Journal Islamic Global Network for Information Technology and Entrepreneurship
Volume. 3, No. 3, Juli 2025
e-ISSN : 3025-2857; dan p-ISSN : 3025-2849; Hal. 11-22
DOI: https://doi.org/10.59841/ignite.v3i1.2957
Available online at: https://jurnal.stikes-ibnusina.ac.id/index.php/IGNITE

Analisis Keamanan Database dalam Menghadapi Ancaman Kebocoran Data di Perusahaan Teknologi Informasi

Nisa Alifatuzzahra
Universitas Islam Negeri Sumatera Utara Medan, Indonesia

Alamat: Jl. IAIN No. 1 Medan, Sumatera Utara, Indonesia, 20235.
Korespondensi penulis: nisaazzahra081@gmail.com

Abstract. *Information technology companies rely heavily on databases to store critical data that is vulnerable to leaks that can be financially and reputationally detrimental. This study aims to analyze the effectiveness of database security mechanisms, especially encryption and access control, in preventing data leaks. The method used is a case study with a qualitative approach through observation and interviews at information technology companies, as well as technical analysis of database protection implementation. The results of the study show that to maintain data security, companies need to use end-to-end encryption and a biometric login system so that only authorized people can access it. Smart technology such as AI is also important for detecting threats quickly. In addition, using special tools to monitor devices and routinely test security helps reduce risks. No less important, providing security training to employees so that they are more vigilant and do not become a gap for data leaks. In this way, companies can be better prepared to face various threats in today's digital era.*

Keywords: *: Cyber Security Threats; Database Security; Data Breach; Access Control; Data Encryption;*

Abstrak. Perusahaan teknologi informasi sangat bergantung pada database untuk menyimpan data penting yang rentan terhadap ancaman kebocoran yang dapat merugikan secara finansial dan reputasi. Penelitian ini bertujuan untuk menganalisis efektivitas mekanisme keamanan database, khususnya enkripsi dan kontrol akses, dalam mencegah kebocoran data. Metode yang digunakan adalah studi kasus dengan pendekatan kualitatif melalui observasi dan wawancara pada perusahaan teknologi informasi, serta analisis teknis implementasi proteksi database. Hasil penelitian menunjukkan bahwa ntuk menjaga keamanan data, perusahaan perlu menggunakan enkripsi menyeluruh dan sistem login dengan biometrik agar hanya orang yang berwenang yang bisa mengakses. Teknologi pintar seperti AI juga penting untuk mendeteksi ancaman secara cepat. Selain itu, memakai alat khusus untuk memantau perangkat dan rutin menguji keamanan membantu mengurangi risiko. Yang tak kalah penting, memberikan pelatihan keamanan kepada karyawan supaya mereka lebih waspada dan tidak menjadi celah kebocoran data. Dengan cara ini, perusahaan bisa lebih siap menghadapi berbagai ancaman di era digital sekarang.

Kata kunci: Ancaman Keamanan Siber; Keamanan Database; Kebocoran Data; Kontrol Akses; Enkripsi Data;

1. LATAR BELAKANG

Di zaman serba digital seperti sekarang, penggunaan database sudah menjadi bagian tak terpisahkan dari berbagai sektor, mulai dari instansi pemerintahan, bisnis, maupun pendidikan. Adapun database ini menyimpan data-data yang sangat penting dan bersifat sensitif, misalnya catatan akademik, informasi keuangan, ataupun data pribadi. Sebab itu, menjaga keamanan database sangatlah krusial, agar data yang tersimpan tetap terlindungi dari pihak-pihak yang tidak berwenang. Seiring dengan pesatnya perkembangan tekhnologi diikuti semakin bertambahnya volume data yang mesti dikelola, tantangan dalam menjaga keamanan database pun semakin besar. Apalagi dengan kecanggihan serangan siber sekarang ini membuat sistem database semakin rentan terhadap berbagai ancaman. Oleh sebab itu, melakukan riset

Received: Mei 15, 2024; Revised:Juni 08, 2024; Accepted: Juni 23, 2025; Online Available: Juni 25, 2025;

(penelitian) dan pengembangan terkait sistem keamanan database menjadi hal yang sangat relevan dan dibutuhkan saat ini.

Upaya menjaga keamanan database adalah serangkaian tindakan yang digunakan untuk melindungi informasi dan sistem basis data (database) dari serangan yang dapat mengubah, mencuri, atau merusak data. Sistem keamanan ini melindungi perangkat keras, perangkat lunak, dan hak akses pengguna untuk memastikan kerahasiaan, ketersediaan, dan integritas data. Keamanan database menjadi masalah yang lebih rumit dan signifikan sebagai akibat dari kemajuan teknologi dan pertumbuhan volume data.

Riset dan hasil temuan terdahulu beberapa tidak menggambarkan secara keseluruhan bagaimana cara mengatasi ancaman kebocoran data secara efektif di perusahaan yang kian berkembang, contohnya saja pada perusahaan tekhnologi informasi. Riset sebelumnya hanya berfokus pada suatu kasus dan aspek-aspek teknis yang spesifik. Sebab itu, dalam riset ini akan berupaya mengisi kekosongan dengan mengulas dan menyimpulkan dari berbagai penelitian yang telah dilakukan sebelumnya tentang bagaimana mekanisme sistem keamanan yang efektif guna mengantisipasi dan mengatasi risiko kebocoran data.

Alasan pokok dari analisis keamanan database ini ialah guna secara spesifik mengidentifikasi, mengevaluasi, dan mengembangkan strategi perlindungan yang efektif terhadap ancaman kebocoran data di perusahaan teknologi informasi. Upaya penyelidikan adalah dengan menyoroti kontrol akses, pengenkripsian data, serta deteksi dini terhadap aktivitas mencurigakan. Selain ketiga upaya tersebut, ada beberapa upaya lain seperti penerapan *Zero Trust Architecture* (ZTA), yang merupakan standar keamanan modern tanpa kepercayaan otomatis, kemudian adanya upaya integrasi *Security Orchestration, Automation, and Response* (SOAR) yang merupakan inovasi yang mulai diadopsi. Selanjutnya, pendekatan proaktif lain yang perlu diperhatikan adalah *Continuous Threat Exposure Management* (CTEM), yang membantu perusahaan secara rutin mengidentifikasi dan mengurangi risiko melalui simulasi serangan dan pengujian kerentanan. Di samping itu, pemanfaatan kecerdasan buatan (AI) dan machine learning tidak hanya berperan dalam mendeteksi ancaman, tetapi juga dalam mengotomatiskan analisis pola perilaku pengguna dan anomali data secara real-time, sehingga memungkinkan tindakan cepat dan tepat untuk mencegah kebocoran data. Hal ini demikian bertujuan agar data yang dianggap sensitif dan penting tersebut dapat tetap terjaga kerahasiaan dan keutuhannya, terhindari dari manipulasi dan kecurangan/penyalahgunaan dalam hal apapun, serta tersedia hanya bagi pihak yang mempunyai wewenang atas data-data tersebut saja. Kemudian, upaya pelatihan atau peningkatan kesadaran dan pemahaman tentang keamanan siber bagi para karyawan perusahaan kini menjadi bagian penting dari sebuah

strategi keamanan secara menyeluruh, terutama sebab banyak insiden kebocoran data yang terjadi akibat kesalahan manusia atau kelalaian dari dalam perusahaan/organisasi. Upaya ini menyoroti pentingnya menciptakan budaya keamanan yang kokoh di lingkungan kerja, yang sejauh ini masih jarang menjadi fokus utama dalam penelitian terkait keamanan database.

Terakhir, penelitian ini tidak hanya menganalisis sistem keamanan database secara dominan, namun juga akan berfokus pada implikasi ancaman kebocoran data oleh tingkat kekuatan sistem keamanan suatu perusahaan, baik dampak terhadap internal maupun eksternal. Demikian penelitian ini juga diharapkan dapat menyumbang kontribusi berupa solusi yang signifikan bagi perusahaan teknologi informasi dalam hal mengatasi kebocoran data dan meningkatkan sistem keamanan databasenya.

2. KAJIAN TEORITIS

Menurut Ujung & Nasution (2023), keamanan database merupakan langkah penting untuk menjaga agar data yang tersimpan dalam sistem tetap aman dan selalu tersedia saat dibutuhkan. Proses ini mencakup berbagai tindakan yang bertujuan memastikan bahwa hanya orang yang memiliki izin yang bisa mengakses data tersebut, sementara pihak lain yang tidak berhak tidak dapat mengaksesnya. Adapun aspek keamanan database meliputi beberapa hal, seperti pembuatan kebijakan keamanan yang menjadi pedoman dalam melindungi data dari penyalahgunaan, pengelolaan akses pengguna agar hanya mereka yang berwenang yang dapat membuka atau mengubah data, serta penggunaan enkripsi untuk menjaga kerahasiaan data. Selain itu, proses backup dan pemulihan data juga sangat penting untuk mengantisipasi kehilangan data, sementara pengawasan dan pemantauan secara terus-menerus membantu mendeteksi aktivitas yang mencurigakan atau tidak biasa. Dengan demikian, keamanan database menjadi fondasi utama dalam menjaga kepercayaan dan integritas informasi di dalam sebuah organisasi.

Hapsah & Nasution (2023), dalam artikelnya membahas bagaimana sistem informasi menjadi sangat penting bagi operasi perusahaan seiring dengan kemajuan teknologi komunikasi dan informasi. Orang-orang menggunakan sistem informasi untuk berinteraksi melalui jaringan, infrastruktur data, sistem kontrol dan pemrosesan informasi (perangkat lunak), dan berbagai perangkat fisik (perangkat keras). Akibatnya, banyak orang yang berpikir bahwa keunggulan sistem informasi sangat penting bagi strategi perusahaan mereka. Sistem informasi dapat mengumpulkan, mengatur, dan menyajikan data yang mendukung manajemen bisnis dalam perencanaan, pengambilan keputusan, dan meningkatkan penjualan barang yang diproduksi.

Dalam studi yang ditulis oleh Lesmana & Nasution (2025), ia mengemukakan bahwa pemanfaatan media sosial beberapa tahun terakhir, tepatnya pada tahun 2024 telah tercatat mengalami perkembangan yang sangat pesat diiringi dengan semakin membludaknya peran intenet di seluruh penjuru dunia dan mengglobal sampai saat ini. Akibatnya, banyak oknum yang tergerak untuk mengambil keuntungan atas hal ini, dimana hal apapun dalam kehidupan sehari hari tak terlepas dari pencatatan, penyimpanan, distribusi data atau penyebaran informasi yang semakin marak, dalam hal ini teknologi informasi berperan sangat penting dalam membantu pekerjaan manusia. Oleh sebab itu, kasus kebocoran data dan ancaman siber menjadi topik yang sudah lumrah. Namun penyebab kebocoran data maupun ancaman siber bukan hanya disebabkan oleh hal diatas, akan tetapi rendahnya literasi digital, adanya praktik data *harvesting* oleh pihak ketiga, kemudian praktik pencurian ilegal data dan jual beli data demi keuntungan komersil ke pihak broker, ancaman dari kelalaian karyawan terkait data sensitif, serta praktik-praktik kecurangan lainnya yang berhubungan dengan platform media digital mungkin menjadi faktor-faktor pemicunya.

Dilansir dari penelitian oleh Fitri & Nasution (2024), mereka menyatakan bahwa meskipun praktik pencurian data kian meningkat, keamanan data masih menjadi perhatian besar di sektor korporat. Dalam praktiknya, banyak perusahaan yang masih kurang memperhatikan keamanan data saat mengembangkan sistem atau memilih penyedia layanan. Biasanya, mereka lebih berkonsentrasi pada fungsi sistem dan biaya yang terkait. Pada kenyataannya, mungkin ada dampak signifikan yang terlihat dan tidak terlihat dari pelanggaran data atau masalah keamanan lainnya. Oleh karena itu, sangat penting bagi bisnis untuk memprioritaskan keamanan data saat menjalankan operasi bisnis tersebut.

Sabila & Nasution (2024) menyatakan bahwa keamanan database mencakup tidak hanya data yang ada dalam database, tetapi juga komponen lain dari sistem database. Untuk memiliki kontrol yang tepat diperlukan untuk keamanan yang baik.

Guna memahami potensi ancaman kebocoran data, ancaman siber dan risiko ancaman dalam aspek digital, maka analisis terhadap keamanan sistem informasi tepatnya keamanan database menjadi hal yang mesti diprioritaskan dan diperhatikan secara terus-menerus. Hal ini sesuai dengan pemaparan oleh Warniwati et al. (2024) dalam jurnalnya, bahwa hal diatas penting dipahami, agar perusahaan dapat mengambil tindakan mitigasi risiko, memperkecil kemungkinan risiko ancaman, dan mengambil keputusan serta solusi yang tepat guna mengatasi tantangan keamanan database tersebut. Dalam penelitian ini juga ditekankan untuk melakukan tindakan peningkatan transparansi data bagi pihak yang berwenang.

Adapun menurut Arfan Dwi Madya et al. (2023) berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), Indonesia menghadapi hampir 190 juta upaya serangan siber selama periode Januari hingga Agustus 2020, jumlah ini melampaui yang tercatat pada tahun 2021. Situasi tersebut mengindikasikan bahwa ancaman serangan siber masih akan terus terjadi, terutama karena pandemi COVID-19 bisa memperburuk tingkat kemiskinan dan berpotensi meningkatkan angka kejahatan, termasuk kejahatan digital. Oleh sebab itu, Indonesia sangat memerlukan strategi keamanan siber nasional yang solid. Keamanan siber sendiri berarti memastikan sistem digital tetap terlindungi dari berbagai risiko atau ancaman di dunia maya, yang sangat penting untuk menjaga keselamatan secara menyeluruh.

Sejak kebocoran data kian disebabkan oleh tindak manipulasi dari karyawan internal, pihak yang terkait dengan basis data secara langsung, dan pihak administrasi basis data, maka hubungan basis data (database) dengan tingkat keamanan dalam suatu jaringan komputer kini telah tidak lagi terjamin menurut Putra Rahmadi & Hilda Dwi Yunita (2020). Dikatakan bahwa kini penyimpanan dan pengelolaan data telah memanfaatkan penggunaan basis data (database) oleh perusahaan/bisnis/organisasi/lembaga sampai kini. Adapun perlindungan terhadap basis data (database) diperlukan untuk memastikan keamanan terhadap data-data yang dicatat dan disimpan. Penggunaan metode kriptografi untuk keamanan, pengenkripsian data mesti berfokus agar tetap menjaga pihak pengguna yang berwenang akan data serta mempertahankan integritas data tersebut. Pemanfaatan metode enkripsi dengan cara mengubah data asli yang diekstrak kedalam kode, sehingga tidak dapat dibaca tanpa kunci khusus. Proses ini menggunakan algoritma tertentu untuk mengacak data sehingga hanya orang yang memiliki kunci dekripsi yang bisa mengembalikannya ke bentuk semula. Ada dua jenis enkripsi yang sering dipakai, yaitu enkripsi simetris yang menggunakan satu kunci untuk mengunci dan membuka data, serta enkripsi asimetris yang memakai dua kunci berbeda, yaitu kunci publik dan kunci privat. Dengan menerapkan enkripsi, data di dalam database tetap terlindungi dari akses ilegal, karena meskipun data tersebut bocor, tanpa kunci yang tepat, informasi tersebut tidak bisa dibaca atau digunakan oleh pihak yang tidak berwenang.

Dalam sistem informasi manajemen, keamanan database mempunyai peran penting yang sangat signifikan, terutama menyangkut data/informasi yang sangat penting. Disebutkan dalam penelitian oleh Daulay, Febriana, Kita, Gunawan, & Nurbaiti (2023), bahwa sistem database merupakan fungsi bagi aplikasi digital seperti e-commerce, aplikasi client server, aplikasi e-business dan lainnya yang banyak diaplikasikan sekarang sebagai sarana pendukung kinerja bisnis suatu perusahaan. Kemudian, syarat agar sistem basis data ini dapat beroperasi adalah dengan menjaga keamanannya. Langkah-langkah yang dapat diterapkan dalam hal melindungi

database adalah dengan mengidentifikasi masalah, melakukan pemeriksaan, membatasi akses, memantau tindakan/aktivitas yang mencurigakan terduga ancaman, dan yang terakhir adalah mengevaluasi.

Pada penelitian sebelumnya oleh Handoko & Rony (2018), penelitiannya membahas penerapan metode enkripsi AES-256 untuk meningkatkan keamanan database di lingkungan sekolah. Fokus utama adalah bagaimana teknik enkripsi AES-256 dapat digunakan untuk melindungi data penting agar tidak mudah diakses atau dicuri oleh pihak yang tidak berwenang. Dalam penelitian ini pun dijelaskan langkah-langkah implementasi enkripsi yang efektif dalam menjaga kerahasiaan dan integritas data sekolah. Secara singkat, penelitiannya menekankan pentingnya keamanan data melalui teknologi kriptografi untuk mengatasi risiko kebocoran informasi pada sistem database sekolah.

3. METODE PENELITIAN

3.1 Metode Penelitian

Pada jurnal ini, model riset kualitatif dipakai dengan memanfaatkan teknik studi literatur (SLR). Pendekatan ini melibatkan analisis mendalam terhadap karya-karya riset sebelumnya, yang mencakup artikel, jurnal, buku, dokumen dan situs web terkemuka yang relevan untuk memahami fenomena yang sedang diteliti yakni memahami kinerja keamanan sistem database (basis data) dalam hal menangani ancaman kebocoran data yang bersifat merugikan pihak-pihak yang memiliki kewenangan terhadap data/informasi tersebut. Subjek penelitian ini ialah perusahaan tekhnologi informasi. Adapun sebagai subjek penelitian yaitu pihak atau entitas yang menjadi fokus utama untuk dipelajari. Sedangkan objek penelitian adalah hal-hal spesifik yang diteliti, seperti ancaman kebocoran data dan sistem keamanan database yang digunakan oleh perusahaan yang bergerak di bidang tekhnologi informasi tersebut. Dengan cara ini, peneliti dapat mengumpulkan informasi yang kaya dan beragam, serta mendapatkan wawasan yang lebih luas mengenai topik yang dibahas. Studi literatur ini bertujuan untuk mengidentifikasi pola, tema, dan konsep yang muncul dalam penelitian sebelumnya, sehingga dapat memberikan dasar yang kuat untuk analisis lebih lanjut. Selain itu tekhnik ini sengaja dipakai guna menghasilkan grounded theory atau teori terbaru dari mengumpulkan, mengidentifikasi, menganalisa dan menarik kesimpulan dari teori-teori sebelumnya.

3.2 Teknik Analisis dan Pengumpulan Data

Tekhnik analisis dan pengumpulan data pada penelitian ini dilakukan dengan memanfaatkan sumber data sekunder yang diperoleh melalui studi literatur terdahulu. Proses ini melibatkan penelaahan sistematis terhadap berbagai publikasi, artikel, jurnal, buku dan

dokumen yang relevan dan mirip dengan judul utama pada jurnal ini untuk mengidentifikasi informasi penting dan temuan yang telah ada sebelumnya yang berhubungan dengan tema riset. Dengan cara ini, peneliti dapat mengumpulkan data yang berharga dan melakukan analisis kritis untuk menemukan pola serta hubungan yang ada dalam konteks penelitian.

3.3 Populasi dan Sampel

Merujuk pada penelitian yang dilakukan, adapun populasi yang menjadi fokus adalah mencakup semua perusahaan yang relevan. Dari populasi ini, peneliti memilih sampel sebagian kecil yang mewakili populasiitu sendiri dengan bersumberkan dari penelitian terlebih dahulu pada beberapa subjek penelitian dan populasi terkait.

3.4 Prosedur Penelitian

Pertama, proses penelitian dimulai dengan menentukan fokus utama yakni ancaman kebocoran data pada database di perusahaan teknologi informasi. Setelah itu, peneliti melakukan pengumpulan data melalui studi literatur dengan mencari dan memilih berbagai referensi ilmiah yang relevan, seperti artikel jurnal dan publikasi terpercaya yang membahas tentang keamanan database serta cara-cara mengatasi ancaman tersebut. Data yang diperoleh kemudian dianalisis secara kualitatif dengan mengevaluasi berbagai metode keamanan, seperti enkripsi data, pengaturan akses berdasarkan peran pengguna, validasi input, dan sistem deteksi intrusi, untuk memahami keunggulan, kelemahan, serta efektivitas masing-masing dalam melindungi database dari kebocoran. Pendekatan dalam penelitian ini dimaksudkan untuk menyusun rangkuman komprehensif tentang langkah-langkah yang dapat diambil untuk menjaga keamanan data di perusahaan teknologi informasi.

4. HASIL DAN PEMBAHASAN

4.1 Pentingnya Keamanan Database

Keamanan database menjadi aspek yang sangat krusial dalam menjaga kelangsungan operasional sebuah perusahaan, terutama di era digital saat ini di mana data merupakan aset utama. Data yang tersimpan di dalam database mengandung informasi penting seperti data pelanggan, transaksi keuangan, dan rahasia bisnis yang jika bocor dapat menimbulkan kerugian besar, baik secara finansial maupun reputasi. Perlindungan yang kuat terhadap database sangat diperlukan agar data tersebut tidak mudah diakses atau dimanipulasi oleh pihak yang tidak berwenang.

Selain menjaga kerahasiaan, keamanan database juga berperan dalam memastikan integritas dan ketersediaan data. Integritas data menjamin bahwa informasi yang tersimpan tetap akurat dan tidak berubah tanpa izin, sementara ketersediaan memastikan data dapat diakses oleh

pengguna yang berhak kapan pun diperlukan. Tanpa perlindungan yang memadai, ketiga aspek ini sulit dijaga, sehingga risiko gangguan operasional dan kerugian bisnis menjadi sangat tinggi.

Tidak hanya dari sisi teknis, keamanan database juga memiliki dimensi hukum dan etika. Banyak regulasi yang mengharuskan perusahaan untuk menjaga keamanan data, seperti perlindungan data pribadi dan standar kepatuhan yang harus dipenuhi. Kegagalan dalam memenuhi standar ini dapat berujung pada sanksi hukum dan hilangnya kepercayaan pelanggan. Oleh karena itu, pengamanan database harus menjadi prioritas utama dalam pengelolaan data perusahaan.

4.2 Peranan Database dalam Mendukung Pekerjaan Manusia

Database memiliki peran penting sebagai fondasi dalam penyimpanan dan pengelolaan data yang mendukung berbagai aktivitas manusia, terutama dalam dunia bisnis dan teknologi. Jenis database yang paling banyak digunakan adalah relational database seperti MySQL, Oracle, dan PostgreSQL, yang unggul dalam pengelolaan data terstruktur dan transaksi kompleks. Selain itu, NoSQL database seperti MongoDB dan Cassandra mulai banyak dipakai untuk menangani data tidak terstruktur dan kebutuhan big data yang semakin meningkat.

Perkembangan teknologi juga membawa inovasi baru dalam dunia database. Database berbasis cloud kini semakin diminati karena menawarkan kemudahan akses, skalabilitas, dan fleksibilitas yang tinggi. Selain itu, integrasi teknologi kecerdasan buatan dan machine learning dalam pengelolaan database memungkinkan proses analisis data menjadi lebih cepat dan akurat, sehingga membantu pengambilan keputusan yang lebih tepat. Teknologi blockchain juga mulai digunakan untuk meningkatkan keamanan dan transparansi data.

Berbagai jenis database digunakan sesuai kebutuhan, mulai dari database operasional yang menangani transaksi harian, data warehouse untuk analisis data besar, hingga database real-time untuk aplikasi yang memerlukan respon cepat. Dengan berbagai fungsi tersebut, database menjadi alat penting yang membantu manusia dalam mengelola informasi, meningkatkan efisiensi kerja, dan mendukung inovasi di berbagai bidang.

4.3 Faktor-faktor Pemicu Kebocoran Data

Kebocoran data sering kali disebabkan oleh berbagai faktor yang berasal dari luar maupun dalam perusahaan. Serangan siber eksternal seperti SQL Injection yang memanfaatkan celah keamanan aplikasi web untuk mengakses database secara ilegal, ransomware yang mengenkripsi data dan menuntut tebusan, serta serangan Man-in-the-Middle yang menyadap komunikasi data menjadi ancaman utama. Serangan Distributed Denial of Service (DDoS) juga dapat melumpuhkan sistem dan membuka celah keamanan lain.

Dari sisi internal, kesalahan konfigurasi sistem yang menyebabkan celah keamanan, pengelolaan hak akses yang tidak tepat, serta kelalaian karyawan menjadi faktor signifikan. Penggunaan password yang lemah, kurangnya pelatihan keamanan, dan praktik kerja yang tidak sesuai prosedur juga meningkatkan risiko kebocoran data. Ancaman dari dalam organisasi sering kali sulit dideteksi dan berpotensi menyebabkan kerugian besar.

Selain itu, kurangnya sistem monitoring yang efektif membuat serangan atau aktivitas mencurigakan sulit terdeteksi sejak dini. Hal ini memungkinkan pelaku kejahatan untuk mengeksploitasi celah keamanan dalam waktu yang cukup lama sebelum akhirnya terungkap. Oleh karena itu, faktor teknis dan human error menjadi kombinasi utama yang memicu kebocoran data.

4.4 Solusi Keamanan Database yang Perlu Diterapkan

Solusi keamanan database yang efektif harus melibatkan berbagai lapisan perlindungan. Salah satu langkah utama adalah penerapan enkripsi data yang kuat, seperti Advanced Encryption Standard (AES) dengan kunci 256 bit, yang mampu melindungi data saat disimpan maupun saat dikirimkan melalui jaringan. Enkripsi memastikan bahwa data yang dicuri tidak dapat dibaca tanpa kunci yang tepat.

Selain itu, pengelolaan akses yang ketat dengan sistem Role-Based Access Control (RBAC) sangat penting agar hanya pengguna yang memiliki otorisasi yang dapat mengakses data tertentu. Validasi input yang ketat juga harus diterapkan untuk mencegah serangan seperti SQL Injection dan Cross-Site Scripting (XSS) yang sering menjadi pintu masuk bagi peretas. Penggunaan firewall, sistem deteksi dan pencegahan intrusi (IDS/IPS), serta monitoring aktivitas secara real-time membantu mendeteksi dan menghentikan serangan sejak awal.

Backup data secara rutin dan rencana pemulihan bencana juga menjadi bagian penting dalam menjaga keamanan database. Selain aspek teknis, pelatihan dan edukasi keamanan bagi seluruh karyawan harus dilakukan secara berkala untuk meningkatkan kesadaran dan mengurangi risiko kesalahan manusia. Kombinasi antara teknologi, prosedur, dan sumber daya manusia yang terlatih merupakan kunci utama dalam menjaga keamanan data secara menyeluruh.

Hasil penelitian ini menunjukkan bahwa keamanan database merupakan aspek yang sangat penting dan tidak dapat diabaikan oleh perusahaan teknologi informasi. Data yang tersimpan dalam database merupakan aset berharga yang harus dilindungi dari berbagai ancaman, baik dari luar maupun dalam organisasi. Tanpa perlindungan yang memadai, risiko kebocoran data dapat menyebabkan kerugian finansial, hilangnya kepercayaan pelanggan, serta dampak negatif terhadap reputasi perusahaan. Oleh karena itu, penerapan sistem keamanan yang

komprehensif, termasuk enkripsi data, pengelolaan hak akses yang ketat, serta monitoring aktivitas secara real-time, menjadi langkah krusial untuk menjaga integritas, kerahasiaan, dan ketersediaan data.

Selain itu, penelitian ini menegaskan bahwa faktor pemicu kebocoran data tidak hanya berasal dari serangan siber eksternal, tetapi juga dari kelemahan internal seperti kesalahan konfigurasi sistem dan kurangnya kesadaran keamanan di kalangan karyawan. Solusi yang efektif harus mencakup aspek teknis dan non-teknis, termasuk pelatihan keamanan bagi staf dan penerapan prosedur yang jelas. Dengan pendekatan yang menyeluruh dan berlapis, perusahaan dapat meningkatkan kemampuan dalam menghadapi ancaman kebocoran data dan memastikan bahwa database tetap terlindungi dengan baik dalam lingkungan yang semakin kompleks dan dinamis.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Keamanan database menjadi elemen krusial yang harus diperhatikan oleh perusahaan teknologi informasi karena data yang tersimpan merupakan aset penting yang mendukung kelangsungan operasional dan pengambilan keputusan. Ancaman kebocoran data dapat menimbulkan dampak serius, mulai dari kerugian finansial hingga menurunnya kepercayaan pelanggan. Oleh sebab itu, perlindungan terhadap database tidak hanya sebatas menjaga kerahasiaan, tetapi juga memastikan integritas dan ketersediaan data agar sistem informasi dapat berjalan dengan optimal dan aman.

Faktor yang menyebabkan kebocoran data sangat beragam, meliputi serangan siber dari luar seperti malware, ransomware, dan eksploitasi celah keamanan, serta faktor internal seperti kesalahan konfigurasi, pengelolaan hak akses yang kurang tepat, dan kurangnya kesadaran keamanan di kalangan karyawan. Kombinasi antara ancaman eksternal dan kelemahan internal ini menuntut perusahaan untuk menerapkan strategi keamanan yang menyeluruh dan berlapis. Penanganan yang efektif harus melibatkan teknologi enkripsi yang kuat, kontrol akses yang ketat, serta sistem monitoring yang mampu mendeteksi aktivitas mencurigakan secara real-time.

Solusi keamanan database yang komprehensif juga perlu didukung dengan pelatihan dan edukasi bagi seluruh staf agar kesadaran akan pentingnya keamanan data terus meningkat. Selain itu, penerapan prosedur backup dan pemulihan data secara rutin menjadi bagian penting dalam menjaga kontinuitas bisnis ketika terjadi insiden keamanan. Secara keseluruhan, pendekatan yang terpadu antara aspek teknis dan manajerial menjadi kunci utama dalam

menghadapi ancaman kebocoran data dan memastikan perlindungan database yang efektif di perusahaan teknologi informasi.

5.2 Saran

Adapun saran peneliti terhadap hasil penelitian tentanga analisa keamanan database dalam menghadapi ancaman kebocoran data di perusahaan teknologi informasi, yakni sebagai berikut :

1) Perusahaan sebaiknya mengadopsi teknologi enkripsi yang handal, seperti AES-256, untuk melindungi data yang tersimpan maupun yang sedang dikirim. Penggunaan enkripsi yang konsisten ini sangat penting agar data tetap aman meskipun terjadi upaya akses ilegal atau pencurian informasi.
2) Pengaturan akses pengguna perlu diperketat dengan menggunakan sistem kontrol akses yang berbasis peran. Dengan cara ini, setiap individu hanya diberikan hak akses sesuai dengan tanggung jawabnya, sehingga potensi penyalahgunaan data oleh pihak internal dapat diminimalkan secara efektif.
3) Penting bagi perusahaan untuk mengembangkan sistem pemantauan dan deteksi ancaman secara aktif dan real-time. Sistem ini akan membantu mengenali aktivitas mencurigakan atau serangan siber sejak dini, sehingga tindakan pencegahan dapat segera dilakukan sebelum kerusakan atau kebocoran data terjadi.
4) Selain teknologi, peningkatan kesadaran dan pemahaman karyawan tentang pentingnya keamanan data harus menjadi fokus utama. Melalui pelatihan rutin, karyawan dapat lebih waspada terhadap risiko yang mungkin muncul dan lebih disiplin dalam menjalankan prosedur keamanan yang berlaku.
5) Terakhir, perusahaan perlu menyiapkan mekanisme backup data secara berkala dan rencana pemulihan yang terstruktur. Hal ini akan memastikan data dapat dipulihkan dengan cepat dan operasional perusahaan tetap berjalan lancar jika terjadi insiden kebocoran atau kehilangan data.
6) Peneliti berharap agar dilakukan studi lebih mendalam oleh peneliti selanjutnya tentang tema yang similar dengan penelitian ini.

Untuk penelitian berikutnya, disarankan untuk melakukan studi yang lebih mendalam dengan pendekatan empiris yang melibatkan pengujian langsung pada sistem keamanan database di berbagai jenis perusahaan, sehingga hasilnya dapat lebih aplikatif dan spesifik sesuai konteks industri. Penelitian juga dapat mengembangkan model keamanan yang mengintegrasikan teknologi baru seperti kecerdasan buatan dan blockchain untuk meningkatkan efektivitas deteksi dan pencegahan kebocoran data. Selain itu, kajian tentang

aspek human error dan perilaku pengguna dalam konteks keamanan data perlu diperluas agar solusi yang dihasilkan tidak hanya bersifat teknis tetapi juga mempertimbangkan faktor manusia. Penelitian lebih lanjut juga dianjurkan untuk mengeksplorasi kebijakan dan regulasi yang efektif dalam mendukung implementasi keamanan database secara menyeluruh di perusahaan. Dengan demikian, hasil penelitian selanjutnya dapat memberikan kontribusi yang lebih komprehensif dan aplikatif dalam menghadapi tantangan keamanan data yang terus berkembang

6. DAFTAR REFERENSI

Arfan Dwi Madya, Bagas Djoko Haryanto, & Devi Putri Ningsih. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. *Indonesian Journal of Education And Computer Science*, *1*(3), 127–135. https://doi.org/10.60076 /indotech.v1i3.236

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. https://doi.org/10.56832/edu.v3i2.357

Fitri, M. A., & Nasution, M. I. P. (2024). Taktik Canggih untuk Memastikan Keamanan Data Perusahaan dan Mengatasi Ancaman Kebocoran Data di Masa Depan. *Journal of Sharia Economics Scholar (JoSES)*, *2*(2), 113–121.

Hapsah, Z. F., & Nasution, M. I. P. (2023). Analisis Tingkat Keamanan Data Perusahaan Yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen. *Jurnal Manajemen Dan Akuntansi*, *1*(2), 338–343.

Lesmana, R., & Nasution, M. I. P. (2025). Kebocoran Data di Media Sosial : Analisis Pola dan Strategi Pencegahannya. *Socius: Jurnal Administrasi Publik Volume*, *2*(10), 123–128.

Nasution, R. S. U. S. & M. I. P. (2024). Cara Mengidentifikasi dan Menghindari Kebocoran Data. *Kohesi: Jurnal Multidisiplin Saintek Volume*, *3*(7).

Putra Rahmadi, & Hilda Dwi Yunita. (2020). Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi. *Jurnal Cendikia*, *19*(1), 413–418.

Rony, H. & M. A. (2018). Implementasi Keamanan Database Dengan Enggunakan Metode Advanced Encryption Standard (Aes-256) Pada Sekolah Smk Islam Al Hikmah Jakarta Berbasis …. *Skanika*, *1*(3), 1137–1142. Retrieved from http:// jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2537

Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *JISKA: Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44. Retrieved from http://jurnal.unidha.ac.id/index.php/jteksis

Warniwati, T., Kedua, Z., Zebua, J. A., Informasi, T., Sains, F., & Nias, U. (2024). *Analisis Keamanan Sistem Informasi Pada Perusahaan E-Commerce Di Indonesia*. *01* (November), 68–75.