

Keamanan dalam Sistem Database Sebagai Sumber Informasi Manajemen Terhadap Perlindungan Data

Anisya Putri Ertani Daulay¹, Vinni Febriana²,

Ayu Diah Adek Kita³, Syahrul Gunawan⁴, Nurbaiti⁵

^{1,2,3,4,5} Universitas Islam Negeri Sumatera Utara Medan, Indonesia

Email : ertanidaulay@gmail.com¹, vinnifebriana03@gmail.com²,

ayudiahadekita08@gmail.com³, syahrulgunawan080303@gmail.com⁴, nurbaiti@uinsu.ac.id⁵

Abstrak

Database menjadi peran penting saat ini dalam sistem informasi manajemen, maka perlunya juga manajemen informasi yang memberikan keamanan fisik data perusahaan terjaga dengan andal. Data rangkuman harian disebarluaskan melalui media sekunder yang dapat diakses secara langsung maupun berurutan. Hal tersebut maka perlunya mengenal lebih dalam keamanan dalam sistem *database* agar sebagai pengguna bisa menggunakan sistem *database* dengan baik dan terjaga dari kebocoran privasi data. Tujuan dari penelitian ini adalah untuk memahami bahwa sistem basis data yang digunakan dalam teknologi informasi tidak hanya merampingkan proses tetapi juga memiliki mekanisme untuk melindungi data yang sensitif atas keamanan data. Kesimpulan dari penelitian ini adalah keberhasilan sistem manajemen informasi tertentu merupakan faktor penting yang lebih meningkatkan kualitas. Oleh karena itu, sangat penting untuk menerapkan sistem *database* yang handal dan dapat melindungi kerahasiaan informasi dengan fasilitas keamanan sistem *database*.

Kata kunci: Database, Informasi, Keamanan, Teknologi, Privasi.

SECURITY IN THE DATABASE SYSTEM AS A SOURCE OF MANAGEMENT INFORMATION FOR DATA PROTECTION

Abstract

Databases play an important role today in management information systems, so there is also a need for information management that provides the physical security of company data to be reliably maintained. Daily summary data is disseminated through secondary media which can be accessed directly or sequentially. For this reason, it is necessary to know more about security in the database system so that users can use the database system properly and are protected from data privacy leaks. The purpose of this study is to understand that database systems used in information technology not only streamline processes but also have mechanisms to protect sensitive data for data security. The conclusion from this study is the success of a particular information management system is an important factor that further enhances quality. Therefore, it is very important to implement a database system that is reliable and can protect the confidentiality of information with database system security facilities.

Keywords: Database, Information, Security, Technology, Privacy.

PENDAHULUAN

Di era sekarang ini sistem informasi sudah sangat banyak dikenal dan digunakan orang-orang, sehingga pengguna *database* banyak meminta untuk kerahasiaan datanya terjaga biasa disebut keamanan terhadap data (Andi, 2003). *Database* adalah kumpulan data yang berfungsi sebagai sumber informasi bagi pengguna. Di mana setiap pengguna diberikan izin untuk mengakses data dalam tabel yang sesuai dengan mengubah, menghapus, menganalisis, menambah, dan memperbaiki data yang digunakan (Kasmir, 2014).

Tujuan sistem basis data termasuk menyediakan sarana yang tersedia, memastikan integritas data, melindungi data dari penggunaan yang tidak sah dan penggunaan ilegal, serta menyediakan sarana untuk digunakan oleh beberapa orang, seperti interkoneksi data (Kroenke, 2003). Pada penelitian sebelumnya juga telah dijelaskan bahwa saat ini, dapat dikatakan hampir semua institusi swasta, pemerintah ataupun perusahaan telah menggunakan sistem informasi untuk dapat menghasilkan informasi yang digunakan oleh berbagai level manajemen (Golds, 1990). Berbagai istilah, seperti data, *database*, informasi dan sistem informasi muncul. Aplikasi dalam organisasi, aplikasi *client - server*, aplikasi *e-Commerce*, aplikasi *e-bussines* merupakan fungsi utama dari basis data (Kadir, 2010). Tujuan basis data adalah membantu orang dan organisasi menelusuri hal-hal tertentu.

Maka benar dari tujuan data tersebut keamanan data merupakan bagian terpenting karena dalam berbisnis perusahaan maupun instansi banyak menggunakan sistem informasi yang berbasis dengan *database* (Susilo, 2017). Jadi dalam esai ini, kita akan mendalami berbicara tentang sistem manajemen basis data yang telah terbukti sangat berguna di dunia modern dengan membuatnya lebih mudah bagi kita untuk mengelola data. Dengan itu, peneliti harus lebih paham mengenai keamanan dalam sistem *database* (Kadir, 2010). Sebagai hasil dari situasi di atas, artikel ini menjelaskan kepada pengguna *database* mengenai keamanan dari *database* yang dikenal dengan membuat hidup lebih mudah bagi konsumen dan memungkinkan untuk juga mengelola data dengan keamanan data yang telah diketahui.

METODE

Penelitian saat ini menggunakan metodologi yang ketat, yaitu melakukan penelitiannya menggunakan temuan-temuan berdasarkan karya yang diterbitkan, jurnal ilmiah, dan situs internet (Assingkily, 2021). Proses editorial artikel melibatkan kepustakaan, yang dilakukan dengan membaca buku-buku yang relevan atau sumber data lainnya. Menurut Darmadi (2013: 153), metodologi yang digunakan untuk penelitian adalah cara yang cocok untuk memperoleh data untuk tujuan yang dimaksudkan. Ungkapan "cara ilmiah" berarti bahwa tujuan penelitian ini didasarkan pada pertimbangan rasional, sistematis, dan empiris.

HASIL DAN PEMBAHASAN

Keamanan *database* merupakan bagian terpenting dalam beroperasinya kegiatan *database*. Maka dari itu, sistem informasi manajemen perlu mendalami keamanan data, agar tidak terjadinya kebocoran data dalam pengelolaan sistem *database*. Adapun aspek keamanannya dengan membatasi akses, melakukan pengecekan terlebih dahulu pada *user*, memantau kegiatan yang mencurigakan (Setiawan & Fatimah, 2021). Berikut fasilitas keamanan *database*:

Publikasi

Mekanisme pada saat mempublikasikan yang telah terpublis tidak dapat untuk diubah. Publikasi menjadi bahan konsumsi ilmiah publik. Proses kegiatan ini meliputi pengaturan properti lain, proteksi, hanya baca, dapat dibaca, *eQuestion* lain, dan dapat diimpor (Iswahyudi, *et.al.*, 2018).

Proteksi

Pada saat penggunaan *database*, pengguna diawal akan dimintai *password* atau biasa disebut dengan kata kunci untuk pengamanan data yang telah dibuat, pada saat pembuatan akun *database* (Timur, 2022).

Hanya Baca (Read-Only)

Jika ditemukan kata seperti "*Read Only*" bahwa jelas itu tidak bisa diganggu gugat untuk pengubahan (Akbar & Waluyo, 2018).

Dapat Dibaca (eQuestion Lain)

Jika pada *set* "*Tidak*" maka hal tersebut menandakan bahwa hanya bisa dibaca oleh *BOCSOft eReader* dan tidak bisa dibaca oleh *BOCSOft equestion* lain (Suyanto, 2012).

Dapat Diimpor

Jika pada *set* "*Ya*", maka hal tersebut menandakan bahwa *eQuestion* bisa digabungkan dengan *database eQuestion* dengan versi yang sama (Bahri & Suhardiyanto, 2018).

Selanjutnya, penanganan terhadap insiden dalam keamanan basis data: *pertama*, mengumpulkan informasi sebanyak banyaknya yang berkaitan tentang sifat insiden. *Kedua*, mencegah maupun membatasi masalah kerusakan yang terjadi diakibatkan oleh insiden yang sedang terjadi. *Ketiga*, mengonversikan kerusakan yang diakibatkan oleh insiden tersebut. *Keempat*, mengakumulasikan bukti insiden itu yang terkait. *Kelima*, memulihkan atau menebus layanan secepatnya. *Keenam*, mengangkat tindakan yang proaktif untuk menurunkan suatu insiden di masa depan (Riyadi, 2022).

Hal tersebut dilakukan ada keinginan *goals*-nya, maka dari itu supaya tujuan di atas dapat terlaksana dengan baik, perlunya menentukan tahap-tahap untuk melakukan penanganan terhadap insiden yang terjadi. *Pertama*, tahap persiapan (*Preparation*); *kedua*, tahap identifikasi; *ketiga*, tahap *containment*; *keempat*, tahap pemberantasan; *kelima*, tahap pemulihan; dan *keenam*, tahap tindak lanjut (Sutabri, 2016).

SIMPULAN

Berdasarkan uraian di atas, disimpulkan bahwa sistem *database* sudah dikenal memudahkan publik, namun karena keamanan sering juga terjadinya kebocoran privasi, maka pihak *user* maupun pengguna sangat menjaga keamanan dengan fasilitas *database* yang mungkin sudah terpercaya keamanannya. Fasilitas keamanan *database* mampu memberikan perlindungan terhadap *server*, maka dari itu sebagai pengguna juga mampu bekerjasama dalam mengontrol data dengan valid, sehingga pengguna tidak merasa takut dan ragu dalam sistem yang digunakan dari kebocoran data maupun pencurian data. Sistem *database*

teknologi informasi pengelolaan yang memberikan kontribusi yang baik terhadap keamanan informasi dengan melakukan *monitoring* dan pengecekan setiap 24 jam sehari melalui penanganan yang telah disediakan oleh pihak *database*.

REFERENSI

- Akbar, F., & Waluyo, S. (2018). "Sistem Keamanan Database Menggunakan Algoritma Advanced Encryption Standard (AES-128) Studi Kasus: Red Avenue Indonesia" *SKANIKA: Sistem Komputer dan Teknik Informatika*, 1(2), 821-828. <https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/296>.
- Andi, A. (2003). *Database Visual Basic 6.0 dengan SQL*. Yogyakarta: Penerbit ANDI DAN MADCOMS.
- Assingkiy, M. S. (2021). *Metode Penelitian Pendidikan: Panduan Menulis Artikel Ilmiah dan Tugas Akhir*. Yogyakarta: K-Media.
- Bahri, S., & Suhardiyanto, S. (2018). "Sistem Keamanan Ruang Server Menggunakan Teknologi RFID dan Password" *eLEKTUM*, 15(1), 11-18. <https://jurnal.umj.ac.id/index.php/elektum/article/view/2117>.
- Darmadi, H. (2013). *Metode Penelitian Pendidikan dan Sosial*. Bandung: Alfabeta.
- Iswahyudi, C., Wahyuda, A. D., & Fatkhiyah, E. (2018). "Analisis dan Implementasi Sistem Keamanan Jaringan Komputer dengan Metode Intrusion Detection System (Studi Kasus: Horison Ultima Riss Hotel)" *Prosiding SNAST*, 71-80. <https://ejournal.akprind.ac.id/index.php/snast/article/view/1495>.
- Kadir, A. (2010). *Dasar Aplikasi Database MySql - Delphi*. Yogyakarta: Penerbit Andi Offset.
- Kasmir, K. (2014). *Bank dan Lembaga Keuangan*. Jakarta: RajaGrafindo Persada.
- Kroenke, M. D. (2003). *Database Processing*. Jakarta: PT. Gelora Aksara Pratama.
- Riyadi, H. S. (2022). *Strategi Manajemen Bank Syariah dalam Meningkatkan Loyalitas Nasabah*. Jakarta: CV. Literasi Nusantara Abadi.
- Setiawan, A., & Fatimah, T. (2021). "Implementasi Algoritma Kriptografi RC4 untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web pada PT. Trans Intra Asia" *SKANIKA: Sistem Komputer dan Teknik Informatika*, 4(1), 66-71. <https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2044>.
- Susilo, G. (2017). "Keamanan Basis Data pada Sistem Informasi di Era Global" *Jurnal Transformasi*, 12(2). <http://ejournal.stmikbinapatria.ac.id/index.php/JT/article/view/70>.
- Sutabri, S. T. (2016). *Sistem Informasi Manajemen (Edisi Revisi)*. Yogyakarta: Penerbit Andi Offset.
- Suyanto, S. (2012). "Keamanan Database Menggunakan Metode Enkripsi" *Jurnal Ilmiah Matrik*, 137-150. <https://www.neliti.com/publications/224902/keamanan-database-menggunakan-metode-enkripsi>.
- Timur, D. P. (2022). "Evaluasi Keamanan Sistem Informasi pada Lembaga Pemerintahan Provinsi Sumatera Selatan" *e-Prints Binadarma*. <http://eprints.binadarma.ac.id/14569/>.