Jurnal Manajemen Bisnis Era Digital
Volume 2, Nomor 2, Mei 2025
e-ISSN: 3046-7748; p-ISSN: 3046-7764, Hal. 99-112
DOI : https://doi.org/10.61132/jumabedi.v2i2.518
Available online at: https://ejournal.arimbi.or.id/index.php/JUMABEDI

Strategi Keamanan Data dalam Database Relasional: Tinjauan Literatur

Dwi Amanda Tanjung[1*], Muhammad Irwan Padli Nasution[2]
[1-2]Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara, Indonesia
E-mail: dwiamandatanjung8@gmail.com[1], irwannst@uinsu.ac.id[2]

**Korespondensi penulis: dwiamandatanjung8@gmail.com*

Abstract. *Relational databases, an essential component in modern information systems, are vulnerable to various security threats, both internal such as abuse of access rights, and external such as SQL injection, malware, and hacking. Given these conditions, how can relevant mitigation strategies be implemented to protect data security in relational databases? This article aims to identify the main threats to relational database security and map out relevant mitigation strategies. The method used is a literature review of various recent scientific journals that discuss aspects of data security in the context of relational databases. The results of the review indicate that threats such as SQL injection can be overcome by strict input validation, abuse of access rights can be prevented through role-based access control (RBAC), malware attacks can be detected using an intrusion detection system (IDS), and hacking actions can be minimized through the implementation of data encryption. This study is expected to be a reference in designing effective security strategies to protect data in relational databases.*

Keywords*: Data Encryption, IDS, RBAC, Relational Database Security, SQL Injection.*

Abstrak. Database relasional, komponen esensial dalam sistem informasi modern, rentan terhadap berbagai ancaman keamanan, baik internal seperti penyalahgunaan hak akses, maupun eksternal seperti SQL injection, malware, dan peretasan. Mengingat kondisi ini, bagaimana strategi mitigasi yang relevan dapat diterapkan untuk melindungi keamanan data dalam database relasional? Artikel ini bertujuan untuk mengidentifikasi ancaman utama terhadap keamanan database relasional dan memetakan strategi mitigasi yang relevan. Metode yang digunakan adalah tinjauan literatur dari berbagai jurnal ilmiah terkini yang membahas aspek keamanan data dalam konteks database relasional. Hasil tinjauan menunjukkan bahwa ancaman seperti SQL injection dapat diatasi dengan validasi input yang ketat, penyalahgunaan hak akses dapat dicegah melalui kontrol akses berbasis peran (RBAC), serangan malware dapat dideteksi menggunakan *intrusion detection system* (IDS), dan tindakan peretasan dapat diminimalisasi dampaknya melalui penerapan enkripsi data. Studi ini diharapkan dapat menjadi referensi dalam merancang strategi keamanan yang efektif untuk melindungi data dalam database relasional.

Kata Kunci: Enkripsi Data, IDS, Keamanan Database Relasioal, RBAC, *SQL Injection.*

1. LATAR BELAKANG

Dalam era digital saat ini, informasi menjadi aset paling berharga bagi berbagai organisasi. Data yang tersimpan dalam sistem informasi harus dikelola dengan baik dan dijaga keamanannya agar tidak mengalami kebocoran, kerusakan, maupun penyalahgunaan. Menurut Ujung & Nasution (2023), Penggunaan database kini menjadi kebutuhan fundamental di berbagai sektor seperti bisnis, pendidikan, dan pemerintahan. Dalam praktiknya, database menyimpan beragam informasi sensitif, termasuk data keuangan, data pribadi, dan data akademik. Oleh karena itu, perlindungan terhadap database menjadi krusial untuk menjaga kerahasiaan, integritas, dan ketersediaan data yang disimpan. Meningkatnya kompleksitas teknologi dan volume data yang besar menjadikan keamanan database sebagai tantangan yang

Received April 23, 2025; Revised Mei 10, 2025; Accepted Mei 24, 2025; Published Mei 27, 2025

semakin besar. Selain itu, kemunculan berbagai serangan siber yang semakin canggih turut memperbesar risiko terhadap kerentanan sistem. Oleh karena itu, peningkatan keamanan database menjadi prioritas utama yang sangat relevan untuk diteliti dalam upaya melindungi keberlanjutan dan keandalan sistem informasi. Salah satu sistem yang paling banyak digunakan untuk menyimpan dan mengelola data adalah database relasional. Sistem ini menyimpan data dalam struktur tabel yang saling terhubung melalui relasi, sehingga memudahkan dalam melakukan pengorganisasian, pencarian, dan pemrosesan informasi. Database relasional dirancang untuk mendukung transaksi yang konsisten dan andal serta menjaga integritas data. Namun, di balik keunggulannya, database relasional juga menyimpan risiko keamanan yang signifikan, terutama jika tidak dilengkapi dengan strategi pengamanan yang memadai.

Ancaman keamanan pada database relasional dapat berasal dari berbagai sumber, baik internal seperti penyalahgunaan hak akses oleh pengguna sah, maupun eksternal seperti serangan SQL injection, malware, atau tindakan peretasan, yaitu usaha masuk ke sistem tanpa izin dengan tujuan mencuri, merusak, atau mengubah data. Beberapa kasus menunjukkan bahwa masalah seperti lemahnya kontrol akses, tidak adanya enkripsi data, dan kurangnya sistem pengawasan bisa menyebabkan kerugian besar. Oleh karena itu, dibutuhkan strategi keamanan data yang komprehensif, tidak hanya dalam aspek teknis seperti penggunaan kriptografi dan firewall, tetapi juga dalam aspek kebijakan dan tata kelola data.

Penelitian ini bertujuan untuk mengkaji berbagai strategi keamanan data dalam konteks database relasional melalui pendekatan studi literatur. Fokus utamanya adalah mengidentifikasi teknik-teknik yang telah terbukti efektif dalam melindungi data, serta mengevaluasi kelebihan dan kekurangannya berdasarkan hasil-hasil penelitian terdahulu. Dengan mengintegrasikan temuan dari berbagai sumber ilmiah, artikel ini diharapkan dapat memberikan gambaran menyeluruh mengenai pendekatan keamanan data yang relevan dan aplikatif.

Pendekatan yang digunakan dalam penelitian ini adalah tinjauan literatur, yang emungkinkan penulis untuk menyusun sintesis konseptual dari berbagai jurnal dan publikasi terkait keamanan database relasional. Pendekatan ini juga memperkuat kontribusi penelitian dalam pengembangan ilmu pengetahuan dan praktik keamanan data di bidang teknologi informasi, khususnya yang berkaitan dengan sistem manajemen basis data relasional.

2. KAJIAN TEORITIS

Keamanan Database

Menurut Ujung & Nasution (2023), Keamanan database merupakan aspek krusial dalam menjaga perlindungan dan ketersediaan data yang tersimpan di dalam basis data. Upaya ini mencakup berbagai tindakan untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki otorisasi, serta mencegah akses dari pihak yang tidak berwenang.

Keamanan database relasional tidak hanya terbatas pada perlindungan akses, tetapi juga mencakup pengelolaan hak akses pengguna, perlindungan terhadap serangan dari luar, serta penerapan kebijakan teknis dan prosedural yang menyeluruh. Dalam konteks sistem basis data relasional, ancaman terhadap keamanan data dapat berasal dari dalam, seperti penyalahgunaan hak akses, maupun dari luar seperti serangan SQL injection, malware, dan peretasan. Oleh karena itu, dibutuhkan strategi keamanan yang komprehensif, mencakup pendekatan teknis seperti validasi input, kontrol akses berbasis peran (RBAC), penggunaan Intrusion Detection System (IDS), hingga penerapan enkripsi.

Database Relasional

Menurut Hasibuan & Nasution (2023), database relasional merupakan salah satu sistem manajemen basis data yang menyimpan dan mengelola informasi dalam bentuk tabel-tabel, di mana setiap tabel terdiri atas baris dan kolom sebagai representasi dari data.Sistem ini memiliki struktur data yang sistematis dan efisien dalam mendukung transaksi serta menjaga integritas data. Namun, di balik keunggulannya, database relasional juga menyimpan risiko keamanan yang signifikan, terutama jika tidak dilengkapi dengan strategi pengamanan yang memadai.

Ancaman Keamanan dalam Database Relasional

Ancaman keamanan pada database relasional dapat dari berbagai sumber, baik dari dalam maupun dari luar sistem. Ancaman internal mencakup penyalahgunaan hak akses oleh pengguna sah, sedangkan ancaman eksternal meliputi SQL injection, malware, atau tindakan peretasan.

1) Ancaman Internal
    a. Penyalahgunaan hak akses oleh pengguna internal

        Penyalahgunaan hak akses oleh pengguna internal merupakan salah satu ancaman paling berbahaya dalam sistem keamanan data, karena dilakukan oleh individu yang sebenarnya memiliki otorisasi sah terhadap sistem. Ancaman ini

sering kali tidak terdeteksi secara langsung karena aktivitas pengguna internal dianggap wajar oleh sistem.

Menurut Gemawaty & Yuliani (2024), risiko penyalahgunaan hak akses meningkat ketika manajemen identitas dan kontrol akses tidak dijalankan secara optimal. Oleh karena itu, penting untuk menerapkan sistem pengelolaan hak akses yang ketat agar hanya pengguna dengan wewenang yang sesuai yang dapat mengakses data sensitif.

2) Ancaman Eksternal

a. SQL Injection

Menurut Mutedi & Tjahjono (2022), serangan SQL Injection merupakan salah satu bentuk serangan yang menargetkan aplikasi web yang terhubung ke database, di mana penyerang menyisipkan kode berbahaya yang kemudian dijalankan oleh sistem. Kerentanan ini biasanya muncul akibat kurangnya validasi input pada aplikasi. Jika sistem tidak dirancang dengan baik, penyerang dapat memanfaatkan celah tersebut untuk memperoleh akses tidak sah ke dalam database.

Menurut Jemal et al. (2020) menyebut bahwa serangan *Structured Query Language Injection* (SQLI) merupakan salah satu bentuk injeksi yang paling berbahaya karena dapat mengancam aspek-aspek utama dalam sistem keamanan, yaitu kerahasiaan, autentikasi, otorisasi, dan integritas data.

b. Malware

Malware merupakan ancaman signifikan terhadap keamanan data di berbagai bidang. Istilah ini berasal dari kombinasi kata malicious dan software, yang merujuk pada perangkat lunak yang memiliki tujuan merusak. Malware umumnya dibuat untuk menyusup ke dalam sistem komputer, melakukan kerusakan, atau mengeksploitasi celah keamanan tanpa persetujuan pengguna. Dalam ranah keamanan digital, keberadaan malware menjadi salah satu ancaman utama yang dapat berdampak pada individu, institusi, hingga negara.

Dalam konteks jaringan pendidikan, Manoppo et al. (2021) mengungkapkan bahwa malware dapat menyusup melalui lalu lintas jaringan yang tidak aman, lalu melakukan aktivitas berbahaya seperti pencurian data, manipulasi informasi, hingga membangun koneksi dengan server eksternal untuk mengontrol sistem dari jarak jauh. Dalam penelitiannya, ditemukan beberapa jenis malware yang umum menyerang sistem, seperti *Trojan*, *keylogger*, dan *ransomware*. Dari ketiganya,

ransomware dinilai sebagai yang paling berbahaya karena tidak hanya mengenkripsi file penting dan melumpuhkan operasional sistem, tetapi juga sering disertai dengan ancaman kebocoran data apabila permintaan tebusan tidak dipenuhi. Hal ini menempatkan institusi pendidikan dalam posisi rawan, terutama jika tidak memiliki sistem pemulihan data atau backup yang memadai. Penelitian tersebut menggunakan pendekatan *dynamic analysis* untuk mengamati langsung perilaku malware di lingkungan jaringan kampus, dan hasilnya menunjukkan pentingnya sistem monitoring aktif serta kebijakan keamanan yang ketat untuk mencegah penyebaran lebih luas.

Di sisi lain, Fitria (2023) menjelaskan bahwa dalam dunia perbankan, serangan malware cenderung bersifat lebih terarah dan sistematis, dengan menggunakan teknik seperti *keylogging* dan *remote access trojan* (RAT) untuk menyusup dan mencuri informasi kredensial dari database finansial. Serangan semacam ini berdampak sangat besar karena menyasar data sensitif milik nasabah. Oleh karena itu,dibutuhkan sistem keamanan berlapis yang tidak hanya bergantung pada perangkat lunak proteksi, tetapi juga pada kesadaran dan kesiapan sumber daya manusia dalam menghadapi potensi serangan.

c. Tindakan peretasan (*hacking*)

Dalam penelitian Aditya et al. (2023) menjelaskan bahwa tindakan peretasan (*hacking*) merupakan salah satu bentuk ancaman siber yang sangat berbahaya, terutama karena didukung oleh penggunaan hacking tools canggih seperti predator. Tools ini dirancang untuk mengeksploitasi celah keamanan pada sistem target dan memungkinkan pelaku mendapatkan akses tanpa izin. Setelah berhasil masuk, peretas dapat melakukan berbagai tindakan merusak, mulai dari memata-matai aktivitas pengguna, mencuri informasi sensitif, hingga mengendalikan perangkat dari jarak jauh.

Serangan seperti ini sering kali sulit dideteksi karena memanfaatkan teknik penyamaran dan infiltrasi tingkat lanjut. Kondisi ini menempatkan sistem digital dalam posisi rentan, terutama jika tidak dilindungi oleh mekanisme pertahanan siber yang kuat dan proaktif. Oleh karena itu, penting bagi setiap institusi untuk membangun kesadaran akan potensi serangan serta menerapkan sistem keamanan berlapis yang mencakup aspek teknis dan kebijakan operasional.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan studi literatur sebagai metode utama untuk mengkaji strategi keamanan data dalam sistem database relasional. Pendekatan ini memungkinkan peneliti untuk menyusun sintesis konseptual berdasarkan berbagai sumber ilmiah yang telah dipublikasikan sebelumnya, tanpa melakukan eksperimen atau pengumpulan data primer. Proses kajian dimulai dengan merumuskan fokus permasalahan terkait ancaman keamanan database, kemudian dilanjutkan dengan penelusuran dan seleksi artikel-artikel yang relevan. Analisis dilakukan secara kualitatif dengan menyoroti strategi keamanan yang digunakan untuk menangani ancaman seperti penyalahgunaan hak akses, SQL injection, malware, dan peretasan, serta mengevaluasi efektivitas, kelebihan, dan keterbatasan dari strategi-strategi tersebut.

Material dalam penelitian ini diperoleh dari berbagai sumber ilmiah daring yang dapat diakses secara terbuka. Artikel-artikel dikumpulkan melalui mesin pencari akademik seperti Google Scholar, database nasional seperti Garuda Ristek-BRIN, serta portal jurnal ilmiah seperti Neliti dan situs resmi jurnal perguruan tinggi.

4. HASIL DAN PEMBAHASAN

Dalam era digital yang semakin kompleks, keamanan datamenjadi aspek krusial dalam pengelolaan sistem informasi, terutama untuk sistem basis data relasional yang menyimpan informasi sensitif. Bagian ini akan mengidentifikasi strategi mitigasi ancaman pada database relasional serta mengevaluasi strategi mitigasi yang relevan, dengan menyoroti kelebihan, kelemahan, dan tantangan implementasinya.

Strategi Mitigasi Ancaman Terhadap Keamanan Database Relasional

Berdasarkan hasil tinjauan literatur dari berbagai sumber terdapat beberapa strategi mitigasi yang telah dikembangkan untuk menghadapi ancaman terhadap keamanan database relasional, yaitu *Role-Based Access Control*/RBAC, validasi input, *Intrusion Detection System* (IDS) dan enkripsi data.

1) *Role-Based Access Control*/RBAC

Yang menetapkan hak akses pengguna berdasarkan tanggung jawab dan fungsi kerja mereka dalam organisasi. Dengan cara ini, hanya pengguna yang memiliki otorisasi sesuai peran yang dapat mengakses data tertentu, sehingga mengurangi potensi penyalahgunaan akses oleh pihak internal. RBAC juga menggabungkan prinsip dari *Mandatory Access Control* (MAC) dan *Discretionary Access Control* (DAC), yang

menjadikannya sistem pengelolaan hak akses yang lebih terstruktur, efisien, serta mudah disesuaikan dengan kebutuhan organisasi yang dinamis.

2) Validasi Input

Validasi input merupakan salah satu strategi krusial dalam menjaga keamanan database relasional. Menurut penelitian Sultana et al. (2023), validasi input merupakan elemen kunci dalam mencegah ancaman keamanan seperti SQL Injection pada sistem database relasional. Pendekatan yang mereka usulkan mencakup proses verifikasi tipe data, panjang input, serta identifikasi karakter atau pola berbahaya sebelum data dikirim ke server database. Selain itu, mereka menekankan pentingnya menggabungkan validasi input dengan teknik sanitasi dan penggunaan prepared statements untuk memastikan bahwa data yang masuk tidak dapat diubah menjadi instruksi berbahaya. Strategi ini membentuk pertahanan berlapis yang efektif dalam menjaga integritas dan kerahasiaan data dalam sistem informasi berbasis relasional.

3) *Intrusion Detection System* (IDS)

Dalam penelitian yang dilakukan oleh Saroha et al. (2024), *Intrusion Detection System* (IDS) dijelaskan sebagai sistem yang berperan penting dalam mendeteksi dan mencegah serangan siber terhadap jaringan, termasuk sistem keamanan yang melibatkan database. IDS berfungsi sebagai benteng digital yang mampu memantau, menganalisis, dan melindungi data dari serangan hacker yang semakin canggih, terutama dengan meningkatnya akses ke jaringan melalui perangkat dan layanan berbasis cloud. Penelitian ini menekankan bahwa IDS dapat digunakan untuk memantau aktivitas jaringan yang mengakses database, mendeteksi anomali atau pola serangan, dan merespons secara otomatis terhadap potensi ancaman. Dalam implementasinya, IDS tidak hanya bertugas mendeteksi serangan yang sedang berlangsung, tetapi juga dapat digunakan secara proaktif untuk menganalisis potensi kerentanan melalui pengumpulan data dan analisis pola akses. Peneliti juga menjelaskan penggunaan *honeypot* sebagai salah satu metode pendukung dalam IDS, di mana sistem jebakan digunakan untuk menarik perhatian hacker dan mempelajari pola serangan mereka tanpa membahayakan sistem utama. Dengan pendekatan ini, IDS memberikan perlindungan berlapis dalam sistem keamanan jaringan yang terhubung ke database, sekaligus memungkinkan pengelola sistem untuk melakukan evaluasi dan perbaikan berdasarkan data serangan yang terpantau.

Sedangkan, menurut penelitian Agustin et al. (2018), *Intrusion Detection System* (IDS) dijelaskan sebagai sistem yang berfungsi untuk mendeteksi penyusup dalam

jaringan komputer dengan cara melakukan analisis terhadap lalu lintas jaringan untuk mencari pola-pola serangan. Pada penelitian ini, IDS diimplementasikan menggunakan *Snort* sebagai alat berbasis rule (*rule-based*) yang berjalan di sistem operasi *Linux*. *Snort* digunakan untuk mendeteksi serangan yang masuk ke dalam jaringan dengan menganalisis data secara real-time. Pengujian dilakukan terhadap tiga jenis serangan umum yaitu TCP Flood, UDP Flood, dan ICMP Flood, yang kemudian dianalisis menggunakan IDS untuk melihat keakuratan alert dan *response time*. Hasilnya menunjukkan bahwa IDS mampu mendeteksi serangan dengan tingkat akurasi alert yang tinggi (99,98%) dan response time yang efisien, baik saat digunakan oleh satu klien maupun dua klien secara bersamaan. Hal ini membuktikan bahwa IDS berbasis *Snort* efektif untuk mendeteksi aktivitas berbahaya di jaringan dengan performa deteksi yang stabil.

4) Enkripsi Data

Teknik ini bekerja dengan mengubah data asli (*plaintext*) menjadi format terenkripsi (*ciphertext*) yang tidak dapat dibaca oleh pihak yang tidak memiliki kunci dekripsi. Tujuannya adalah untuk melindungi informasi sensitif, baik saat disimpan maupun saat ditransmisikan, dari akses yang tidak sah atau penyalahgunaan. Penerapan algoritma enkripsi simetris seperti AES (*Advanced Encryption Standard*) dan algoritma enkripsi asimetris seperti RSA (*Rivest-Shamir-Adleman*) telah terbukti mampu meningkatkan lapisan keamanan database secara signifikan.

Menurut Suyanto (2012) dalam penelitiannya mengembangkan perangkat lunak enkripsi untuk database *SQL Server*, *Access*, dan *Oracle*, yang dapat mengubah data menjadi format XML terenkripsi agar tidak mudah dibaca atau dimodifikasi selama proses pemindahan antar sistem. Sementara itu, penelitian Hermawan & Ujianto (2021) menekankan bahwa kombinasi AES dan RSA dalam satu sistem enkripsi mampu memberikan perlindungan ganda terhadap data. AES digunakan untuk mengenkripsi isi data, sedangkan RSA mengenkripsi kunci rahasia itu sendiri, sehingga proses dekripsi memerlukan dua langkah dan menambah tingkat kesulitan bagi pihak yang ingin membobol sistem.

Evaluasi Strategi Mitigasi Ancaman

Bagian ini menyajikan evaluasi terhadap strategi mitigasi yang telah diidentifikasi sebelumnya, dengan menyoroti kelebihan, kelemahan, serta tantangan implementasi di berbagai konteks penggunaan.

1) Evaluasi Strategi *Role-Based Access Control* (RBAC)

Role-Based Access Control (RBAC) merupakan pendekatan kontrol akses yang menetapkan hak akses pengguna berdasarkan peran (*role*) yang dimilikinya dalam sebuah sistem. Pendekatan ini terbukti efektif dalam meningkatkan keamanan data, khususnya ketika digunakan untuk mengelola akses terhadap data sensitif seperti data kependudukan. Dalam penelitian yang dilakukan oleh Rubiyanto et al. (2017), RBAC diterapkan untuk mengatur akses sistem informasi di tingkat kabupaten terhadap layanan *web service* data kependudukan. Sistem informasi yang berbeda diberikan kewenangan akses yang berbeda pula, sesuai dengan kebutuhan data dan fungsi pelayanan publik masing-masing. Penelitian ini menunjukkan bahwa pemetaan kebutuhan data berdasarkan peran sistem informasi sangat penting agar hanya data yang relevan dan diperlukan saja yang diekspos, sehingga mengurangi risiko kebocoran data dan meningkatkan efisiensi penggunaan sumber daya.

Implementasi RBAC dalam konteks ini tidak hanya membatasi akses berdasarkan peran, tetapi juga mengatur klasifikasi data menjadi dua kelompok: data umum dan data sensitif. Data sensitif seperti informasi biometrik dan kondisi disabilitas memerlukan perizinan khusus dan tidak bisa diakses sembarangan. Pembagian hak akses dilakukan melalui Perjanjian Kerja Sama (PKS) yang disesuaikan dengan ketentuan dalam permendagri No. 61 Tahun 2015. Penelitian ini juga menyoroti tantangan yang mungkin muncul, seperti perubahan struktur organisasi atau keinginan sistem untuk mengakses data lebih dari yang dibutuhkan. Oleh karena itu, dibutuhkan evaluasi berkala dan komitmen dari pihak pengelola data agar implementasi RBAC dapat berjalan optimal dan tetap sesuai dengan prinsip keamanan data yang berlaku.

2) Evaluasi Strategi Validasi Input

Menurut penelitian Sultana et al. (2023), validasi input merupakan salah satu strategi dalam menghadapi ancaman keamanan pada database relasional, khususnya serangan SQL Injection. Strategi ini dilakukan melalui proses input sanitization di sisi klien, yaitu dengan menyaring dan memverifikasi data yang dimasukkan oleh pengguna sebelum membentuk *query SQL* dinamis. Validasi ini bertujuan untuk memastikan bahwa hanya data yang aman yang diteruskan ke lapisan database, sehingga serangan seperti tautologies, *piggybacked queries*, dan *alternate encodings* dapat dicegah secara langsung. Strategi ini memiliki sejumlah kelebihan, antara lain ringan dan cepat karena tidak memerlukan proses kompleks seperti tokenisasi atau *prepared statements*, serta

mudah diintegrasikan ke dalam sistem yang sudah ada tanpa membebani performa aplikasi.

Meskipun begitu, strategi validasi input ini juga memiliki beberapa kekurangan dan tantangan. Di antaranya, metode ini belum mampu mencegah semua jenis serangan, seperti *error-based attacks*, *union queries*, dan *inference attacks*. Selain itu, proses validasi yang hanya dilakukan di sisi klien masih menyisakan celah keamanan, terutama jika terdapat intersepsi pada saluran komunikasi antara lapisan logika bisnis dan database. Oleh karena itu, penelitian ini menyarankan perlunya penguatan melalui sanitasi tambahan di sisi server, meskipun bagian tersebut masih menjadi pekerjaan lanjutan yang belum dijelaskan secara rinci dalam penelitian ini. Tantangan lainnya adalah memastikan bahwa seluruh input divalidasi secara konsisten dan menyeluruh, serta memperbarui aturan sanitasi sesuai dengan perkembangan teknik serangan yang semakin kompleks.

3) Evaluasi Strategi *Intrusion Detection System* (IDS)

Menurut Aljanabi et al. (2021), *Intrusion Detection System* (IDS) merupakan salah satu komponen penting dalam strategi keamanan sistem karena mampu memantau lalu lintas jaringan dan mendeteksi aktivitas mencurigakan yang mengindikasikan adanya serangan. Salah satu kelebihan utama IDS adalah kemampuannya dalam mendeteksi ancaman secara *real-time* dan memberikan peringatan dini, sehingga administrator dapat merespons sebelum kerusakan terjadi. Selain itu, IDS juga berguna dalam mendokumentasikan pola serangan dan aktivitas jaringan yang mencurigakan, yang dapat dimanfaatkan untuk analisis forensik dan perbaikan sistem keamanan.

Namun, di balik manfaat tersebut, IDS juga menghadapi sejumlah tantangan serius. Tantangan utamanya meliputi tingginya tingkat false alarm (peringatan palsu yang bukan ancaman nyata), rendahnya tingkat deteksi terhadap serangan baru, serta ketidakseimbangan data pelatihan, yang membuat model deteksi sulit membedakan antara aktivitas normal dan berbahaya. Selain itu, waktu respons yang lambat dan kerumitan dalam memperbarui profil deteksi sesuai perkembangan protokol baru juga menjadi hambatan. Beberapa pendekatan IDS, seperti berbasis tanda tangan (*signature-based*), juga tidak mampu mengenali serangan yang belum dikenal. Solusi berbasis pembelajaran mesin telah diajukan, tetapi tetap menghadapi kesulitan karena ketergantungan pada pelatihan manusia dan potensi kesalahan klasifikasi.

4) Evaluasi Strategi Enkripsi Data

Enkripsi data menjadi strategi utama dalam melindungi integritas dan kerahasiaan informasi dalam database. Enkripsi bertujuan menjaga kerahasiaan dan integritas data dengan cara mengubah data asli (*plaintext*) menjadi bentuk terenkripsi (*ciphertext*) yang tidak dapat dibaca tanpa kunci tertentu. Salah satu algoritma enkripsi yang paling banyak diterapkan adalah *Advanced Encryption Standard* (AES), sebuah algoritma simetris yang ditetapkan sebagai standar oleh *National Institute of Standards and Technology* (NIST) Amerika Serikat. Dalam studi yang dilakukan oleh Asriyanik (2017), dijelaskan secara rinci bagaimana algoritma AES bekerja dalam mengamankan data melalui proses substitusi, permutasi, serta penggunaan putaran (*round*) yang dilengkapi dengan kunci yang berbeda pada setiap tahapannya. AES memiliki keunggulan dalam kecepatan proses dan efisiensi komputasi, sehingga cocok diterapkan pada sistem yang membutuhkan kecepatan tinggi seperti aplikasi *real-time*.

Kelebihan AES terletak pada struktur matematisnya yang kompleks dan panjang kunci minimal 128 bit, yang membuatnya tahan terhadap serangan *brute force*. Dalam implementasinya, AES juga dapat digunakan dalam beberapa varian panjang kunci seperti AES-128, AES-192, dan AES-256, sesuai kebutuhan sistem. Algoritma ini terbukti mampu bertahan dari berbagai jenis serangan klasik seperti *differential cryptanalysis* dan *linear cryptanalysis*. Namun demikian, studi tersebut juga mengungkap sejumlah kelemahan AES yang tidak dapat diabaikan. Salah satu tantangan utama adalah dari sisi manajemen kunci: karena AES menggunakan kunci simetris, maka baik pengirim maupun penerima harus memiliki kunci yang sama, yang berarti distribusi kunci harus dilakukan secara aman. Jika kunci ini bocor, seluruh keamanan sistem bisa terancam. Selain itu, ditemukan pula bahwa jika algoritma matematis yang mendasari AES berhasil dipecahkan, maka seluruh sistem keamanan AES dapat dilumpuhkan secara menyeluruh, karena keamanannya bertumpu pada struktur matematis yang saat ini dianggap aman.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil tinjauan literatur, dapat disimpulkan bahwa sistem database relasional menghadapi berbagai ancaman keamanan, baik yang bersumber dari faktor internal maupun eksternal, seperti SQL injection, penyalahgunaan hak akses, malware, dan peretasan. Masing-masing ancaman memiliki strategi mitigasi yang spesifik dan efektif apabila diterapkan secara tepat. Validasi input sangat penting untuk mencegah SQL injection,

sementara kontrol akses berbasis peran (RBAC) efektif untuk mengatasi penyalahgunaan hak akses. Ancaman malware dapat diminimalisasi dengan sistem deteksi intrusi (IDS), sedangkan peretasan dapat dicegah dampaknya dengan menerapkan enkripsi data, sehingga informasi sensitif tetap terlindungi meskipun sistem berhasil ditembus.

Dengan memahami ancaman dan strategi mitigasinya, pengelolaan keamanan pada database relasional dapat dilakukan secara lebih optimal dan preventif. Meskipun strategi-strategi ini menawarkan solusi yang signifikan, perlu diakui adanya keterbatasan seperti potensi *false alarm* pada IDS, celah keamanan pada validasi input di sisi klien, serta tantangan manajemen kunci pada enkripsi simetris seperti AES. Oleh karena itu, disarankan untuk mengimplementasikan kombinasi strategi keamanan berlapis dan melakukan evaluasi berkala untuk menyesuaikan dengan perkembangan teknik serangan siber. Penelitian di masa mendatang dapat berfokus pada pengembangan solusi yang lebih adaptif dan otomatis dalam menghadapi ancaman yang semakin canggih, serta eksplorasi integrasi teknologi kecerdasan buatan untuk deteksi dan mitigasi serangan yang lebih efektif.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada para peneliti dan penulis artikel terdahulu yang karyanya telah menjadi landasan utama dalam penyusunan tinjauan literatur ini. Kontribusi mereka sangat membantu dalam mengidentifikasi dan menganalisis strategi keamanan data dalam database relasional. Artikel ini merupakan bagian dari studi literatur yang diharapkan dapat berkontribusi pada pengembangan ilmu pengetahuan di bidang keamanan data, khususnya dalam konteks sistem manajemen basis data relasional.

DAFTAR REFERENSI

Aditya, A. R. M., Putri, A. W. O. K., Musthofa, D. L., & Widodo, P. (2022). Serangan hacking tools sebagai ancaman siber dalam sistem pertahanan negara (studi kasus: Predator). *Global Political Studies Journal, 6*(1), 35–46. https://doi.org/10.34010/gpsjournal.v6i1

Agustin, R., Fitri, I., & Nathasia, N. D. (2018). Implementasi metode Intrusion Detection Systems (IDS) dan Intrusion Prevention System (IPS) berbasis Snort server untuk keamanan jaringan LAN. *Jurnal Informatika, 18*(1), 71–82.

Aljanabi, M., Ismail, M. A., & Ali, A. H. (2021). Intrusion detection systems, issues, challenges, and needs. *International Journal of Computational Intelligence Systems*. https://doi.org/10.2991/ijcis.d.210105.001

Asriyanik. (2017). Studi terhadap Advanced Encryption Standard (AES) dan algoritma Knapsack dalam pengamanan data. *Jurnal SANTIKA: Jurnal Ilmiah Sains dan Teknologi, 7*(1), 553–560.

Fitria, K. M. (2023). Analisis serangan malware dalam perbankan dan perencanaan solusi keamanan. *Jurnal Informatika dan Teknik Elektro Terapan, 11*(3), 721–731. https://doi.org/10.23960/jitet.v11i3.3312

Gemawaty, C. A., & Yuliani, Y. (2024). Manajemen Identitas dan Akses dalam Keamanan Sistem Informasi (Pendekatan literature review). *Jurnal Manajemen Informatika Jayakarta, 4*(4), 396–403. https://doi.org/10.52362/jmijayakarta.v4i4.1527

Hasibuan, S. H., & Nasution, M. I. P. (2023). A comparative study of relational and NoSQL database for big data analytics. *Jurnal Pendidikan, Sains dan Teknologi (JPST), 2*(3), 513–516. http://jurnal.minarits.com/index.php/jpst/

Hermawan, A., & Ujianto, E. I. H. (2021). Implementasi enkripsi data menggunakan kombinasi AES dan RSA. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 5*(2), 326–330. https://doi.org/10.30743/infotekjar.v5i2.3585

Jemal, I., Cheikhrouhou, O., Hamam, H., & Mahfoudhi, A. (2020). SQL injection attack detection and prevention techniques using machine learning. *International Journal of Applied Engineering Research*.

Manoppo, V. A., Lumenta, A. S. M., & Karouw, S. D. S. (2020). Analisa malware menggunakan metode dynamic analysis pada jaringan Universitas Sam Ratulangi. *Jurnal Teknik Elektro dan Komputer, 9*(3), 181–188. https://journal.unsrat.ac.id/index.php/elekdankom

Mutedi, A., & Tjahjono, B. (2022). Systematic literature review: Preventing SQL injection attacks using tools OWASP CSR Web Application Firewall. *Jurnal Informatika Universitas Pamulang, 7*(1), 151–156. https://doi.org/10.32493/informatika.v7i1.17590

Rubiyanto, Selo, & Widyawan, W. (2017). Implementasi role-based access control (RBAC) pada pemanfaatan data kependudukan di tingkat kabupaten. *Seminar Nasional Sains dan Teknologi 2017, Fakultas Teknik Universitas Muhammadiyah Jakarta*, 1–10. http://jurnal.umj.ac.id/index.php/semnastek

Saroha, L., Octavianto, R., & Sakti, E. M. S. (2024). Pencegahan dan konsep IDS (Intrusion Detection System) dalam mendeteksi serangan siber pada sistem keamanan di Universitas Persada Indonesia Y.A.I. *Tekinfo: Jurnal Ilmiah Teknologi Informasi, 25*(1), 168–176. https://doi.org/10.37871/tekinfo.v25i1

Sultana, P., Sharma, N., Nalini, N., Pathak, G., & Pandey, A. (2023). Prevention of SQL injection using a comprehensive input sanitization methodology. In *Recent Developments in Electronics and Communication Systems*. IOS Press. https://doi.org/10.3233/ATDE221269

Suyanto, S. (2012). Keamanan database menggunakan metode enkripsi. *Jurnal Ilmiah MATRIK, 14*(2), 137–150.

Ujung, A. M., & Nasution, M. I. P. (2023, Juli). Pentingnya sistem keamanan database untuk melindungi data pribadi. *JISKA: Jurnal Sistem Informasi dan Informatika, 1*(2), 44–47. http://jurnal.unidha.ac.id/index.php/jteksis