meningkatnya pemanfaatan layanan digital menyebabkan proses pengelolaan data menjadi lebih kompleks dan rentan terhadap ancaman keamanan, sehingga diperlukan mekanisme seperti enkripsi dan kontrol akses untuk membantu menjaga kerahasiaan dan integritas data [14] [15].

Salah satu organisasi kemanusiaan di Indonesia yang berperan penting dalam bidang kesehatan adalah Palang Merah Indonesia (PMI). PMI merupakan salah satu organisasi kemanusiaan nasional yang memiliki peran penting dalam pelayanan kesehatan dan kegiatan sosial termasuk dalam pengelolaan data pasien, pendonoran darah serta penerima layanan kesehatan [16]. Dalam menjalankan kegiatannya, PMI mengelola berbagai jenis data yang bersifat sensitif seperti data identitas pengguna layanan, data pendonor darah, informasi layanan kesehatan serta riwayat interaksi layanan. Oleh karena itu, pemanfaatan sistem basis data menjadi bagian yang tidak terpisahkan dalam mendukung operasional PMI khususnya dalam proses penyimpanan dan pengolahan data yang dilakukan [17]. Namun, berdasarkan hasil wawancara dengan pihak PMI, meskipun PMI telah memiliki sistem terpusat untuk mengelola dan menyimpan data yang dikirimkan oleh masing-masing cabang, pengelolaan dokumen operasional, SOP, serta berbagai informasi pendukung layanan pada tingkat cabang masih banyak dilakukan secara terpisah oleh masing-masing divisi. Informasi tersebut umumnya disimpan pada perangkat yang digunakan oleh setiap unit kerja sesuai kebutuhan operasionalnya. Kondisi ini menyebabkan proses pencarian, pengelolaan, dan pemanfaatan informasi pada tingkat cabang masih bergantung pada masing-masing divisi sehingga belum tersedia repositori informasi yang terintegrasi dan mudah diakses untuk mendukung layanan informasi kepada masyarakat.

Selain itu, masyarakat secara aktif memanfaatkan WhatsApp dan media sosial untuk memperoleh informasi terkait donor darah, layanan kesehatan, kegiatan sosial, serta layanan PMI lainnya. Berdasarkan hasil wawancara, jumlah pesan yang

diterima melalui kanal komunikasi digital mencapai sekitar 80 hingga 100 pesan per hari, sedangkan pesan yang dapat ditangani secara optimal hanya berkisar 60 hingga 70 pesan per hari. Proses pelayanan informasi yang masih dilakukan secara manual menyebabkan waktu respons bergantung pada ketersediaan petugas, terutama untuk pertanyaan yang bersifat berulang seperti jadwal pelayanan, persyaratan donor darah dan ketersediaan stok darah. Kondisi tersebut menunjukkan adanya kebutuhan terhadap sistem yang mampu membantu penyediaan informasi secara lebih cepat dan konsisten. Oleh karena itu, chatbot menjadi salah satu layanan digital yang berpotensi dikembangkan untuk mendukung layanan informasi PMI kepada masyarakat.

Pengembangan *chatbot* dapat menjadi salah satu upaya untuk meningkatkan kualitas layanan informasi kepada masyarakat. Namun, sistem basis data yang digunakan untuk menyimpan dan mengelola informasi memerlukan mekanisme keamanan yang memadai. Berdasarkan informasi publik pada kebijakan privasi PMI Jakarta Barat, perlindungan data yang dijelaskan berfokus pada penggunaan *Secure Sockets Layer* (SSL) untuk mengamankan transmisi data serta pembatasan akses terhadap *server (data in transit)* [18]. Namun demikian, belum ditemukan penjelasan terkait mekanisme perlindungan data saat tersimpan (*data at rest*) pada basis data. Pendekatan tersebut belum mencakup perlindungan secara menyeluruh terhadap seluruh rangkaian proses pengelolaan data. Untuk meminimalkan risiko tersebut, sistem chatbot perlu dilengkapi dengan mekanisme perlindungan basis data yang mendukung pengaturan hak akses pengguna, penerapan enkripsi, serta pembatasan akses terhadap data yang telah diotorisasi [19]. Penerapan mekanisme keamanan ini penting karena chatbot berinteraksi secara langsung dengan pengguna dan berpotensi menjadi salah satu titik masuk terhadap sistem apabila tidak diberikan perlindungan yang memadai [20].

Dalam pengembangannya, rancangan *chatbot* PMI menggunakan pendekatan *hybrid database* yang mengombinasikan relational database menggunakan PostgreSQL dan vector database melalui ekstensi pgvector. PostgreSQL berperan sebagai penyimpanan utama untuk data yang memiliki struktur yang jelas seperti data layanan, jadwal, aktivitas pengguna serta berbagai informasi administratif [21]. Sementara itu, pgvector digunakan untuk mendukung penyimpanan vector

embedding dan data chatbot dalam lingkungan basis data yang sama [22]. Pendekatan ini memungkinkan data relasional dan data berbasis vektor dikelola secara terintegrasi tanpa memerlukan sistem penyimpanan terpisah sehingga proses pengelolaan data menjadi lebih sederhana dan terpusat. Namun, integrasi berbagai jenis data dalam satu lingkungan basis data juga memerlukan mekanisme perlindungan yang mampu mengamankan data selama proses penyimpanan, transmisi maupun akses oleh pengguna yang berbeda.

Berdasarkan penelitian terdahulu, sebagian besar penelitian masih berfokus pada penerapan mekanisme keamanan tertentu secara terpisah atau pada pengembangan sistem berbasis AI dan chatbot tanpa menitikberatkan pada perlindungan basis data secara menyeluruh. Selain itu, penelitian yang membahas implementasi berbagai mekanisme perlindungan basis data pada lingkungan hybrid database yang menggabungkan data relasional dan data berbasis vektor dalam satu platform PostgreSQL masih relatif terbatas. Oleh karena itu, diperlukan penelitian yang berfokus pada perancangan dan evaluasi mekanisme perlindungan basis data pada arsitektur hybrid database untuk mendukung pengelolaan data chatbot secara lebih aman.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang mekanisme perlindungan basis data pada sistem *chatbot* PMI yang menggunakan arsitektur hybrid database berbasis PostgreSQL dan pgvector. Mekanisme yang dirancang mencakup *encryption at rest* menggunakan AES-256, pengamanan komunikasi data menggunakan TLS melalui OpenSSL, *Role-Based Access Control* (RBAC), *Row-Level Security* (RLS), *parameterized query* serta *resource limiting*. Selanjutnya, mekanisme tersebut akan dievaluasi melalui pengujian fungsional, pengujian keamanan dan *benchmarking* untuk menilai efektivitas perlindungan data serta dampaknya terhadap performa basis data. Diharapkan penelitian ini dapat memberikan kontribusi dalam pengembangan mekanisme perlindungan basis data yang lebih aman serta menjadi referensi dalam pengembangan sistem chatbot pada sektor kesehatan.

1.2 Rumusan Masalah

Berdasarkan pada permasalahan yang diangkat diatas, berikut adalah beberapa rumusan masalah yang diusulkan dalam penelitian ini:

1. Bagaimana penerapan mekanisme perlindungan basis data pada *chatbot* PMI dalam menjaga kerahasiaan data?
2. Bagaimana hasil evaluasi terhadap mekanisme perlindungan basis data yang dirancang dalam meningkatkan perlindungan data pada rancangan sistem *chatbot* PMI?

1.3 Batasan Masalah

Berdasarkan topik yang diangkat pada penelitian ini, terdapat beberapa batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Perancangan mekanisme perlindungan basis data chatbot PMI akan menggunakan beberapa metode keamanan yang mencakup *Encryption at Rest* menggunakan algoritma AES-256, *Transport Layer Security* (TLS) menggunakan OpenSSL, *Role Based Access Control* (RBAC), *Row-Level Security* (RLS), *audit logging*, *parameterized query* dan *resource limiting*.
2. Perancangan yang dibuat dibatasi pada rancangan basis data chatbot PMI yang digunakan untuk mengelola informasi umum dan khusus terkait layanan PMI serta data interaksi pengguna yang tersimpan dalam basis data.
3. Penelitian ini hanya berfokus pada perancangan dan implementasi mekanisme keamanan pada basis data yang digunakan oleh rancangan *chatbot* PMI. Penelitian ini tidak mencakup pengembangan, implementasi maupun pengujian rancangan *chatbot* sebagai aplikasi pada lingkungan operasional (*real environment*).
4. Mekanisme perlindungan yang dirancang berfokus pada sisi basis data dan pengelolaan akses data. Aspek keamanan jaringan hanya dibatasi pada implementasi TLS untuk mengamankan komunikasi data antara aplikasi dan basis data sehingga tidak mencakup keamanan infrastruktur jaringan secara menyeluruh, server fisik, keamanan aplikasi (*application-level security*) maupun keamanan *endpoint* pengguna.

5. Implementasi dan pengujian dilakukan pada lingkungan pengembangan (*development*/*testing environment*) menggunakan data dan skenario simulasi yang disusun berdasarkan hasil wawancara dan kebutuhan sistem, sehingga tidak mencakup implementasi pada lingkungan operasional PMI secara langsung (*real environment*)
6. Penelitian tidak mencakup pengembangan dan implementasi *chatbot* secara penuh, melainkan hanya berfokus pada perancangan, implementasi dan evaluasi mekanisme perlindungan pada basis data yang mendukung sistem *chatbot* pada level *Database Management System* (DBMS).
7. Evaluasi penelitian difokuskan pada pengujian efektivitas mekanisme perlindungan basis data yang diimplementasikan dari aspek fungsionalitas, keamanan, dan performa. Evaluasi terhadap penggunaan sistem dalam lingkungan operasional serta aspek keamanan di luar ruang lingkup basis data tidak dibahas dalam penelitian ini.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dibuat, adapun tujuan dari penelitian ini yaitu:

1. Menerapkan dan menghasilkan mekanisme perlindungan basis data yang ditujukan untuk perancangan *chatbot* PMI dengan menggunakan beberapa metode yang mencakup enkripsi dan kontrol akses.
2. Melakukan evaluasi terhadap kinerja mekanisme perlindungan basis data chatbot PMI melalui pengujian keamanan data saat tersimpan, keamanan data saat transmisi, kontrol akses pengguna, ketahanan terhadap serangan basis data serta pengukuran dampaknya terhadap performa basis data.

1.4.2 Manfaat Penelitian

Penelitian ini dibuat dengan harapan dapat memberikan banyak manfaat. Manfaat dari penelitian ini yaitu sebagai berikut:

1. Manfaat Teoritis: Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang sistem

informasi khususnya terkait perancangan mekanisme perlindungan basis data pada layanan berbasis *chatbot* di sektor kesehatan. Penelitian ini dapat menambah referensi akademik mengenai penerapan enkripsi dan kontrol akses dalam lingkungan basis data hybrid yang mengombinasikan *structured database* dan *vector database*. Selain itu, hasil penelitian ini diharapkan dapat menjadi dasar bagi penelitian selanjutnya yang membahas keamanan data, privasi informasi, serta pengelolaan akses data pada sistem chatbot atau sistem informasi kesehatan berbasis teknologi digital.

2. Manfaat Praktis: Penelitian ini diharapkan dapat memberikan solusi dan rekomendasi bagi PMI dalam merancang dan menerapkan mekanisme perlindungan basis data yang aman pada sistem chatbot yang digunakan. Mekanisme yang dirancang diharapkan mampu membantu PMI dalam mencegah kebocoran data, membatasi akses terhadap informasi sensitif, serta menjaga integritas dan kerahasiaan data yang dikelola. Selain itu, penelitian ini juga diharapkan dapat menjadi acuan bagi organisasi atau institusi kesehatan lainnya dalam mengembangkan sistem chatbot yang aman tanpa mengurangi efektivitas layanan informasi kepada masyarakat.

1.5 Sistematika Penulisan

Terdapat sistematika penulisan yang akan diikuti dalam menyajikan laporan penelitian ini yaitu sebagai berikut:

BAB I PENDAHULUAN

Bagian ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat dari penelitian yang dilaksanakan. Bagian ini adalah komponen utama yang berfungsi sebagai pengantar dari permasalahan yang diangkat dan solusi yang ditawarkan pada penelitian ini

BAB II LANDASAN TEORI

Bagian ini akan berisi teori-teori yang digunakan sebagai landasan seputar topik yang diangkat dalam penelitian ini. Teori ini dikumpulkan dari berbagai sumber yaitu berbagai penelitian terdahulu dengan topik serupa, website resmi yang memberikan data kredibel dan buku yang informasinya relevan.

BAB III METODOLOGI PENELITIAN

Bagian ini berisi berbagai langkah-langkah yang dicapai untuk mencapai hasil yang telah ditetapkan pada penelitian ini. Bagian ini juga berisi gambaran umum terkait objek yang diangkat dalam penelitian beserta metode yang digunakan dalam melakukan perancangan.

BAB IV ANALISIS DAN HASIL PENELITIAN

Bagian ini berisi implementasi metode-metode yang telah disebutkan pada bagian sebelumnya dan mencantumkan hasil perancangan dari mekanisme perlindungan basis data yang telah diusulkan pada penelitian ini.

BAB V SIMPULAN DAN SARAN

Bagian ini akan berisi kesimpulan dari hasil pelaksanaan penelitian ini dan saran yang dapat diberikan untuk penelitian dengan topik serupa.