Socius: Jurnal Penelitian Ilmu-Ilmu Sosial
Volume 02, Nomor 12, June 2025, P. 561-567
E-ISSN: 3025-6704
DOI: https://doi.org/10.5281/zenodo.15683326

Analisis Implementasi Model Kontrol Akses Berbasis Peran dan Enkripsi untuk Keamanan Data pada Sistem Basis Data Relasional

Fatimah az Zahra, Muhammad Irwan Padli Nasution
[12]Universitas Islam Negeri Sumatera Utara

ARTICLE INFO

Article history:
Received May 15, 2025
Revised May 23, 2025
Accepted May 28, 2025
Available online June 08, 2025

Keywords
Data security, rational database, information security

ABSTRACT

Although data is now produced very quickly, databases remain a collection of structured information that is easy to access, manage, and update. To monitor sales transactions, product stock, customer data, and marketing strategies, companies need a good database system. The Database Management System (DBMS) is an important element in the process of managing and manipulating this data. In making decisions related to data security and efficiency, careful consideration is needed so that important information remains well protected. Understanding security risks in database systems and preventing them does require in-depth knowledge, considering that information is a very important asset for every company. Therefore, this paper discusses various important aspects related to database security, including the latest technologies that can help protect data from possible threats.

ABSTRAK

Meskipun data kini diproduksi dengan sangat cepat, basis data tetap menjadi kumpulan informasi yang terstruktur dan mudah diakses, dikelola, serta diperbarui. Untuk memantau transaksi penjualan, stok produk, data pelanggan, hingga strategi pemasaran, perusahaan membutuhkan sistem basis data yang baik. Sistem Manajemen Basis Data (DBMS) menjadi elemen penting dalam proses pengelolaan dan manipulasi data tersebut. Dalam pengambilan keputusan yang berkaitan dengan keamanan dan efisiensi data, dibutuhkan pertimbangan yang matang agar informasi penting tetap terlindungi dengan baik. Memahami risiko keamanan dalam sistem basis data dan mencegahnya memang membutuhkan pengetahuan yang mendalam, mengingat informasi merupakan aset yang sangat penting bagi setiap perusahaan. Oleh karena itu, makalah ini membahas berbagai aspek penting terkait keamanan basis data, termasuk teknologi terbaru yang dapat membantu melindungi data dari ancaman yang mungkin terjadi.

PENDAHULUAN

Pengelolaan basis data relasional menjadi aspek yang penting seiring dengan berjalannya perkembangan teknologi informasi. Basis data relasional memiliki fungsi yaitu untuk menjaga dan menyimpan informasi yang terkait dan menjadi data yang yang sangat penting bagi organisasi. Namun, dengan berkembangnya teknologi informasi ini, ancaman terhadap keamanan data juga meningkat yang dimana data tersebut berupa akses tidak sah, mnipulasi data, maupun kebocoran informasi yang terkait. Hal seperti ini tidak diabaikan karna dapat membuat keresahan bagi penggunanya.

Keamanan data dalam basis data relasional harus melakukan langkah yang cermat seperti memilih model keamanan yang bisa melindungi data dari ancaman atau risiko. Adapun beberapa jenis dari keamanan yang sering digunakan yaitu kontrol akses, enkripsi, serta sistem audit yang memantau aktivitas dalam bentuk data. Dengan penerapan sistem-sistem keamanan ini, organisasi dapat memeriksa apakah data yang mereka kelola itu tetap terlindungi dari ancaman yang dapat merusak integritasnya.

Perlu diingat bahwa keamanan data bukan hanya masalah teknis; kebijakan dan kesadaran sumber daya manusia yang mengelola data juga berperan. Banyak kebocoran terjadi karena kesalahan yang tidak disadari atau kelalaian pengguna.

Paper ini bertujuan untuk mengeksplorasi berbagai model keamanan yang diterapkan dalam basis data relasional dan menilai bagaimana masing-masing model dapat menghadapi tantangan yang muncul dalam dunia yang semakin bergantung pada data.

*Corresponding Author
Email: faz83307@gmail.com, irwannst@uinsu.ac.id

METODE

Penelitian ini menggunakan metode penulisan literature review (studi pustaka) dengan pendekatan kualitatif deskriptif. Data yang diperoleh berasal dari berbagai sumber, termasuk jurnal ilmiah, buku, dan laporan industri yang berhubungan dengan topik data referensi dan data master. Selain itu, penelitian ini juga melakukan analisis terhadap beberapa studi kasus perusahaan yang telah berhasil menerapkan sistem pengelolaan data master secara efisien untuk menilai dampaknya terhadap peningkatan efisiensi dalam proses bisnis.

HASIL DAN PEMBAHASAN

Keamanan data adalah hal yang dilakukan di dasar dan tidak bisa abaikan dalam proses pengejaan dan pengelolaan data di informai digital. Dalam sistem pengelolaan ini, data-data disimpan didalam bentuk tabel dan saling terkoneksi atau terhubung sehingga menjadikan data rapi dan juga efisien. Walaupun begitu, struktur relasional yang rumit juga memungkinkan terjadinya kebocoran, terutama jika sistem tidak dikelola oleh sistem yang merata. Masalah bisa datang darimana saja, dimulai dari akses yang illegal, manipulasi data, sabotase, hingga penggunaan sembarangan oleh pihak internal.

Basis data relasional adalah penyimpanan data yang merupakan sistem dalam mengorganisasikan informasi kedalam bentuk tabel-tabel yang saling terikat atau terhubung dengan cara melalui kunci primer dan kunci asing. Struktur ini dapat memberikan efisiensi di dalam penyimpanan serta pengambilan data yag mudah. Selain itu, struktur ini juga dapat membuat konsistensi dalam membuat data. Tetapi, terkadang ada muncul kompleksitas yang mendatangkan berbagai masalah pada keamanan yang serius. Seiring dengan berkembangnya jumlah dan nilai data dalam organisasi modern, risiko terhadap basis data pun meningkat.

Salah satu tantangannya yang utama adalah akses. Hal ini dapat terjadi jika pengguna yang tidak memiliki hak ingin mencoba mengakses data yag sensiitf. Pelanggaran seperti ini bisa terjadi baik dari luar sistem, contohnya serangan SQL injection, maupun dari dalam organisasi, seperti pegawai yang menyabotase atau menyalahgunakan akses. Menurut Kamra, Bertino, dan Terzi (2008), ancaman dari dalam justru lebih berbahaya karena pelaku sudah mengetahui sistem dan memiliki akses yang sah, sehingga lebih sulit terdeteksi.

Masalah berikutnya adalah manipulasi data, yang terjadi ketika data diubah secara ilegal untuk kepentingan pihak tertentu. Pemalsuan transaksi, perubahan data pelanggan, dan penghapusan bukti digital adalah beberapa contoh penipuan ini. Reputasi publik, kepercayaan publik, dan legitimasi operasi organisasi semuanya dapat dipengaruhi oleh manipulasi data. Hartono (2013) menjelaskan bahwa ketidakkonsistenan data yang disebabkan oleh manipulasi dapat merusak integritas data dalam basis data. Pada akhirnya, hal ini dapat berdampak negatif pada sistem informasi manajemen secara keseluruhan.

Penyalahgunaan internal oleh pengguna resmi juga menjadi masalah besar. Administrator basis data dan orang lain dengan hak istimewa mungkin menyalahgunakan wewenang mereka. Seringkali, organisasi mengabaikan prinsip "hak terkecil", yang berarti memberikan akses hanya sebatas yang diperlukan untuk menyelesaikan tugas. Kemungkinan besar penyalahgunaan data karena kelalaian atau kesengajaan meningkat sebagai akibat dari kegagalan ini. Menurut studi yang dilakukan oleh Rahmad dan Wibowo pada tahun 2019, sebagian besar pelanggaran keamanan sistem basis data disebabkan oleh kesalahan manusia daripada kerentanan teknis.

Selain itu, serangan berbasis jaringan, sniffing, dan denial-of-service (DoS) adalah masalah tambahan yang dihadapi oleh basis data yang terhubung ke jaringan internet atau digunakan dalam sistem terdistribusi seperti cloud computing. Data yang dikirim melalui jaringan dapat disadap oleh pihak ketiga jika tidak ada sistem enkripsi dan pengendalian akses yang kuat.

Organisasi harus menerapkan pendekatan keamanan berlapis (layered security), yang mencakup kontrol akses, enkripsi, audit trail, dan sistem deteksi intrusi (IDS). Penting juga untuk meningkatkan kesadaran pengguna tentang keamanan melalui pelatihan dan kebijakan yang jelas.

Oleh sebab itu, penerapan berbagai macam sistem keamanan merupakan langkah yang krusial supaya data tetap aman oleh pihak tertentu saja.

Salah satunya cara yang biasanya digunakan untuk melindungi keamanan data ialah kontrol akses berbasis peran. Dengan metode ini, setiap akses hanya berisikan data yang sesuai dengan tanggung jawab maupun kedudukannya didalam pekerjaan. Metode seperti ini juga bisa mengurangi terjadinya penyalahgunaan data. selain itu, cara seperti ini juga bisa dengan mudah di diperbaharui pada saat terjadinya perubahan di dalam struktur kerja tanpa perlu menyajikan ulang keseluruhan pengaturan akses.

Salah satunya cara yang biasanya digunakan untuk melindungi keamanan data ialah kontrol akses berbasis peran. Dengan metode ini, setiap akses hanya berisikan data yang sesuai dengan tanggung jawab maupun kedudukannya didalam pekerjaan. Metode seperti ini juga bisa mengurangi terjadinya penyalahgunaan data. selain itu, cara seperti ini juga bisa dengan mudah di diperbaharui pada saat

terjadinya perubahan di dalam struktur kerja tanpa perlu menyajikan ulang keseluruhan pengaturan akses. Dalam pengelolaan keamanan sistem basis data relasional, metode ini salah salah satu cara yang paling banyak dilakukan karena keahliannya mengatur hak akses bagi pengguna berdasarkan peran dalam organisasi. RBAC tidak hanya menetapkan hak akses secara langsung bagi pengguna individu, tetapi secara menetapkannya kepada peran, kemudian pengguna diberikan hak tersebut. Model ini memungkinkan organisasi untuk mengelola akses secara teratur dan efisien, konsisten, dan terskala.

RABC terdiri dari tiga komponen utama: pengguna (users), peran (roles), dan izin. Pengguna diberi peran, dan setiap peran memiliki seperangkat izin untuk objek atau sumber daya dalam basis data. Sebagai contoh, orang yang memegang peran "Admin" dapat memiliki akses penuh ke data, termasuk membaca, menulis, dan menghapusnya, sementara orang yang memegang peran "Staf" hanya dapat membaca dan menulis.

Menurut Sandhu et al. (1996), RBAC mempermudah manajemen keamanan sistem berskala besar. Jika ada perubahan dalam struktur organisasi atau perpindahan karyawan, manajemen hanya perlu mengubah tugas-tugas yang diberikan, tanpa perlu menyesuaikan akses setiap orang. Dengan prinsip least privilege, di mana setiap pengguna hanya menerima akses minimum yang diperlukan, ini juga membantu mengurangi kemungkinan pengguna yang memiliki lebih banyak keistimewaan.

Selain memberikan kemudahan administrasi, RBAC juga memiliki kekuatan untuk pencatatan dan audit. Sistem keamanan dapat lebih mudah menemukan pelanggaran akses atau penyalahgunaan karena setiap aktivitas pengguna dapat dilacak berdasarkan peran. Hartono (2013) memberikan penjelasan tentang bagaimana RBAC berhasil digunakan di organisasi dengan struktur kerja yang jelas, seperti lembaga keuangan, rumah sakit, dan lembaga pendidikan.

Sebaliknya, RBAC juga memiliki batasan. RBAC menjadi kurang fleksibel dalam situasi yang membutuhkan kebijakan akses yang selalu berubah, seperti akses berbasis lokasi, waktu, atau konteks perangkat. Di sinilah model seperti Kontrol Masuk Berbasis Attribute (ABAC) dan Kontrol Masuk Berbasis Kebijakan (PBAC) mulai dipandang sebagai alternatif atau pelengkap.

Namun demikian, RBAC masih relevan dan efektif dalam banyak sistem, terutama ketika digunakan bersama dengan mekanisme keamanan lainnya seperti enkripsi, sistem logging, dan autentikasi multifaktor. Fitur RBAC termasuk dalam banyak sistem database modern seperti PostgreSQL, Oracle, dan SQL Server, yang merupakan bagian dari sistem manajemen keamanan bawaan yang dapat dikustomisasi sesuai kebutuhan perusahaan.

Selain dari kontrol akses berbasis peran, organisasi juga perlu dan harus menerapkan kebijakan keamanan berbasis kebijakan (policy-based security) yang digunakan untuk mengatur hak akses yang tidak hanya berdasarkan peran, tetatpi juga bisa mempertimbangkan lokasi, waktu, dan juga perangkat yang sedang digunakan.

kebijakan (policy-based security) yang mengatur hak akses berdasarkan peran, waktu, tempat, dan perangkat. Sebagai contoh, anggaplah seorang pekerja hanya memiliki akses ke data tertentu dan menggunakan jaringan internal perusahaan selama jam kerja. Dengan demikian, risiko akses legal dapat diminimalkan.

Di zaman teknologi yang terus maju, pengaturan akses ke data menjadi semakin penting. Banyaknya pengguna, berbagai tempat kerja, dan cara akses sistem yang beragam menjadikan kebutuhan akan kontrol akses yang fleksibel semakin tidak terhindarkan. Untuk mengatasi tantangan ini, pendekatan keamanan yang berbasis kebijakan mulai banyak diterapkan dalam sistem database. Pendekatan ini berbeda dari model tradisional seperti Role-Based Access Control (RBAC) yang hanya menetapkan hak akses berdasarkan peran, karena model berbasis kebijakan memperhitungkan faktor tambahan seperti waktu, perangkat, lokasi, dan atribut lain yang dimiliki pengguna.

Salah satu model kontrol akses yang menggunakan kebijakan dan umum digunakan adalah Attribute-Based Access Control (ABAC). Pada model ini, hak akses ditentukan oleh berbagai atribut yang dimiliki pengguna, objek yang akan diakses, dan kondisi saat akses dilakukan. Misalnya, seorang pegawai hanya akan diizinkan untuk mengakses laporan keuangan jika ia adalah seorang manajer, berada di kantor pusat, dan mengaksesnya pada jam kerja. Fleksibilitas ABAC menjadikannya sangat sesuai untuk sistem yang kompleks dan dinamis seperti layanan cloud dan Internet of Things (IoT). Menurut Hu et al. (2014), ABAC menawarkan pengaturan akses yang lebih rinci dibandingkan dengan RBAC. Walaupun begitu, model ini juga memiliki tantangan tersendiri, terutama dalam hal implementasi dan pengelolaan kebijakan yang rumit. Diperlukan sistem pendukung seperti mesin kebijakan atau XACML untuk mengotomatiskan proses evaluasi akses.

Secara umum, ABAC menawarkan sejumlah keunggulan, seperti kemampuan memberikan akses yang sangat khusus, fleksibilitas tinggi terhadap perubahan kondisi pengguna, dan relevansi yang tinggi untuk sistem yang berkembang pesat. Namun di sisi lain, model ini dianggap cukup rumit untuk diterapkan,

sulit diaudit akibat kebijakannya yang sering berubah, dan memerlukan infrastruktur tambahan agar kebijakan dapat berjalan dengan baik.

PBAC sangat cocok digunakan dalam arsitektur sistem yang rumit dan dinamis seperti microservices atau layanan berbasis cloud, di mana aturan bisnis sering kali berubah. Keunggulan PBAC terletak pada kemampuannya mendukung kebijakan akses yang kompleks dan adaptif sesuai dengan kebutuhan bisnis, serta memisahkan aturan akses dari logika aplikasi sehingga lebih mudah dikelola. Namun, tantangannya juga tidak sedikit, seperti perlunya infrastruktur pendukung berupa server kebijakan dan titik keputusan, serta adanya kurva belajar yang tinggi bagi tim pengembang dan administrator sistem.

Dengan mengintegrasikan kebijakan dalam sistem basis data, organisasi dapat menerapkan kontrol akses yang lebih kontekstual dan sesuai dengan kebutuhan operasional mereka. Pendekatan ini tidak hanya meningkatkan aspek keamanan, tetapi juga memberikan fleksibilitas dalam pengelolaan data sensitif di lingkungan digital yang terus berubah.

Adapun juga penerapan enkripsi data yang menjadi bagian penting dalam menjaga keamanan data. Data yang di enkripsi akan menjadi sulit dibaca dan juga dimanipulasi oleh pihak yang tidak memiliki akses kepada kunci enkripsinya. Dan jika terjadi pelanggaran, data tetap terjaga dan aman. Enkripsi harus dilakukan pada saat data sedang disimpan dan juga pada waktu dikirimkannya melalui jaringan, terutama untuk data yag sensitif dan penting contohnya informasi pribadi, transaksi-transaksi keuangan, maupun riwayat atau catatan medis. Penerapan enkripsi yang konsisten dapat menguatkan kepercayaan pada pengguna terhadap sistem yang diterapkan serta menja keamanan informasi tanpa kebocoran data. Tetapi, enkripsi saja tidak cukup jika tidak dikelola secara baik. Sistem manajemen kunci (key management system) harus dipersiapkan supaya proses enkripsi-deskripsi dapat berjalan dengan efisien dan aman. Jika terjadi kebocoran kepada kunci, itu sama saja dengan membuka pintu untuk peretas. Oleh karena itu, perusahaan perlu mengatur agar kunci dapat disimpan dengan aman dan hanya bisa diakses oleh oihak yang memiliki otoritas yang tinggi.

Pengaturan akses ke data menjadi semakin penting di zaman teknologi yang terus berkembang. Kontrol akses yang fleksibel semakin tidak terhindarkan karena banyaknya pengguna, tempat kerja, dan berbagai cara untuk mengakses sistem. Pendekatan keamanan berbasis kebijakan telah banyak digunakan dalam sistem database untuk mengatasi masalah ini. Ini berbeda dari model keamanan konvensional, seperti Pengendalian Akses Berbasis Peran (RBAC), yang hanya menetapkan hak akses berdasarkan peran dan memperhitungkan atribut tambahan seperti waktu, perangkat, lokasi, dan informasi lainnya yang dimiliki pengguna.

Attribute-Based Access Control (ABAC) adalah salah satu model kontrol akses yang paling umum dan ketat. Dalam model ini, berbagai atribut pengguna, objek yang akan diakses, dan kondisi yang harus dipenuhi untuk memungkinkan akses diberikan kepada pengguna. Misalnya, seorang pegawai hanya dapat mengakses laporan keuangan selama jam kerja jika mereka adalah manajer di kantor pusat. Menurut Hu et al. (2014), ABAC lebih rinci dalam pengaturan akses dibandingkan dengan RBAC karena lebih fleksibel, sehingga cocok untuk sistem yang kompleks dan dinamis seperti layanan cloud dan Internet of Things (IoT). Walau bagaimanapun, ada beberapa masalah yang dihadapi model ini, terutama berkaitan dengan implementasi dan pengelolaan kebijakan yang kompleks. Untuk mengotomatiskan proses evaluasi akses, sistem pendukung seperti mesin kebijakan atau XACML diperlukan.

Secara keseluruhan, ABAC menawarkan sejumlah keunggulan, termasuk akses yang sangat unik, fleksibilitas yang tinggi terhadap perubahan kondisi pengguna, dan relevansi yang tinggi untuk sistem yang berkembang pesat. Di sisi lain, model ini dianggap cukup rumit untuk diterapkan, sulit untuk diaudit, dan membutuhkan infrastruktur tambahan untuk menjalankan kebijakan.

PBAC sangat cocok untuk digunakan dalam arsitektur sistem yang kompleks dan selalu berubah seperti microservices atau layanan berbasis cloud. PBAC memiliki kelebihan karena dapat mendukung kebijakan akses yang rumit dan dapat disesuaikan dengan kebutuhan bisnis serta memisahkan aturan akses dari logika aplikasi, yang membuatnya lebih mudah untuk diawasi. Namun, ada banyak tantangan yang harus diatasi. Beberapa di antaranya adalah kebutuhan akan infrastruktur pendukung yang terdiri dari server kebijakan dan titik keputusan, serta tingkat pembelajaran yang tinggi bagi tim pengembang dan administrator sistem.

Dengan mengintegrasikan kebijakan ke dalam sistem basis data, organisasi dapat menerapkan kontrol akses yang lebih kontekstual dan sesuai dengan kebutuhan operasional mereka. Metode ini meningkatkan keamanan dan memberikan fleksibilitas dalam mengelola data sensitif di lingkungan digital yang terus berubah.

Sistem log atau audit trail juga menjadi bagian penting dalam pengamanan data. Sistem ini dapat memantau aktivitas pengguna yang akan dicatat otomatis dimulai dari proses login sampai perubahan data. Dengan adanya sistem ini, administrator dapat memantau dan juga mengidentifikasi adanya hal yang

mencurigakan maupun pelanggaran yang mungkin terjadi. Dikarenakan setiap tindakan bisa dilacak, sistem audit juga dapat membantu dalam menjaga akuntabilitas pengguna dan dapat mereview ulang jika diperlukan. Selain itu, audit trail membutuhkan sistem notifikasi yang aktif. Artinya, ketika terjadi aktivitas yang mencurigakan, seperti login dari lokasi yang tidak biasa atau percobaan akses berulang, sistem harus segera mengirimkan peringatan kepada administrator. Ini memungkinkan tindakan cepat sebelum pelanggaran menjadi lebih umum. Untuk menghadapi ancaman yang terus berkembang, audit pasif tidak cukup.

Salah satu cara penting untuk memastikan keamanan data dalam sistem basis data relasional adalah jejak audit, yang mencatat semua tindakan pengguna secara menyeluruh dan terorganisir, mulai dari proses masuk dan query yang dieksekusi hingga perubahan data yang dilakukan. Tujuan utama sistem audit ini adalah untuk meningkatkan transparansi, meningkatkan tanggung jawab pengguna, dan menemukan dan menghilangkan aktivitas yang mencurigakan yang dapat mengancam integritas sistem.

Pencatatan audit biasanya merekam informasi berikut dalam basis data: identitas pengguna (user ID) waktu akses (timestamp) aktivitas yang dilakukan (query, update, delete) objek yang diakses (nama tabel, kolom) lokasi/IP address

Aspek lain dari keamanan yaitu menjaga integritas data yang berarti memeriksa dan memastikan data tersimpan tetap konsisten tanpa adanya perubahan tanpa izin. Sistem relasional menjaga integritasnya melalui penggunaan aturan seperti kunci primer dan kunci asing, serta berbagai jenis batasan yang mencegah duplikat atau ketidakkonsistenan. Sistem basis data yang tidak memiliki jaminan integritas dapat menghasilkan informasi yang salah, terutama ketika digunakan untuk mendukung pengambilan keputusan strategis perusahaan. Jika tanpa jaminan integritas pada saat digunakan untuk memutuskan keputusan yang strategis, sistem basis data bisa saja salah maupun menyesatkan.

Penggunaan model keamanan diperlukan secara menyeluruh dan saling melengkapi antara satu mekanisme dengan mekanisme yang lainnya. Kombinasi-kombinasi ini dapat membuat sistem keamanan yang berlapis serta mampu menanggulangi berbagai macam ancaman. Sistem-sistem seperti ini dapat membantu menjaga atau melindungi dari sisi teknis dan juga mendukung pengelolaan data atau informasi secara strategis. Di tengah perkembangan teknologi dan juga ancaman yang terus berubah, sistem keamanan juga harus terus berkembang maupun beradaptasi supaya memberikan perlindungan yang baik terhadap data yang dikelola.

Selain itu, pelatihan keamanan secara berkala untuk staf serta penerapan sistem keamanan berbasis AI juga diperlukan guna menganalisis dan mendeteksi pola akses yang mencurigakan maupun yang tidak wajar secara real-time. Hal ini dilakukan agar mencegah terjadinya potensi kebocoran sebelum benar-benar terjadi

Selain mekanisme dasar seperti kontrol akses berbasis peran, enkripsi, dan audit trail, pengembangan teknologi keamanan basis data juga mencakup penerapan metode autentikasi multi-faktor serta penggunaan sistem deteksi intrusi yang dapat mengidentifikasi pola aktivitas tidak wajar secara real-time. Hal ini sangat penting mengingat ancaman keamanan yang semakin beragam dan canggih saat ini, termasuk serangan yang datang dari dalam organisasi maupun dari pihak lain. Pendekatan keamanan yang berlapis, juga dikenal sebagai pertahanan mendalam, menggabungkan berbagai strategi dan kebijakan untuk membuat lingkungan data lebih tahan terhadap kerusakan dan perubahan.

Terakhir, membangun budaya yang mendukung keamanan informasi didalam organisasi sangat penting. Pengamanan teknologi yang canggih akan sia-sia jika sumber daya manusianya tidak diperhatikan. Strategi perlindungan data secara menyeluruh harus meliputi pelatihan rutin, simulasi serangan, dan juga kebijakan disiplin terhadap pelanggaran keamanan. Penggerak teknologi adalah manusia, bukan teknologi itu sendiri.

Dalam era digital saat ini, risiko terhadap sistem basis data muncul tidak hanya dari satu sumber, tetapi dari berbagai jalur serangan yang bisa bersifat internal maupun eksternal, serta teknis atau non-teknis. Oleh karena itu, pendekatan keamanan yang berlapis, sering kali dikenal sebagai pertahanan dalam kedalaman, menjadi sangat penting untuk melindungi data secara menyeluruh. Konsep ini mencakup penerapan beragam mekanisme keamanan yang saling melengkapi di berbagai tingkatan sistem, sehingga ketika satu lapisan mengalami kegagalan, lapisan lain masih dapat memberikan perlindungan.

Dalam melindungi sistem basis data, teknologi bukan satu-satunya elemen yang mempengaruhi keberhasilan perlindungan data. Sumber daya manusia (SDM) memiliki peranan penting sebab mereka yang mengelola, mengakses, dan bertanggung jawab langsung atas penggunaan sistem itu. Bahkan teknologi yang paling maju sekalipun bisa gagal jika pengguna tidak paham cara mengoperasikan sistem dengan aman atau tidak menyadari tanggung jawab mereka dalam menjaga kerahasiaan informasi. Oleh karena itu, faktor manusia menjadi komponen penting dalam strategi keamanan informasi yang komprehensif.

Salah satu masalah utama dalam keamanan sistem informasi ialah manusia yang sering kali menjadi titik lemah. Penelitian yang dilakukan oleh Rahmad dan Wibowo (2019) mengungkapkan bahwa lebih dari 80% pelanggaran dalam keamanan informasi disebabkan oleh kesalahan pengguna, baik yang sengaja maupun yang tidak. Beberapa kesalahan umum yang banyak terjadi termasuk penggunaan kata sandi yang lemah atau dibagikan, mengakses sistem melalui jaringan publik, lupa logout dari perangkat bersama, serta terjaring dalam serangan phishing melalui tautan mencurigakan. Hadnagy (2018) menjelaskan bahwa manusia sering menjadi celah paling besar dalam sistem karena mereka bisa dimanipulasi menggunakan teknik rekayasa sosial. Teknik ini tidak menyerang teknologi dengan langsung, melainkan menggunakan kelemahan psikologis pengguna untuk memperoleh akses secara ilegal.

Untuk meminimalkan risiko terkait faktor manusia, organisasi perlu secara aktif memberikan pendidikan dan meningkatkan kesadaran pengguna mengenai keamanan data. Pelatihan tentang keamanan informasi yang dilakukan secara rutin terbukti efektif dalam membangun pemahaman dan kewaspadaan terhadap ancaman digital. Pelatihan ini perlu meliputi simulasi serangan phishing, pengenalan standar keamanan seperti ISO 27001, pedoman penggunaan perangkat lunak yang aman, serta proses pelaporan insiden keamanan. Di samping itu, organisasi dapat melengkapi pelatihan formal dengan kampanye kesadaran seperti pemasangan poster edukatif, pengingat berkala melalui sistem, atau kuis interaktif tentang keamanan. Tujuannya agar kesadaran terhadap keamanan tidak hanya sebatas teori, tetapi benar-benar menjadi bagian integral dari budaya organisasi.

Namun, hanya meningkatkan kesadaran saja tidak cukup. Organisasi juga harus merancang dan menerapkan kebijakan keamanan yang jelas, tertulis, dan terukur. Beberapa kebijakan penting yang perlu diterapkan meliputi kewajiban penggunaan kata sandi minimal 12 karakter yang terdiri dari huruf, angka, dan simbol; penerapan autentikasi dua faktor untuk semua akun; serta penerapan prinsip "*least privilege*" yang memastikan setiap pengguna hanya memiliki akses sesuai kebutuhan. Kebijakan ini harus disertai dengan sanksi yang tegas untuk pelanggaran, misalnya bagi pengguna yang membagikan akun atau mengakses sistem tanpa izin. Disterer (2013) menekankan bahwa sistem keamanan akan lebih efektif jika didukung oleh kebijakan internal yang konsisten dan penegakan aturan yang kuat.

Selain dari sudut pandang individu, juga penting untuk ditekankan bahwa keamanan bukan hanya tanggung jawab tim teknologi informasi (IT), tetapi merupakan kewajiban seluruh bagian di dalam organisasi. Misalnya, divisi keuangan harus mengerti bahwa data transaksi bersifat sensitif dan perlu dilindungi. Divisi sumber daya manusia (HR) harus menjaga kerahasiaan informasi karyawan agar tidak disalahgunakan. Bahkan pihak manajemen juga memiliki andil dalam menyediakan anggaran untuk audit sistem, pelatihan keamanan, serta pengembangan teknologi pendukung. Kerjasama antara berbagai divisi ini memperkuat ketahanan organisasi secara keseluruhan, karena setiap pihak memahami risiko yang ada serta peran masing-masing dalam melindungi aset informasi perusahaan.

SIMPULAN

Keamanan data dalam sistem basis data relasional adalah hal yang sangat penting untuk memastikan keandalan, kerahasiaan, dan integritas informasi yang dikelola oleh organisasi. Dengan cepatnya perkembangan teknologi informasi, risiko terhadap data kini tidak hanya bersifat teknis tetapi juga mencakup aspek sosial, organisasi, serta psikologis. Kompleksitas ancaman ini memerlukan pendekatan keamanan yang menyeluruh dan dapat beradaptasi, yang tidak hanya berfokus pada perangkat lunak atau perangkat keras, tetapi juga mencakup kebijakan, kontrol, dan kesadaran pengguna sistem tersebut.

Penerapan mekanisme keamanan seperti kontrol akses berdasarkan peran (RBAC), atribut (ABAC), dan kebijakan (PBAC) memberi kesempatan kepada organisasi untuk mengelola hak akses secara dinamis sesuai dengan kebutuhan dan tingkat sensitivitas data. Di sisi lain, penggunaan sistem enkripsi berdasarkan peran (RBE), kriptografi RBAC (cRBAC), dan enkripsi berbasis atribut (ABE) semakin memperkuat perlindungan data, baik saat disimpan maupun saat dikirim. Teknologi ini tidak hanya melindungi dari pencurian data tetapi juga memastikan bahwa data yang mungkin dicuri tidak dapat digunakan tanpa izin yang sah.

Selain kontrol akses dan enkripsi, menjaga integritas data juga merupakan aspek krusial dalam keamanan basis data. Dengan menerapkan prinsip-prinsip seperti integritas entitas, referensial, dan domain serta penggunaan transaksi dengan prinsip ACID, sistem basis data tetap terjaga konsistensinya meskipun terjadi gangguan atau konflik dalam transaksi. Jejak audit dan sistem pencatatan yang efektif memungkinkan pemantauan aktivitas pengguna secara menyeluruh, sehingga pelanggaran atau upaya manipulasi data bisa terdeteksi dan ditindaklanjuti dengan segera. Strategi keamanan berlapis juga penting untuk memastikan bila satu lapisan keamanan gagal, masih ada lapisan lain yang berfungsi sebagai pengaman tambahan.

Namun, sekuat apapun teknologi yang diterapkan, sistem keamanan tidak akan berfungsi maksimal tanpa dukungan sumber daya manusia yang menyadari dan disiplin terhadap kebijakan keamanan. Banyak pelanggaran keamanan yang disebabkan oleh unsur manusia, baik karena kelalaian maupun kurangnya pelatihan. Oleh karena itu, organisasi perlu aktif mengadakan pelatihan keamanan, merumuskan kebijakan internal yang jelas dan konsisten, serta mendorong kerja sama antar divisi untuk membangun budaya keamanan yang menyeluruh.

Dengan mengimplementasikan strategi keamanan yang menyeluruh yang meliputi kontrol akses, enkripsi, integritas data, jejak audit, keamanan berlapis, dan penguatan peran sumber daya manusia organisasi dapat menciptakan sistem basis data yang tidak hanya tahan secara teknis, tetapi juga kuat secara operasional dan etis. Pendekatan ini menjamin bahwa data yang dikelola tidak hanya terlindungi dari ancaman eksternal, tetapi juga aman dari kemungkinan kesalahan dan penyalahgunaan di lingkungan internal. Di era digital yang penuh tantangan dan kompleksitas ini, keamanan data telah menjadi suatu keharusan untuk mempertahankan keberlanjutan dan reputasi sebuah institusi.

REFERENSI

Database Security: Concepts, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2-19.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(2), 92–100.

Elmasri, R., & Navathe, S. B. (2015). Fundamentals of Database Systems (7th ed.). Pearson.

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking (2nd ed.). Wiley.

Hartono, R. (2013). Keamanan data dalam sistem basis data relasional. Jurnal Teknologi dan Sistem Informasi, 9(2), 56–65.

Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Guide to Attribute Based Access Control (ABAC): Definition and considerations (NIST Special Publication 800-162). National Institute of Standards and Technology.

Kamra, A., Bertino, E., & Terzi, E. (2008). Detecting anomalous access patterns in relational databases. The VLDB Journal, 17(5), 1063–1077.

Mukti, M. A., & Hidayanto, A. N. (2017). Implementasi teknologi enkripsi untuk keamanan data pada sistem basis data relasional. Jurnal Sistem Informasi, 13(3), 201–210.

Rahmad, R., & Wibowo, A. (2019). Implementasi mekanisme keamanan basis data menggunakan metode enkripsi dan autentikasi pengguna. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 6(2), 243–250.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. IEEE Computer, 29(2), 38–47.

Siregar, F. D., & Maulidina, N. (2020). Analisis dan implementasi kontrol akses berbasis peran pada sistem basis data relasional. *Jurnal Sistem Informasi*, *16*(1), 45–52

Yu, S., Ren, K., Lou, W., & Li, J. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. IEEE INFOCOM 2010, 1–9.