Jurnal Penelitian Teknologi Informasi Dan Sains
Vol. 1 No. 2 Juni 2023
e-ISSN :2985-7635, p-ISSN :2985-6280, Hal 50-57
DOI: https://doi.org/10.54066/jptis.v1i2.480

Sistem Keamanan Database

Adelia Marwah Ujung[1]
Universitas Islam Negeri Sumatera Utara
adeliamarwaadel@gmail.com

Muhammad Irwan Padli Nasution[2]
Universitas Islam Negeri Sumatera Utara
irwannst@uinsu.ac.id

Universitas Islam Negeri Sumatera Utara (UINSU), Medan, Indonesia.
Korespondensi penulis, e-mail : adeliamarwaadel@gmail.com

Abstract. *This research is conducted with the aim of database security and protecting users' personal information. The study focuses on the database security system, which is an essential aspect in the field of information technology. The research is carried out by conducting a literature review and case studies on various existing database security systems. The fundamental concepts of the database security system, types of database security systems, and the latest technologies that can be used to enhance database security are explained in this research. Furthermore, the potential risks that can arise when the database security system is not properly maintained and strategies to address database security issues are also discussed. This research is expected to provide a better understanding of the importance of maintaining database security for organizations and companies.*

Keywords : *data, security, system, servers.*

Abstrak. Penelitian ini dilakukan bertujuan untuk keamanan database dan melindungi informasi pribadi pengguna. Penelitian ini membahas mengenai sistem keamanan database, yang merupakan salah satu hal penting dalam dunia teknologi informasi. Penelitian ini dilakukan dengan cara melakukan survei literatur dan studi kasus pada berbagai sistem keamanan database yang telah ada. Konsep dasar dari sistem keamanan database, jenis-jenis sistem keamanan database, serta teknologi terbaru yang dapat digunakan untuk meningkatkan keamanan database dijelaskan dalam penelitian ini. Selain itu, bahaya-bahaya yang dapat terjadi apabila sistem keamanan database tidak dijaga dengan baik dan strategi untuk mengatasi masalah keamanan database juga dibahas. Penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik mengenai pentingnya menjaga keamanan database bagi organisasi dan perusahaan.

Kata kunci : data, keamanan, database, server.

Received April 07; Revised Mei 30, 2023; Accepted Juni 30, 2023
** Adelia Marwah Ujung, adeliamarwaadel@gmail.com*

1. PENDAHULUAN

Dalam era digital saat ini, penggunaan database telah menjadi hal yang sangat penting dan umum dalam berbagai bidang seperti bisnis, pendidikan, pemerintahan, dan lain-lain. Dalam penggunaannya, database menyimpan berbagai informasi sensitif seperti data keuangan, data pribadi, data akademik, dan lain-lain. Oleh karena itu, keamanan database menjadi sangat penting untuk melindungi informasi sensitif yang disimpan di dalamnya. Dalam konteks ini, meningkatkan keamanan database menjadi prioritas utama, karena semakin kompleksnya teknologi dan semakin banyaknya data yang disimpan, keamanan database menjadi tantangan yang semakin besar. Selain itu, serangan cyber yang semakin canggih juga membuat keamanan sistem database semakin rentan. Oleh karena itu, penelitian tentang sistem keamanan database sangatlah relevan dan penting.

Penelitian tentang sistem keamanan database bertujuan untuk mengeksplorasi dan menganalisis berbagai aspek sistem keamanan database, seperti metode enkripsi data, manajemen hak akses, dan metode deteksi serangan. Dengan melakukan penelitian ini, diharapkan dapat ditemukan solusi terbaik dalam meningkatkan keamanan database.Tujuan utama dari penelitian ini adalah untuk meningkatkan keamanan database dan melindungi informasi pribadi pengguna. Diharapkan hasil dari penelitian ini dapat memberikan kontribusi yang signifikan dalam pengembangan sistem keamanan database yang lebih baik dan dapat diandalkan di masa depan.

Penelitian ini dilakukan dengan cara melakukan survei literatur dan studi kasus pada berbagai sistem keamanan database yang telah ada. Dari hasil analisis, diharapkan dapat ditemukan solusi terbaik dalam meningkatkan keamanan database. Selain itu, penelitian ini juga akan memperkenalkan berbagai teknologi baru yang dapat digunakan untuk meningkatkan keamanan database seperti blockchain dan teknologi kecerdasan buatan.

Diharapkan hasil dari penelitian ini dapat memberikan kontribusi yang signifikan dalam pengembangan sistem keamanan database yang lebih baik dan dapat diandalkan di masa depan. Dengan adanya sistem keamanan database yang lebih baik dan kuat, maka informasi sensitif yang disimpan di dalamnya dapat terlindungi dengan baik dan kepercayaan pengguna terhadap sistem database dapat meningkat.Dalam hal ini, penelitian tentang sistem keamanan database menjadi sangat penting untuk dilakukan agar penggunaan database menjadi lebih aman dan dapat diandalkan di masa depan.

2. METODE PENELITIAN

Pengumpulan Metode penelitian studi literatur digunakan dalam penelitian sistem keamanan database untuk mendapatkan pemahaman yang lebih mendalam tentang topik tersebut. Metode ini melibatkan analisis dan evaluasi terhadap literatur-literatur yang berkaitan dengan sistem keamanan database.

Pertama, peneliti melakukan pencarian literatur yang relevan dengan topik penelitian. Ini dapat dilakukan melalui database online seperti Google Scholar, IEEE, ScienceDirect, dan sebagainya. Setelah itu, peneliti membaca dan mengevaluasi literatur yang ditemukan, mencatat informasi penting, dan menyusunnya dalam bentuk rangkuman. Selanjutnya, peneliti melakukan analisis terhadap informasi yang telah dikumpulkan. Hal ini meliputi identifikasi dan analisis tema-tema utama, perbedaan, dan persamaan dalam literatur yang dibaca. Peneliti juga dapat melakukan kritik terhadap literatur yang digunakan, seperti mempertanyakan metodologi atau penggunaan data yang digunakan dalam penelitian.

Dalam penelitian sistem keamanan database, metode penelitian studi literatur dapat membantu peneliti untuk memahami konsep-konsep dasar dan teknologi yang digunakan dalam sistem keamanan database. Metode ini juga membantu peneliti untuk mengidentifikasi kelemahan dan tantangan dalam sistem keamanan database, dan mencari solusi yang tepat.

3. HASIL PENELITIAN

A. Pengertian Keamanan Database

Keamanan Keamanan database adalah suatu proses yang sangat penting dalam memastikan bahwa data yang disimpan dalam sebuah basis data tetap terlindungi dan terjaga ketersediaannya. Proses keamanan ini melibatkan serangkaian tindakan untuk memastikan bahwa data hanya tersedia bagi pihak yang berwenang, dan tidak dapat diakses oleh pihak yang tidak berwenang.

Keamanan database meliputi berbagai aspek, termasuk kebijakan keamanan, manajemen akses, enkripsi data, backup dan recovery, serta pengawasan dan monitoring. Kebijakan keamanan database adalah panduan dan aturan yang ditetapkan untuk memastikan bahwa data tetap terlindungi dan tidak disalahgunakan. Manajemen akses, pada sisi lain, melibatkan pengaturan hak akses untuk pengguna dalam basis data,

sehingga hanya pengguna yang berwenang yang dapat mengakses data yang disimpan.

Enkripsi data adalah proses untuk mengubah data menjadi bentuk yang tidak dapat dibaca tanpa kunci enkripsi yang sesuai. Backup dan recovery, di sisi lain, melibatkan proses untuk membuat salinan cadangan data dan memulihkan data yang hilang atau rusak. Terakhir, pengawasan dan monitoring dilakukan untuk memastikan bahwa semua akses ke basis data dicatat dan dipantau untuk mendeteksi potensi ancaman keamanan.

Secara keseluruhan, keamanan database sangat penting untuk memastikan bahwa data tetap aman dan terlindungi dari akses yang tidak sah atau tidak diinginkan. Dengan memastikan bahwa kebijakan keamanan yang tepat diimplementasikan, manajemen akses yang tepat ditetapkan, dan proses enkripsi, backup, dan recovery yang efektif dilakukan, organisasi dapat memastikan bahwa data mereka tetap aman dan tersedia bagi pihak yang berwenang saja

B. Tujuan Keamanan Databes

Tujuan dari keamanan database adalah untuk melindungi informasi yang disimpan dalam basis data dari akses yang tidak sah atau tidak diinginkan dan memastikan bahwa data tetap rahasia, utuh, dan tersedia hanya bagi pihak yang berwenang. Beberapa tujuan kunci dari keamanan database antara lain:

1. Kerahasiaan: Tujuan pertama dari keamanan database adalah untuk memastikan bahwa informasi yang disimpan di dalamnya tetap rahasia dan tidak dapat diakses oleh pihak yang tidak berwenang. Hal ini dapat dicapai dengan menerapkan sistem otorisasi yang ketat, pengaturan hak akses yang tepat, dan enkripsi data.
2. Keutuhan: Tujuan kedua dari keamanan database adalah untuk memastikan bahwa data di dalam basis data tetap utuh dan tidak rusak atau dimanipulasi oleh pihak yang tidak berwenang. Hal ini dapat dicapai dengan menggunakan teknologi checksum atau tanda tangan digital, dan dengan menerapkan sistem validasi data yang ketat.
3. Ketersediaan: Tujuan ketiga dari keamanan database adalah untuk memastikan bahwa data tetap tersedia bagi pihak yang berwenang dan tidak terganggu oleh serangan atau gangguan sistem. Hal ini dapat dicapai dengan menggunakan sistem backup dan recovery yang efektif, teknologi load balancing, dan monitoring sistem yang berkesinambungan.
4. Kepatuhan: Tujuan keempat dari keamanan database adalah untuk memastikan kepatuhan terhadap peraturan dan aturan yang berlaku terkait dengan privasi data,

seperti GDPR, HIPAA, dan sebagainya. Hal ini dapat dicapai dengan menerapkan kebijakan keamanan yang sesuai dan melakukan audit secara berkala untuk memastikan bahwa sistem keamanan database tetap mematuhi persyaratan yang berlaku.

Secara keseluruhan, tujuan dari keamanan database adalah untuk melindungi informasi sensitif dan penting dari kerusakan, pencurian, atau penggunaan yang tidak sah, sambil memastikan bahwa data tetap tersedia bagi pihak yang berwenang saja. Dengan menerapkan sistem keamanan yang tepat, organisasi dapat memastikan bahwa data mereka tetap aman dan terlindungi dari ancaman keamanan yang muncul.

C. Kategori Keamanan Databes

Kategori keamanan database mencakup berbagai aspek yang harus diperhatikan untuk melindungi data yang disimpan di dalamnya. Berikut adalah beberapa kategori keamanan database yang umum:

1. Keamanan fisik: Melibatkan perlindungan fisik terhadap server dan infrastruktur yang menjalankan database. Ini termasuk pengendalian akses fisik ke fasilitas server, pemantauan lingkungan suhu dan kelembaban, penggunaan sistem pemadaman listrik cadangan, dan perlindungan terhadap bencana alam atau kejadian darurat lainnya.
2. Keamanan akses: Mencakup kontrol dan pengaturan akses ke database. Ini termasuk otentikasi pengguna dengan penggunaan kata sandi yang kuat, kebijakan pengguna yang sesuai, pengendalian hak akses (misalnya, hak akses pengguna terhadap tabel atau kolom tertentu), dan monitoring aktivitas pengguna untuk mendeteksi aktivitas yang mencurigakan atau tidak sah.
3. Keamanan jaringan: Merupakan perlindungan terhadap serangan melalui jaringan. Ini termasuk penggunaan firewall untuk mengendalikan lalu lintas jaringan, enkripsi data yang dikirim melalui jaringan (misalnya, SSL/TLS untuk koneksi yang aman), dan pengaturan segmenasi jaringan untuk membatasi akses ke database dari jaringan yang tidak terpercaya.
4. Keamanan data: Mencakup perlindungan terhadap kebocoran, modifikasi, atau pencurian data. Ini melibatkan penggunaan enkripsi data untuk melindungi data saat istirahat atau saat disimpan di server, serta mekanisme cadangan dan pemulihan untuk melindungi data dari kehilangan atau kerusakan.
5. Keamanan aplikasi: Mencakup keamanan perangkat lunak aplikasi yang mengakses database. Ini termasuk memastikan bahwa perangkat lunak aplikasi diperbarui dengan patch keamanan terbaru, melindungi aplikasi dari serangan seperti SQL injection atau

cross-site scripting, dan membatasi akses aplikasi ke sumber daya database yang tidak perlu.

6. Keamanan audit dan kepatuhan: Melibatkan pemantauan dan audit aktivitas database untuk mendeteksi ancaman keamanan atau pelanggaran kebijakan. Ini juga mencakup kepatuhan terhadap regulasi keamanan data yang berlaku, seperti GDPR (General Data Protection Regulation) di Uni Eropa.

Selain kategori-kategori di atas, ada banyak faktor lain yang harus dipertimbangkan dalam menjaga keamanan database, tergantung pada kebutuhan dan konteks organisasi. Penting untuk mengadopsi pendekatan yang komprehensif dan mengikuti praktik terbaik keamanan database untuk melindungi data yang berharga

D. Ancaman Keamanan Database

Ancaman keamanan database merupakan suatu hal yang sangat serius dan dapat menyebabkan kerugian besar bagi organisasi. Beberapa ancaman keamanan database yang umum terjadi adalah:

1. Serangan Malware: Malware adalah program jahat yang dirancang untuk merusak atau mencuri data dari sistem atau jaringan. Beberapa jenis malware yang umum digunakan untuk melakukan serangan keamanan database adalah virus, worm, trojan, dan ransomware.
2. Serangan SQL Injection: Serangan SQL Injection adalah sebuah teknik serangan yang memanfaatkan celah keamanan pada aplikasi web yang memungkinkan penyerang untuk mengirimkan perintah SQL yang berbahaya ke basis data. Serangan ini dapat menyebabkan kerusakan pada data dan bahkan mengambil alih sistem.
3. Serangan DDoS: Serangan DDoS (Distributed Denial of Service) adalah serangan yang dilakukan dengan cara membanjiri jaringan atau sistem dengan lalu lintas yang sangat besar sehingga sistem menjadi tidak dapat diakses oleh pengguna yang sah.
4. Serangan Man in the Middle: Serangan Man in the Middle adalah serangan yang dilakukan dengan cara menyusup ke dalam komunikasi antara pengguna dan sistem, sehingga penyerang dapat mengakses data yang dikirim atau diterima oleh pengguna.
5. Serangan Password Cracking: Serangan Password Cracking adalah serangan yang

dilakukan dengan cara mencoba untuk menebak atau mengambil kata sandi atau password pengguna. Serangan ini dapat dilakukan dengan menggunakan teknik brute force, dictionary attack, atau social engineering.

6. Serangan Phishing: Serangan Phishing adalah serangan yang dilakukan dengan cara memancing pengguna untuk memberikan informasi sensitif seperti username, password, atau informasi kartu kredit melalui email atau situs web palsu.

Ancaman keamanan database dapat menyebabkan kerusakan yang sangat besar bagi organisasi, seperti kerugian finansial, reputasi yang buruk, atau kehilangan data penting. Untuk mengatasi ancaman keamanan tersebut, organisasi harus menerapkan sistem keamanan yang ketat, melakukan monitoring dan pemantauan secara berkala, dan memberikan pelatihan keamanan kepada pengguna untuk mengurangi risiko serangan.

4. KESIMPULAN

Informasi penting harus dilindungi dari pihak yang tidak berwenang yang dapat mencoba mencuri atau menghapusnya menggunakan keamanan data. Keamanan data, dalam bentuk yang paling sederhana, mencakup semua langkah yang diperlukan yang diambil oleh individu atau organisasi untuk melindungi seluruh ekosistem teknologi informasi. Kekhawatiran tentang pelanggaran keamanan dapat berhasil dikurangi dengan membangun prosedur keamanan data yang memadai. Untuk memberikan penjelasan lebih lanjut, langkah-langkah keamanan data mencegah pengguna yang tidak berwenang mengakses komputer, database, atau situs web dengan tujuan mengumpulkan informasi digital yang sensitif.

Komponen penting lainnya dalam menjaga keamanan data adalah melakukan backup secara rutin. Backup sangat penting untuk menjaga keutuhan situs web dan mencegah terjadinya kerusakan. Oleh karena itu, sangat penting untuk secara berkala melakukan backup menyeluruh terhadap data yang penting. Langkah pencegahan ini memungkinkan pemulihan cepat situs web ke kondisi aslinya dalam situasi yang tak terduga.

DAFTAR PUSTAKA

Suyanto,Mail. 2012. Keamanan Database Menggunakan Metode Enkripsi. Jurnal ilmiah MATRIKVol.14. No.2, Agustus 2012: 137-150. Palembang

Hafiz, Aliy. 2022. Keamanan Database: Pengertian, Konsep, Serangan dan Pengamanannya. https://aliyhafiz.com/keamanan-database-pengertian-dan-pengamanannya/ Diakses pada tanggal 01 Mei 2023

Noname. Http://idwebhost.com/blog/panduan-lengkap-tentang-database/ Diakses pada tanggal 01Mei 2023