KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Nusantara (JINU)
Vol.2, No.4 Juli 2025
e-ISSN: 3047-7603, p-ISSN :3047-9673, Hal 183-197
DOI : https://doi.org/10.61722/jinu.v2i4.4997

KEAMANAN DATA DALAM SISTEM DATABASE

Annisa Hafsah
annisahfsh132@gmail.com
Universitas Islam Negeri Sumatera Utara
Aininta Alivia Br. Kaban
ainintaalivia@gmail.com
Universitas Islam Negeri Sumatera Utara
Said Luthfi Ramadhan
saidluthfi909@gmail.com
Universitas Islam Negeri Sumatera Utara
Nurbaiti
nurbaiti@uinsu.ac.id
Fakultas Ekonomi dan Bisnis Islam
Universitas Islam Negeri Sumatera Utara
Korespondensi Penulis: *annisahfsh132@gmail.com*

Abstract *The rapid development of information technology has encouraged various organizations to implement database-based management information systems (MIS) as a means of increasing operational efficiency and the quality of decision making. However, dependence on this system also increases vulnerability to data security disturbances, both from external parties such as cyber attacks and malicious software, as well as from internal parties through misuse of access rights. This research aims to analyze the effectiveness of implementing data protection mechanisms in management database systems using a literature study and case study approach. The research focus includes evaluation of encryption systems, role-based access control (RBAC), as well as threat detection and response systems in maintaining aspects of confidentiality, integrity and data availability. Simulations were carried out on two database management systems, namely MySQL and PostgreSQL, to assess how effective security features are in responding to attacks and their impact on system performance. The research results show that with proper security implementation, organizations can improve data protection without sacrificing system performance. In addition, this study emphasizes the important role of organizational awareness of information security as well as the need for internal regulations such as security training and implementing strong authentication. It is hoped that these findings will provide benefits both conceptually and practically for strengthening safe and reliable information systems in the organizational environment.*
Keywords: *Encryption, Data Security, Database System, Management Information System (SIM)*

Abstrak Perkembangan teknologi informasi yang pesat telah mendorong berbagai organisasi untuk menerapkan sistem informasi manajemen (SIM) berbasis database sebagai sarana peningkatan efisiensi operasional dan kualitas pengambilan keputusan. Akan tetapi, ketergantungan terhadap sistem ini juga meningkatkan kerentanan terhadap gangguan keamanan data, baik dari sisi eksternal seperti serangan siber dan perangkat lunak berbahaya, maupun dari pihak internal melalui penyalahgunaan hak akses. Penelitian ini bertujuan untuk menganalisis efektivitas penerapan mekanisme perlindungan data pada sistem database manajemen dengan menggunakan pendekatan studi literatur dan studi kasus. Fokus penelitian mencakup evaluasi sistem enkripsi, Role Bassed Acces Control (RBAC), serta sistem deteksi dan respons terhadap ancaman dalam menjaga aspek kerahasiaan, integritas, dan ketersediaan data. Simulasi dilakukan pada dua sistem manajemen basis data, yakni MySQL dan PostgreSQL, untuk menilai seberapa efektif fitur keamanan dalam merespons serangan serta dampaknya terhadap kinerja sistem. Hasil penelitian menunjukkan bahwa dengan implementasi keamanan yang tepat, organisasi dapat meningkatkan perlindungan data tanpa mengorbankan performa sistem. Selain itu, studi ini menekankan pentingnya peran kesadaran organisasi terhadap keamanan informasi serta perlunya regulasi internal seperti pelatihan keamanan dan penerapan autentikasi yang kuat. Diharapkan temuan ini memberikan manfaat baik secara konseptual maupun praktis bagi penguatan sistem informasi yang aman dan terpercaya di lingkungan organisasi.
Kata Kunci : Enkripsi, Keamanan Data, Sistem database, Sistem Informasi Manajemen (SIM)

Received April 28, 2025; Revised Mei 30, 2025; juni 05, 2025
* Annisa Hafsah, annisahfsh132@gmail.com

PENDAHULUAN

Perkembangan teknologi informasi yang begitu pesat telah membawa perubahan signifikan dalam cara organisasi mengelola sumber daya dan informasi. Salah satu implementasi teknologi tersebut adalah penerapan sistem informasi manajemen (SIM) yang berbasis database untuk mengelola data penting seperti kepegawaian, keuangan, aset, dan kinerja organisasi. Sistem ini dirancang untuk meningkatkan efisiensi operasional serta mendukung pengambilan keputusan strategis di level manajerial. Namun, semakin kompleks dan terintegrasinya sistem ini juga memperbesar risiko terhadap keamanan data. Oleh karena itu, keamanan data dalam sistem database menjadi isu krusial yang perlu mendapatkan perhatian serius, terutama dalam konteks manajemen organisasi.

Keamanan data dalam sistem informasi manajemen tidak hanya berkaitan dengan perlindungan terhadap kebocoran informasi, tetapi juga menyangkut integritas dan ketersediaan data. Informasi manajerial bersifat sensitif dan strategis, seperti data pegawai, gaji, evaluasi kinerja, dan struktur organisasi. Apabila data ini jatuh ke tangan yang salah atau mengalami modifikasi oleh pihak yang tidak berwenang, maka dampaknya dapat merusak proses pengambilan keputusan bahkan menimbulkan konflik internal dalam organisasi. Berbagai bentuk ancaman terhadap keamanan data telah diidentifikasi, mulai dari serangan siber seperti SQL Injection, malware, hingga ancaman internal dari pihak pengguna yang menyalahgunakan akses. Oleh karena itu, dibutuhkan penerapan strategi keamanan data yang mencakup aspek teknis maupun kebijakan organisasi. Pendekatan teknis dapat berupa penggunaan enkripsi, kontrol akses berbasis peran (RBAC), dan sistem deteksi intrusi (IDS). Sementara dari sisi kebijakan, organisasi perlu menetapkan standar operasional prosedur (SOP) serta melakukan pelatihan keamanan informasi kepada seluruh pengguna sistem.

Dalam penelitian ini, penulis mengacu pada studi kasus yang dibahas oleh (Daulay et al., 2023) dalam jurnal Edu Societ: Jurnal Pendidikan,Ilmu Sosial,dan Pengabdian Kepada Masyarakat yang membahas pentingnya sistem keamanan database dalam mendukung pengambilan keputusan manajerial. Studi ini menyoroti bahwa banyak organisasi belum memaksimalkan perlindungan data dalam sistem manajemen karena kurangnya kesadaran terhadap ancaman digital. Dengan pendekatan literatur, jurnal ini menunjukkan bahwa perlindungan fisik dan logis terhadap data sangat penting untuk

menjaga keandala sistem informasi manajemen. Hal ini bertujuan untuk mengevaluasi efektivitas penerapan mekanisme keamanan data dalam sistem database manajemen, khususnya melalui pendekatan kuantitatif. Fokus utama penelitian adalah menilai sejauh mana fitur keamanan seperti enkripsi dan pengelolaan hak akses dapat meningkatkan perlindungan terhadap data, tanpa mengganggu performa sistem. Pengujian dilakukan melalui simulasi skenario pada sistem informasi kepegawaian berbasis MySQL dan PostgreSQL, dengan parameter pengukuran berupa tingkat keberhasilan serangan simulasi, waktu tanggap sistem terhadap ancaman, serta evaluasi performa sistem setelah penerapan fitur keamanan.

Dengan pendekatan studi kasus yang berbasis pada sumber jurnal ilmiah penelitian ini diharapkan dapat memberikan gambaran yang aplikatif dan relevan dengan kebutuhan dunia manajemen. Kontribusi penelitian tidak hanya terletak pada aspek teknis, tetapi juga dalam memberikan rekomendasi kebijakan keamanan informasi yang dapat diterapkan oleh organisasi untuk meningkatkan ketahanan digital mereka. Dalam konteks manajemen modern yang berbasis data, sistem database tidak hanya berfungsi sebagai alat penyimpanan informasi, melainkan juga sebagai fondasi dari pengambilan keputusan dan perencanaan strategis. Oleh karena itu, keamanan sistem database merupakan bagian tak terpisahkan dari strategi pengelolaan organisasi. Penerapan keamanan data yang baik tidak hanya menjaga organisasi dari ancaman eksternal, tetapi juga menciptakan kepercayaan internal dan tata kelola yang transparan.

TINJAUAN TEORITIS

Keamanan Data Base

Keamanan database merupakan serangkaian langkah dan kebijakan yang dirancang untuk melindungi sistem basis data dari berbagai ancaman. Ancaman tersebut bisa bersifat disengaja, seperti peretasan atau pencurian data, maupun tidak disengaja, seperti kesalahan pengguna atau kegagalan sistem. Tujuan utama dari perlindungan ini adalah untuk memastikan kerahasiaan, integritas, dan ketersediaan data yang tersimpan. Perlindungan keamanan database tidak hanya berfokus pada data yang ada, tetapi mencakup keseluruhan komponen dalam sistem, termasuk perangkat lunak, perangkat keras, jaringan, serta akses pengguna. Oleh karena itu, upaya pengamanan memerlukan pendekatan yang menyeluruh, mulai dari penetapan hak akses, autentikasi pengguna,

hingga audit log yang memantau aktivitas dalam sistem. Agar sistem keamanan database dapat berfungsi secara efektif, diperlukan pengendalian yang ketat dan sistematis. Di sinilah peran Administrator Database (DBA) menjadi sangat penting (Rahmadi & Yunita, 2020). Seorang DBA bertanggung jawab untuk mengelola, memelihara, dan mengamankan database secara menyeluruh. Tugas mereka mencakup memberikan otorisasi kepada pengguna, mengatur cadangan dan pemulihan data, memperbarui sistem, serta memantau aktivitas mencurigakan dalam database. Beberapa strategi kunci dalam penerapan keamanan database meliputi pengendalian akses, otentikasi dan otorisasi, enkripsi data, audit dan logging, serta backup dan recovery. Penting bagi setiap organisasi untuk menyadari bahwa sistem database adalah aset yang sangat vital. Oleh karena itu, investasi dalam keamanan database bukan hanya langkah teknis untuk proteksi, tetapi juga merupakan upaya untuk menjaga keberlanjutan operasional, kepercayaan pengguna, dan reputasi perusahaan secara keseluruhan.

Role-Based Acces Control (RBAC)

Role-Based Access Control (RBAC) merupakan salah satu pendekatan dalam sistem manajemen kontrol akses yang mendasarkan hak akses pengguna pada peran atau jabatan yang dimilikinya dalam suatu organisasi. Model ini bertujuan untuk menyederhanakan proses pemberian otorisasi dengan mengelompokkan pengguna berdasarkan tanggung jawab atau fungsi mereka di dalam struktur organisasi. Dalam implementasinya, RBAC memberikan efisiensi pengelolaan hak akses dengan menjadikan peran sebagai penghubung antara pengguna dan izin akses. Salah satu keunggulan utama dari RBAC adalah stabilitas relasi antara peran dan izin akses, di mana perubahan lebih sering terjadi pada hubungan antara pengguna dan peran daripada antara peran dan izin. Hal ini secara langsung mengurangi kompleksitas administratif serta menurunkan beban manajemen sistem. RBAC juga mampu mengakomodasi kebijakan keamanan yang dinamis dan adaptif terhadap kebutuhan perubahan struktur sistem, menjadikannya fleksibel untuk berbagai skenario organisasi (Yuricha & Phan, 2023).

Secara operasional, penggunaan RBAC memungkinkan distribusi hak akses yang lebih intuitif dan mudah dimengerti. Dengan struktur hierarki peran yang dapat mencerminkan level organisasi, sistem dapat menyajikan kontrol akses yang sesuai dengan tingkatan pengguna. Selain itu, RBAC mendukung konsep reusability yang

tinggi, karena peran yang telah ditentukan dapat digunakan kembali oleh banyak pengguna yang memiliki tanggung jawab serupa. Melalui pengelompokan pengguna berdasarkan jabatan dan pemberian akses yang melekat pada jabatan tersebut, proses manajemen hak akses menjadi lebih sistematis dan mudah dipelihara. Oleh karena itu, RBAC dianggap sebagai pendekatan yang efektif dan efisien dalam mengatasi tantangan pengelolaan akses di lingkungan perusahaan, khususnya dalam sistem yang memiliki banyak pengguna dan kompleksitas tinggi dalam struktur organisasi.

MySQL

MySQL merupakan salah satu sistem manajemen basis data relasional (Relational Database Management System atau RDBMS) yang bersifat open-source dan banyak digunakan secara luas di berbagai platform. Sistem ini menggunakan Structured Query Language (SQL) sebagai bahasa utama untuk melakukan operasi terhadap data, seperti penyimpanan, pengambilan, pembaruan, dan penghapusan. Dengan menyusun data dalam bentuk tabel yang terdiri dari baris dan kolom, MySQL memungkinkan pengelolaan informasi yang terstruktur serta membangun relasi antar-tabel secara sistematis. MySQL bekerja berdasarkan arsitektur client-server, di mana perangkat klien mengirimkan perintah dalam bentuk query SQL kepada server. Server MySQL kemudian memproses permintaan tersebut dan mengembalikan hasilnya kepada klien. Kemampuan MySQL dalam menangani banyak pengguna secara bersamaan (multi-user) dan mendukung skala basis data besar menjadikannya pilihan utama dalam pengembangan aplikasi, khususnya di lingkungan web. Secara fungsional, MySQL memiliki beberapa kegunaan utama, yaitu:

- Menyimpan data dalam struktur tabel yang relasional.
- Mengambil data sesuai kebutuhan melalui sintaks SQL yang fleksibel.
- Memungkinkan perubahan dan penghapusan data dengan presisi.
- Menjamin integritas data melalui dukungan sistem transaksi yang handal.

Popularitas MySQL juga dipengaruhi oleh sifatnya yang terbuka untuk publik (open-source), sehingga mudah diakses, dikembangkan, dan disesuaikan oleh berbagai kalangan, termasuk pengembang independen hingga perusahaan besar. Keunggulan ini membuat MySQL menjadi fondasi penting dalam pengembangan sistem informasi, terutama yang berbasis website atau aplikasi daring. Singkatnya, MySQL merupakan

solusi database server yang efisien dan fleksibel untuk menyimpan serta mengelola data, didukung oleh ekosistem dan komunitas global yang terus berkembang (Silalahi, Fujiama Diapoldo, S.Kom, 2022).

PostgreSQL

PostgreSQL merupakan salah satu sistem manajemen basis data relasional berorientasi objek (Object-Relational Database Management System atau ORDBMS) yang dikenal karena kestabilan, fleksibilitas, dan dukungannya terhadap berbagai fitur canggih. Sebagai perangkat lunak sumber terbuka (open-source), PostgreSQL tidak hanya dapat digunakan secara bebas tanpa lisensi komersial, tetapi juga memungkinkan pengembang untuk memodifikasi dan menyesuaikannya sesuai kebutuhan spesifik sistem informasi yang dibangun. Proyek pengembangan PostgreSQL berakar dari University of California di Berkeley, melalui Berkeley Computer Science Department, yang kemudian terus berkembang menjadi salah satu database server paling andal di dunia. PostgreSQL dilengkapi dengan berbagai kemampuan yang sebelumnya hanya dimiliki oleh sistem database komersial, seperti dukungan penuh terhadap perintah SQL standar, kemampuan menyusun kueri kompleks dengan klausa yang beragam, dan manajemen hak akses pengguna yang granular hingga tingkat kolom data (Munawaroh, 2005).

Salah satu kekuatan utama PostgreSQL adalah fleksibilitas dalam pengelolaan data dan kontrol pengguna. Administrator database dapat menetapkan hak akses secara rinci terhadap pengguna, bahkan hingga pembatasan akses ke kolom tertentu dalam suatu tabel. Hal ini memperkuat sistem keamanan dan menjaga kerahasiaan data dalam lingkungan multi-user. Selain itu, PostgreSQL mendukung pembuatan fungsi, stored procedures, dan triggers, yang memungkinkan logika bisnis dijalankan langsung pada sisi server. Pendekatan ini tidak hanya mempercepat proses eksekusi data karena mengurangi beban pada klien, tetapi juga membuat aplikasi yang dibangun lebih ringan, terutama untuk model thin client. Dalam hal integrasi dengan teknologi lain, PostgreSQL sangat kompatibel dengan berbagai bahasa pemrograman populer, baik untuk pengembangan aplikasi desktop (seperti Java dan Gambas) maupun web (seperti Python, PHP, Java Server Pages, dan Perl). Hal ini menjadikannya pilihan utama dalam pengembangan sistem informasi modern yang membutuhkan fleksibilitas tinggi dan skalabilitas tanpa batas. Singkatnya, PostgreSQL adalah solusi basis data tingkat lanjut yang menawarkan

keseimbangan antara fitur, keamanan, kinerja, dan kemudahan integrasi. Kemampuan untuk menangani kebutuhan kompleks dalam pengelolaan data menjadikan PostgreSQL sangat ideal untuk berbagai skenario pengembangan perangkat lunak, baik skala kecil hingga enterprise.

Perspektif organisasi terhadap keamanan Sistem

Keamanan sistem informasi bukan hanya sekadar tanggung jawab teknis, melainkan juga merupakan elemen krusial dalam strategi keseluruhan suatu organisasi. Dari sudut pandang organisasi, keamanan sistem informasi mencakup berbagai komponen penting yang saling terhubung dan mendukung satu sama lain. Organisasi dituntut untuk melindungi aset informasi dengan efektif, mematuhi regulasi dan standar yang berlaku, serta menerapkan manajemen risiko dengan cara mengidentifikasi potensi ancaman dan kerentanan. Dukungan dari manajemen dan penerapan tata kelola yang baik adalah kunci untuk menciptakan budaya keamanan yang berkelanjutan. Lebih lanjut, meningkatkan kesadaran dan pemahaman karyawan mengenai isu-isu keamanan melalui program pelatihan merupakan langkah penting dalam meminimalkan kemungkinan kesalahan manusia. Penggunaan teknologi keamanan mutakhir perlu diimbangi dengan kesiapan untuk merespons insiden secara cepat dan efektif. Semua elemen ini menunjukkan bahwa keamanan sistem informasi tidak hanya merupakan tanggung jawab teknis, tetapi juga merupakan aspek strategis yang mendukung keberlangsungan dan reputasi organisasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan untuk memahami secara mendalam bagaimana keamanan data diterapkan dalam sistem database, terutama dalam lingkungan organisasi. Informasi dalam penelitian ini dikumpulkan melalui studi pustaka, yaitu dengan membaca dan mengkaji berbagai sumber seperti jurnal ilmiah, artikel, dan dokumen lain yang membahas keamanan database, sistem informasi manajemen, dan pengaturan akses pengguna berdasarkan peran (RBAC). Dalam menganalisis data, peneliti mengelompokkan ide-ide utama yang ditemukan dari berbagai sumber, lalu membandingkannya dengan teori yang sudah ada untuk mendapatkan pemahaman yang lebih jelas tentang cara kerja perlindungan data. Penelitian ini lebih fokus pada pemahaman teori dan penerapan nyatanya, bukan pada angka atau data statistik. Hasil dari penelitian ini diharapkan bisa memberikan gambaran

menyeluruh tentang pentingnya perlindungan data untuk mendukung pengelolaan organisasi yang lebih baik dan meningkatkan keamanan digital.

HASIL DAN PEMBAHASAN

A. Penerapan Enskripsi dalam Sistem Database

Enkripsi adalah proses mengubah data yang mudah dibaca menjadi format yang tidak dapat dipahami, sehingga hanya individu dengan akses yang sah yang dapat mengembalikannya ke bentuk semula. Tujuan utama dari enkripsi adalah untuk melindungi informasi sensitif agar tidak jatuh ke tangan yang tidak berwenang, terutama di tengah maraknya ancaman siber seperti phishing, peretasan, pencurian identitas, dan carding. Dengan mengenkripsi data, informasi penting akan tetap aman meskipun pihak yang tidak bertanggung jawab berhasil mengakses system (Rahmadi & Yunita, 2020). Dalam sistem database, enkripsi memainkan peran penting sebagai metode pengamanan. Basis data sering kali menyimpan informasi yang sangat sensitif, seperti data pengguna, informasi finansial, catatan medis, dan data strategis lainnya. Oleh karena itu, penerapan enkripsi dalam database bertujuan untuk memastikan bahwa data tersebut tetap terlindungi meskipun terjadi pelanggaran keamanan. Enkripsi dapat diterapkan pada berbagai level, mulai dari tingkat kolom (seperti mengenkripsi nomor kartu kredit atau password) hingga enkripsi pada seluruh database. Banyak sistem manajemen basis data modern, seperti MySQL, PostgreSQL, atau Oracle, yang menyediakan fitur enkripsi data transparan (TDE). Dengan menggunakan TDE, data yang disimpan di disk akan dienkripsi secara otomatis tanpa perlu mengubah aplikasi secara signifikan. Ketika pengguna yang sah mengakses data, sistem akan mendekripsinya secara otomatis. Pendekatan ini memastikan keseimbangan antara keamanan dan kinerja. Selain itu, manajemen kunci enkripsi juga merupakan aspek penting, di mana kunci-kunci enkripsi disimpan dengan aman dan hanya dapat diakses oleh pihak yang memiliki otorisasi. Dengan demikian, enkripsi menjadi elemen penting dalam memastikan kerahasiaan, integritas, dan ketersediaan data dalam sistem database.

B. Pengaruh Enskripsi dalam pengaturan akses

Enkripsi memiliki peran penting dalam menjaga keamanan informasi sekaligus mengatur hak akses terhadap data yang bersifat sensitif. Dengan mengenkripsi data,

hanya pihak yang memiliki kunci autentikasi yang tepat yang dapat membaca atau mengakses informasi tersebut. Hal ini sangat efektif untuk mencegah kebocoran data, karena walaupun sistem berhasil ditembus, isi data tetap tidak dapat dimengerti oleh pihak yang tidak berwenang. Sistem enkripsi yang menggabungkan penggunaan kunci publik dan kunci privat yang dikenal sebagai kriptografi hibrida memberikan perlindungan lebih kuat dalam pengaturan akses (Wulandari & Hwihanus, 2023). Kunci publik digunakan untuk mengenkripsi informasi, sementara proses dekripsi hanya dapat dilakukan oleh pemilik kunci privat yang sah. Mekanisme ini menjamin bahwa akses terhadap data benar-benar terbatas pada pihak tertentu, dan sangat ideal digunakan dalam sistem-sistem yang membutuhkan tingkat keamanan tinggi, seperti layanan keuangan atau komunikasi rahasia antar lembaga. Selain itu, enkripsi juga dapat memperkuat sistem manajemen akses berbasis peran (Role-Based Access Control/RBAC), dengan menetapkan kunci enkripsi berbeda sesuai level otorisasi masing-masing pengguna. Dengan begitu, informasi hanya dapat diakses oleh individu dengan hak akses yang sesuai, sekaligus membatasi ruang gerak pengguna internal yang tidak memiliki wewenang. Penerapan teknik ini mampu meningkatkan perlindungan data secara menyeluruh, memperkecil potensi ancaman dari dalam, serta memperkuat kepercayaan terhadap keamanan sistem digital yang digunakan.

Dalam konteks organisasi atau perusahaan, enkripsi berfungsi sebagai fondasi utama dalam arsitektur keamanan data. Melalui penerapan kebijakan akses berbasis enkripsi, perusahaan dapat memastikan bahwa data strategis hanya dapat diakses oleh karyawan dengan tanggung jawab tertentu. Ini tidak hanya membantu melindungi rahasia bisnis, tetapi juga mendukung kepatuhan terhadap regulasi perlindungan data. Selain itu, integrasi enkripsi ke dalam system manajemen akses juga menciptakan audit trail yang jelas, sehingga memudahkan pengawasan dan deteksi terhadap aktivitas mencurigakan di dalam jaringan perusahaan.

C. Kontrol akses pengguna RBCA

Role-Based Access Control (RBAC) merupakan salah satu pendekatan dalam sistem kontrol akses yang mengatur hak akses pengguna berdasarkan peran atau jabatan mereka dalam organisasi. Berbeda dengan metode kontrol akses lainnya seperti Mandatory Access Control (MAC) dan Discretionary Access Control (DAC), RBAC tidak memberikan izin akses langsung kepada masing-masing individu,

melainkan melalui pengelompokan berdasarkan jabatan. Pendekatan DAC dan MAC cenderung menghadapi kendala dalam hal skalabilitas, terutama ketika jumlah pengguna dan sumber daya dalam sistem terus bertambah, yang menjadikannya kurang efisien dalam pengelolaan akses. Salah satu keunggulan utama RBAC adalah kemampuannya dalam menyederhanakan proses manajemen hak akses, karena perubahan izin biasanya hanya perlu dilakukan pada tingkat peran, bukan per individu. Hal ini mengurangi beban administrasi serta meningkatkan fleksibilitas dalam merespons perubahan struktur organisasi. Selain itu, RBAC mempermudah dalam menetapkan otorisasi yang bersifat hierarkis, sejalan dengan tingkatan jabatan pengguna dalam organisasi. Pendekatan ini juga mendukung penerapan kebijakan keamanan secara adaptif dan dapat digunakan kembali di berbagai bagian sistem, menjadikannya lebih efisien dari segi operasional.

Dalam konteks perusahaan seperti PT XYZ, penerapan RBAC memungkinkan pembagian hak akses yang lebih terstruktur, di mana setiap jabatan diberikan akses ke fitur sistem yang relevan. Dengan demikian, pemeliharaan dan pengelolaan hak akses menjadi lebih mudah, khususnya pada perusahaan dengan jumlah pegawai yang besar. RBAC terbukti relevan dan sesuai untuk mengatasi permasalahan manajemen hak akses di lingkungan kerja yang kompleks. Studi ini menunjukkan bahwa penerapan RBAC dalam organisasi, terutama pada institusi dengan sifat kolaboratif, mampu meningkatkan keamanan serta efisiensi dalam pengelolaan sumber daya dan informasi. Fokus dari penelitian ini terletak pada pengembangan sistem otorisasi terpusat dengan menggunakan model RBAC, berbeda dengan penelitian Dr. Asif yang menitikberatkan pada arsitektur hierarkis RBAC. Model RBAC yang diusulkan akan diintegrasikan ke dalam sistem informasi PT XYZ untuk menyederhanakan proses pengelolaan hak akses berdasarkan jabatan pengguna (Prasetia & Manongga, 2024) .

Proses penelitian dimulai dengan memahami konsep dasar RBAC serta kelebihan dan kekurangannya dalam pengaturan akses. Selanjutnya dilakukan analisis terhadap sistem informasi yang telah digunakan di PT XYZ untuk mengidentifikasi kebutuhan dan kelemahan yang ada. Berdasarkan hasil tersebut, dirancanglah sistem baru dengan pendekatan RBAC yang kemudian diimplementasikan dan diuji guna memastikan kesesuaian dengan spesifikasi awal dan kebutuhan organisasi. Dengan

penerapan RBAC, perusahaan dapat mengelola hak akses secara lebih efisien dan aman, terutama pada struktur organisasi yang bersifat hierarkis. Pengaturan akses berdasarkan jabatan memungkinkan efisiensi tinggi dan kemudahan dalam pemeliharaan sistem, dibandingkan dengan pemberian akses individu secara manual yang memakan waktu dan rentan terhadap kesalahan. Oleh karena itu, RBAC menjadi solusi ideal dalam mengelola otorisasi sistem informasi perusahaan secara terstruktur dan efektif.

D. Analisis perbandingan MySQL dan PostgreSQL

Pemilihan sistem manajemen basis data (DBMS) merupakan elemen yang sangat vital dalam perancangan sistem, terutama karena sistem ini akan digunakan untuk mengelola data dalam jumlah besar dan harus mampu mempertahankan performa yang stabil. Dua aplikasi database yang sering digunakan dan akan dibandingkan dalam konteks ini adalah MySQL dan PostgreSQL. MySQL telah lama dikenal sebagai salah satu sistem database yang paling banyak digunakan. Sejak dirilis secara publik pada tahun 2000 di bawah lisensi GNU GPL, MySQL dengan cepat meraih popularitas. Kemampuannya dalam menangani ribuan tabel dan miliaran baris data dengan efisien menjadikannya pilihan utama untuk berbagai jenis aplikasi. MySQL dikenal sebagai RDBMS (Relational Database Management System) yang mendukung pemrosesan data cepat dan dapat digunakan oleh banyak pengguna secara bersamaan. Keunggulannya terletak pada struktur yang simpel, efisiensi pengelolaan tabel, serta kemampuannya untuk menangani beban kerja yang besar.

Sementara itu, PostgreSQL merupakan sistem manajemen basis data relasional berbasis objek (ORDBMS) yang bersifat open source. Ketersediaannya secara bebas memungkinkan pengguna untuk memodifikasi dan mengembangkan sesuai kebutuhan. PostgreSQL mendukung berbagai fitur canggih, termasuk transaksi tingkat lanjut, subquery kompleks, pemicu (triggers), serta integritas data yang tinggi. Sistem ini juga kompatibel dengan berbagai platform seperti Linux, Windows, MacOS, dan Unix, serta menawarkan fleksibilitas dalam pemodelan data dan dukungan penuh terhadap standar SQL. Dalam dunia pengembangan perangkat lunak, baik MySQL maupun PostgreSQL sama-sama memiliki reputasi yang kuat dalam hal kinerja, keamanan, dan fleksibilitas. Oleh sebab itu, keduanya banyak digunakan oleh berbagai jenis organisasi, mulai dari perusahaan rintisan hingga

perusahaan besar. Namun, masing-masing memiliki kekuatan tersendiri dalam penyediaan solusi basis data yang optimal(Ahsana et al., 2023).

Analisis performa antara kedua DBMS ini menjadi penting, terutama dalam konteks aplikasi berskala besar atau yang memproses data kompleks. Aspek performa yang dianalisis meliputi waktu respons query, kemampuan optimasi perintah, penggunaan indeks, serta konfigurasi sistem yang dapat memengaruhi kinerja secara keseluruhan. Untuk itu, pengujian performa dilakukan melalui eksekusi berbagai query dan membandingkan waktu respon masing-masing sistem. Dari hasil perbandingan tersebut, dapat disimpulkan bahwa PostgreSQL cenderung menunjukkan performa yang lebih unggul dibandingkan MySQL, khususnya ketika digunakan untuk mengelola database dengan jumlah record yang sangat besar. Meski demikian, performa akhir juga sangat dipengaruhi oleh spesifikasi perangkat keras, sistem operasi yang digunakan, serta pengaturan perangkat lunak secara keseluruhan. Oleh karena itu, pemilihan DBMS harus mempertimbangkan kebutuhan aplikasi, skala data, dan karakteristik pengguna sistem secara menyeluruh (Praba & Safitri, 2020).

E. Kecepatan respon terhadap ancaman

Keamanan siber merupakan elemen penting dalam melindungi data, sistem, dan infrastruktur digital dari berbagai ancaman yang berasal dari dunia maya, seperti peretasan, malware, dan pencurian informasi. Fungsinya mencakup menjaga kerahasiaan data pribadi, memastikan integritas informasi tetap utuh, serta menjamin ketersediaan layanan bagi pengguna yang sah. Dalam dunia yang semakin terkoneksi secara digital, keamanan siber juga berperan besar dalam membangun kepercayaan terhadap layanan online dan transaksi digital. Selain perlindungan data, keamanan siber sangat penting dalam menjaga stabilitas berbagai sektor penting, seperti perbankan, energi, dan layanan kesehatan. Penerapan sistem keamanan yang kuat juga membantu organisasi mematuhi regulasi yang berlaku, mengurangi risiko pencurian identitas, dan menjaga reputasi bisnis. Dalam menghadapi serangan yang semakin kompleks dan canggih, organisasi perlu mengembangkan kesadaran dan budaya keamanan digital yang menyeluruh di semua lini (Santoso, 2023).

Kecepatan respons terhadap ancaman siber menjadi kunci dalam mengurangi dampak kerusakan. Deteksi dini dan tindakan cepat memungkinkan organisasi untuk

mengisolasi ancaman sebelum menyebar lebih luas, memulihkan sistem lebih efisien, dan mempertahankan kelangsungan operasional. Oleh karena itu, sistem keamanan yang efektif harus bersifat preventif dan responsif, didukung oleh teknologi real-time serta tim yang siap bertindak. Dengan pendekatan ini, keamanan siber mampu menciptakan ekosistem digital yang lebih aman dan berkelanjutan.

F. Kesadaran, keamanan dan kebijakan Organisasi

Salah satu bentuk kontrol autentikasi yang paling sering diterapkan dalam sistem informasi adalah penggunaan kata sandi. Namun, masih banyak celah dalam pemahaman karakteristik password yang umum digunakan dalam kehidupan sehari-hari. Kombinasi kata sandi yang lemah dan mudah ditebak kerap menjadi sasaran empuk bagi peretas, terutama saat mereka menggunakan berbagai metode seperti keylogger, phishing, shoulder surfing, serangan kamus (dictionary attack), hingga rainbow table. Kondisi ini menuntut pengguna untuk lebih berhati-hati ketika mengakses berbagai layanan digital seperti situs web dan penyimpanan berbasis cloud yang membutuhkan verifikasi login dengan username dan password. Dalam keseharian, hampir setiap orang menggunakan username dan password untuk masuk ke berbagai layanan digital. Proses ini dikenal sebagai autentikasi, yaitu metode yang digunakan untuk memastikan identitas pengguna yang mencoba mengakses suatu sistem (Jadhao & Dole, 2013). Setiap organisasi biasanya menetapkan standar autentikasi yang berbeda, tergantung pada tingkat sensitivitas dan kebutuhan sistem yang dimiliki. Tujuan utamanya adalah mencegah akses yang tidak sah serta menjaga integritas dan keamanan data. Mekanisme ini diterapkan secara luas, termasuk di instansi pemerintahan, militer, rumah sakit, dan berbagai sektor bisnis (Jansen, 2015). Dengan meningkatnya jumlah serangan siber dan pelanggaran data, kesadaran akan pentingnya keamanan digital pun semakin tinggi. Sayangnya, masih banyak pengguna yang membuat kesalahan umum dengan memilih kata sandi yang terlalu sederhana, seperti ‘123456’, ‘password’, atau kombinasi serupa yang sangat mudah ditebak. Tantangan lainnya adalah kecenderungan menggunakan informasi pribadi dalam pembuatan password, yang justru meningkatkan risiko peretasan. Meskipun kata sandi yang kompleks, minimal delapan karakter dan mengandung kombinasi huruf, angka, serta simbol, dapat memperlambat proses peretasan, kesalahan sering terjadi ketika satu password digunakan di berbagai platform. Hal ini membuka celah

yang lebih besar bagi pelaku kejahatan siber untuk mengakses banyak akun hanya dengan satu informasi login (Komalasari, 2018).

KESIMPULAN

Penelitian ini menyimpulkan bahwa penerapan strategi perlindungan data yang tepat dalam sistem manajemen basis data sangat krusial untuk menjaga aspek kerahasiaan, integritas, dan ketersediaan informasi. Studi ini menggarisbawahi pentingnya penggunaan teknologi seperti enkripsi, kontrol akses berbasis peran atau Role Bassed Acces Control (RBAC), serta mekanisme deteksi ancaman dalam menghadapi risiko dari pihak luar maupun dalam organisasi. Temuan menunjukkan bahwa sistem keamanan yang dirancang dengan baik mampu memberikan perlindungan optimal terhadap data tanpa mengganggu performa sistem secara keseluruhan.

Selain itu, pemahaman dan kesadaran organisasi mengenai pentingnya keamanan informasi, disertai dengan kebijakan internal yang memadai, merupakan elemen vital dalam menciptakan sistem informasi yang kuat dan terpercaya. Penulis juga merekomendasikan adanya pelatihan bagi pengguna sistem serta penerapan autentikasi yang aman sebagai tindakan pencegahan. Namun, ruang lingkup penelitian ini terbatas pada dua jenis DBMS, yaitu MySQL dan PostgreSQL, sehingga belum mencakup keseluruhan variasi sistem database yang ada. Untuk pengembangan selanjutnya, disarankan agar penelitian mencakup lebih banyak platform database guna memperoleh hasil yang lebih komprehensif dan aplikatif.

DAFTAR PUSTAKA

Ahsana, S. H., Syahputra, M. B., Putri, A. F. F. M., & Prasetyo, A. A. (2023). ANALISIS PERBANDINGAN PERFORMA ANTARA MySQL dan PostgreSQL. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi (SITASI)*.

Daulay, A. P. E., Febriana, V., Kita, A. D. A., Gunawan, S., & Nurbaiti, N. (2023). Keamanan dalam Sistem Database Sebagai Sumber Informasi Manajemen Terhadap Perlindungan Data. *Edu Society: Jurnal Pendidikan, Ilmu Sosial Dan Pengabdian Kepada Masyarakat*, *3*(2), 988–991.

Komalasari, R. (2018). Kesadaran Akan Keamanan Penggunaan Username Dan Password. *TEMATIK*, *5*(2), 141–152.

Munawaroh, S. (2005). Mengeksplorasi Database PostgreSQL dengan PgAdmin III. *Dinamik*, *10*(2).

Praba, A. D., & Safitri, M. (2020). Studi perbandingan performansi antara mysql dan

postgresql. *Jurnal Khatulistiwa Informatika*, *8*(2).

Prasetia, Y. A., & Manongga, D. (2024). ROLE-BASED ACCESS CONTROL (RBAC) UNTUK SISTEM OTORISASI TERPUSAT BERBASIS FLASK STUDI KASUS PT. XYZ. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *9*(4), 1768–1778.

Rahmadi, P., & Yunita, H. D. (2020). Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi. *Jurnal Cendikia*, *19*(1), 413–418.

Santoso, J. T. (2023). Teknologi Keamanan Siber (Cyber Security). In *Penerbit Yayasan Prima Agus Teknik*. https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/458%0Ahttps://penerbit.stekom.ac.id/index.php/yayasanpat/article/download/458/483

Silalahi, Fujiama Diapoldo, S.Kom, M. K. (2022). *Manajemen Databse MySQL*. 1–158.

Wulandari, I. W., & Hwihanus, H. (2023). Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan. *Jurnal Kajian Dan Penalaran Ilmu Manajemen*, *1*(1), 11–25.

Yuricha, Y., & Phan, I. K. (2023). Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud: The Implementation of Role Based Access Control in a Cloud-Based Supply Chain Management System. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *3*(2), 339–348.