KEAMANAN DATABASE DALAM BORLAND DELPHI

APRILIA PUTRI

165100010

Fakultas Komputer, 448757257

Apriliaputria.student@umitra.ac.id

Abstract

Menumbuhkan teknologi pemrosesan data, ini telah mengakibatkan implementasi sistem komputerisasi di semua bidang. Semua bagian organisasi atau perusahaan telah menerapkan berbagai aplikasi untuk memenuhi kebutuhan mereka. Aplikasi yang diterapkan secara terpisah menimbulkan masalah tersendiri yang membutuhkan data yang sama. Sehingga pertukaran data menjadi solusi alternatif. Persyaratan keamanan data pada proses pertukaran database menjadi masalah baru dalam prosesnya. Untuk memastikan keamanan data pada proses pertukaran, metode enkripsi adalah cara terbaik. Dengan implementasi enkripsi pada data yang dipertukarkan, maka data dijamin aman dan hanya bisa dibaca oleh mereka yang membutuhkannya. Aplikasi yang menggunakan database berbeda membutuhkan format standar sehingga semua aplikasi dapat membacanya. Format ini adalah XML. Dengan XML, database (tabel) dapat dibaca oleh aplikasi lain meskipun dengan platform yang berbeda.

Kata kunci: Enkripsi, Dekripsi, Keamanan, Basis Data, Cipher, XML.

A. INTRODUCTION

Materi Ke 1 membahas mengenai i cloud system ...dst
tambahkan gambar untuk memperkuat penjelasan (Gunakan Minimal 600 kata)

Jawaban :

Database Security (Keamanan Database) pada borland delphi

A. Pengertian Database

Database atau basis data adalah kumpulan data yang disimpan secara sistematis di dalam komputer dan dapat diolah atau dimanipulasi menggunakan perangkat lunak (program aplikasi) untuk menghasilkan informasi. Pendefinisian basis data meliputi spesifikasi berupa tipe data, struktur, dan juga batasan-batasan data yang akan disimpan. Basis data merupakan aspek yang sangat penting dalam sistem informasi dimana basis data merupakan gudang penyimpanan data yang akan diolah lebih lanjut. Basis data menjadi penting karena dapat menghindari duplikasi data, hubungan antar data yang tidak jelas, organisasi data, dan juga update yang rumit. Atau kumpulan informasi yang disimpan di dalam komputer secara sistematis sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut. Perangkat lunak yang digunakan untuk mengelola dan memanggil kueri (query) basis data disebut sistem manajemen basis data (database management system, DBMS). Sistem basis data dipelajari dalam ilmu informasi.

Istilah basis data mengacu pada koleksi dari data-data yang saling berhubungan, dan perangkat lunaknya seharusnya mengacu sebagai sistem manajemen basis data (database management system/DBMS). Jika konteksnya sudah jelas, banyak administrator dan programmer menggunakan istilah basis data untuk kedua arti tersebut.

B. Pengertian Keamanan Database

Keamanan database adalah suatu cara untuk melindungi database dari ancaman, baik dalam bentuk kesengajaan atau pun bukan. Ancaman adalah segala situasi atau kejadian baik secara sengaja maupun tidak yang bersifat merugikan dan mempengaruhi system serta secara konsekuensi terhadap perusahaan/organisasi yang memiliki system database. Keamanan database tidak hanya berkenaan dengan data yang ada pada database saja, tetapi juga meliputi bagian lain dari system database, yang tentunya dapat mempengaruhi database tersebut. Hal ini berarti keamanan database mencakup perangkat keras, perangkat lunak, orang dan data.

C. Penyalahgunaan Database

- a) Tidak disengaja, jenisnya :
- Kerusakan selama proses transaksi
 - Anomali yang disebabkan oleh akses database yang konkuren
 - Anomali yang disebabkan oleh pendistribusian data pada beberapa komputer
 - Logika error yang mengancam kemampuan transaksi untuk

mempertahankan konsistensi database.

b) Disengaja, jenisnya :

- Pengambilan data / pembacaan data oleh pihak yang tidak berwenang.
- Pengubahan data oleh pihak yang tidak berwenang.
- Penghapusan data oleh pihak yang tidak berwenang.

D. Teknik Pengamanan Basis Data (Database)

Melihat banyaknya ancaman yang bisa mengganggu bahkan merusak sistem komputer maka perlu diadakan tindakan-tindakan pengamanan data agar bisa menghindari atau paling tidak mengurangi risiko yang mungkin timbul. Beberapa tindakan pengamanan sistem data pada komputer diuraikan berikut ini.

- Administrative Security
Pengamanan data secara administratif (administrative security) perlu dilakukan untuk menjaga kemungkinan gangguan keamanan data yang datangnya dari “orang dalam” atau kerja sama orang dalam dengan orang luar.

- Network Security
- Anti Virus

Anti virus diciptakan untuk mencegah meluasnya infeksi virus dan untuk memperbaiki file-file yang telah terinfeksi. Satu hal yang perlu diperhatikan adalah anti virus dibuat hanya untuk mendeteksi dan mencegah jenis atau kategori virus yang pernah ada, dan tidak bisa mendeteksi jenis atau kategori virus baru. Anti virus harus selalu di-update secara reguler agar bisa mendeteksi virus-virus baru.

- Firewall

Firewall berarti dinding api, biasanya dibuat pada bangunan besar untuk mencegah menjalarnya api dari satu bagian gedung ke bagian lainnya. Firewall pada jaringan komputer adalah perangkat lunak yang dipasang pada komputer server sehingga dapat melindungi jaringan dari serangan yang datangnya dari luar

- Proxy Server

Proxy server pada dasarnya berfungsi seperti firewall jenis application level gateway, suatu server yang berada antara server jaringan dan internet. Proxy server melaksanakan beberapa proses aplikasi yang telah ditetapkan lebih dulu, misalnya melayani akses dari terminal ke suatu situs web, atau berfungsi sebagai “transfer agent” terhadap berbagai aplikasi yang memiliki akses keluar atau akses dari luar ke dalam jaringan.

- Enkripsi-Dekripsi
Data yang dikirim melalui jaringan tidak jarang disadap oleh orang lain untuk kepentingan tertentu, sehingga timbul usaha untuk melakukan pengkodean terhadap data sebelum dikirim melalui jaringan agar tidak bisa dibaca oleh penyadap. Pengubahan data asli menjadi kode rahasia disebut proses data encryption atau enkripsi data. Setelah data rahasia sampai ke tujuan maka data ini dikembalikan ke bentuk aslinya, proses ini disebut data decryption. Ilmu matematik yang mendasari teknik enkripsi dan dekripsi disebut kriptologisedangkan teknik dan sains dari proses enkripsi-dekripsi disebut kriptografi. Naskah asli disebut sebagai plaintext dan naskah rahasia

(yang telah di-enkrip) disebut ciphertext.

Terdapat tiga level enkripsi basis data yang meliputi :

- o Enkripsi pada level penyimpanan (storage)

Enkripsi data dilakukan pada subsistem storage (penyimpanan), baik pada level file maupun pada level blok. Enkripsi level ini cocok untuk mengenkripsi file, folder, media storage dan media tape.

- o Enkripsi pada level basis data

Enkripsi dilakukan pada saat data ditulis dan dibaca dari basis data. Enkripsi jenis ini dilakukan pada level kolom pada tabel basis data. Level ini melindungi data pada Database Management System (DBMS) dari berbagai macam serangan

- o Enkripsi pada level aplikasi

Aplikasi menangani proses enkripsi data. Kelebihannya adalah tidak terjadi penurunan performansi pada basis data, karena DBMS tidak menangani enkripsi data. Akan tetapi, ketika terjadi perubahan strategi enkripsi atau perubahan data yang dienkripsi, akan banyak terjadi modifikasi pada level aplikasi

· Autentikasi

Autentikasi adalah salah satu bentuk identifikasi untuk meyakinkan bahwa orang yang sedang berkomunikasi dengan kita adalah benar adanya, bukan pemalsuan identitas. Salah satu bentuk autentikasi yang paling sering dijumpai adalah: UserID disertai dengan Password, bahwa UserID adalah pernyataan tentang siapa yang sedang akses sistem atau sedang berkomunikasi, dan Password membuktikan bahwa orang tersebut benar adanya. Hanya saja sistem UserID dan Password ini ada

kelemahannya, karena ada saja cara untuk mencari tahu password seseorang sehingga bisa terjadi pemalsuan identitas.

Salah satu sistem untuk mengurangi efek pemalsuan identitas atau pencurian password adalah dengan menerapkan OTP (One Time Password), dimana satu password hanya digunakan untuk satu kali akses, akses berikutnya harus menggunakan password yang berbeda. Sistem lain yang mengamankan autentikasi adalah Passport dan Kerberos.

Salah satu tujuan dari security adalah menjamin agar resource hanya boleh diakses oleh orang yang berhak dan orang yang berhak itu bisa mengakses resource tanpa halangan.

Authorization adalah proses menentukan apa sajakah layanan yang bisa dinikmati pengguna yang telah jelas identitasnya (authenticated user). Jadi sebelum ada authorization, harus melalui proses authentication. Identitas yang telah dibuktikan di proses authentication menjadi dasar untuk menentukan layanan yang berhak dinikmati seorang pengguna.

Logikanya adalah tanpa mengetahui siapa anda, saya tidak tahu apa saja yang boleh dan tidak boleh untuk anda. Jadi tanpa authentication tidak ada authorization. Contohnya setelah saya tahu anda adalah Tukul Arwana, maka saya tahu anda boleh memandu acara empat mata, dan tidak boleh memandu di acara Dorce Show. Biasanya pengguna yang tidak terotentikasi (anonymous guest) tetap

bisa menikmati layanan, namun dengan akses yang sangat terbatas.

Hubungan antara client, server, authentication dan authorization system bisa dilihat pada gambar di atas. Client sebelum bisa menikmati layanan server harus melalui proses authentication. Setelah authentication berhasil akan terjalin hubungan trust antara client dan server sehingga cukup sekali saja authentication sampai client logout/keluar. Selanjutnya setiap ada permintaan layanan, server akan menghubungi system authorization untuk menentukan apakah client tersebut berhak atas layanan yang dimintanya.

B. CONCLUSION

Kesimpulan dari materi ini adalah(minimal 150 kata)

Jawaban :

Database adalah kumpulan data yang disimpan secara sistematis di dalam komputer dan dapat diolah atau dimanipulasi menggunakan perangkat lunak (program aplikasi) untuk menghasilkan informasi. Dari pengertian diatas untuk informasi atau

databasenya dicuri atau diambil dll, maka kita harus melindungi database dari ancaman tersebut, baik dalam bentuk kesengajaan atau pun bukan. Dengan cara seperti pengamanan yang ditulis pada artikel ini.

Authentikasi adalah salah satu bentuk identifikasi untuk meyakinkan bahwa orang yang sedang berkomunikasi dengan kita adalah benar adanya, bukan pemalsuan identitas. Salah satu bentuk autentikasi yang paling sering dijumpai adalah: UserID disertai dengan Password, bahwa UserID adalah pernyataan tentang siapa yang sedang akses sistem atau sedang berkomunikasi, dan Password membuktikan bahwa orang tersebut benar adanya. Hanya saja sistem UserID dan Password ini ada kelemahannya, karena ada saja cara untuk mencari tahu password seseorang sehingga bisa terjadi pemalsuan identitas.

Salah satu tujuan dari security adalah menjamin agar resource hanya boleh diakses oleh orang yang berhak dan orang yang berhak itu bisa mengakses resource tanpa halangan.

C. ACKNOWLEDGEMENT

University Of Indonesia
University Of Mitra Indonesia
Telkom University
University Of Melbourne
Saitama University

D. REFERENCE (Based ISO 690)

- [1] A. S. Putra And O. M. Febriani, "Knowledge Management Online Application In Pdam Lampung Province," In *Prosiding International Conference On Information Technology And Business (Icith)*, 2018, Pp. 181–187.
- [2] A. S. Putra, O. M. Febriani, And B. Bachry, "Implementasi Genetic Fuzzy System Untuk Mengidentifikasi Hasil Curian Kendaraan Bermotor Di Polda Lampung," *J. Sist. Inf. Dan Manaj. Basis Data*, Vol. 1, No. 1, Pp. 21–30, 2018.
- [3] O. M. Febriani And A. S. Putra, "Sistem Informasi Monitoring Inventori Barang Pada Balai Riset Standardisasi Industri Bandar Lampung," *J. Inform.*, Vol. 13, No. 1, Pp. 90–98, 2014.
- [4] Putra, Arie Setya. "2018 Artikel Struktur Data, Audit Dan Jaringan Komputer." (2018).
- [5] Putra, A. S. (2018, July 17). Paperplain Fundamental Create Application With Borland Delphi 7.0 University Of Mitra Indonesia. Retrieved From [Osf.io/Pbrn9](https://osf.io/Pbrn9).

E. REFERENCE (Based APA)

Putra, A. S., Aryanti, D. R., & Hartati, I. (2018, November). Metode SAW (Simple Additive Weighting) sebagai Sistem Pendukung Keputusan Guru Berprestasi (Studi Kasus: SMK Global Surya). In *Prosiding Seminar Nasional Darmajaya* (Vol. 1, No. 1, pp. 85-97).

Sari, D. P., Febriani, O. M., & Putra, A. S. (2018, November). Perancangan Sistem Informasi SDM Berprestasi pada SD Global Surya. In *Prosiding Seminar Nasional Darmajaya* (Vol. 1, No. 1, pp. 289-294).

Putra, A. S. (2018). Paperplain: Execution Fundamental Create Application With Borland Delphi 7.0 University Of Mitra Indonesia.

Putra, A. S., Sukri, H., & Zuhri, K. Sistem Monitoring Realtime Jaringan Irigasi Desa (JIDES) Dengan Konsep Jaringan Sensor Nirkabel. *IJEIS (Indonesian Journal of Electronics and Instrumentation Systems)*, 8(2), 221-232.

Darmawan, A., Yuliawati, D., Marcella, O., & Firmandala, R. (2016). Sistem Absensi dan Pelaporan Berbasis Fingerprint dan SMS Gateway. *EXPLORE*, 7(1).

Febriani, O. M., Wahyuni, T., & Yusuf, S. (2017). DESIGN OF WEBSITE-BASED INFORMATION SYSTEM FOR EDOCUMENT ADMINISTRASI IN THE COMMUNITY SERVICE UNIT (A Case Study at Rajabasa District). *INTERNATIONAL JOURNAL OF*

COMPUTERS & TECHNOLOGY,
16(7), 7010-7020.

Febriani, O. M., & Wahyuni, T. (2017, October). PERANCANGAN SISTEM E-DOCUMENT ADMINISTRASI LOGBOOK PENELITIAN PADA UNIT LAYANAN DI BANDAR LAMPUNG. In *Prosiding Seminar Nasional Darmajaya* (Vol. 1, No. 1, pp. 187-194).

Febriani, O. M., & Permadi, A. B. (2017). Implementasi Sistem Aplikasi Data Bimbingan dan Pelanggaran Siswa pada Sekolah Menengah Atas di Lampung Tengah dengan Metode Analisis dan Desain Sistem Terdistribusi (SSAD). *EXPERT*, 7(1).

Febriani, O. M., & Ambarwati, L. (2015). PERANCANGAN APLIKASI PENGOLAHAN DATA PENJUALAN UKM KELANTING KHAS TELO DESA SIDOHARJO KECAMATAN JATI AGUNG KABUPATEN LAMPUNG SELATAN. *Jurnal Teknologi Informasi dan Bisnis Pengabdian Masyarakat Darmajaya*, 1(1), 77-95.

Febriani, O. M. (2015). Rancang Bangun Aplikasi E-commerce menggunakan Freewebstore pada UKM Kelanting di Desa Sidoharjo Lampung Selatan. *Prosiding Sembistek 2014*, 1(02), 446-458.