JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 7 Desember 2025
ISSN 3025-0919 (media online)
Hal 1557-1560

Manajemen User Dan Keamanan Akses Data Dalam DBMS

Aldi Juli Wahyudi

Fakultas ilmu komputer, Universitas Pamulang - Indonesia

Email : aldijuliwahyudi2024@gmail.com

Abstrak- Sistem Manajemen Basis Data (Database Management System/DBMS) berfungsi tidak hanya sebagai media penyimpanan data, tetapi juga sebagai lapisan perlindungan yang krusial terhadap ancaman keamanan. Dengan semakin berkembangnya teknologi dan meningkatnya ancaman siber, penerapan manajemen user yang efektif dan sistem keamanan akses data yang kuat menjadi prioritas utama dalam desain dan pengoperasian DBMS modern. Penelitian ini bertujuan menjelaskan prinsip-prinsip manajemen user, mekanisme keamanan akses data seperti autentikasi, otorisasi, Role-Based Access Control (RBAC), enkripsi, serta logging dan auditing, serta meninjau penerapannya pada sistem MySQL dan PostgreSQL. Kajian ini juga membahas tantangan implementasi serta rekomendasi praktis yang dapat digunakan untuk meningkatkan keamanan DBMS dalam berbagai lingkungan operasional.

Kata kunci: DBMS, keamanan data, manajemen user, autentikasi, otorisasi, RBAC, enkripsi, audit log.

Abstract—A Database Management System (DBMS) functions not only as a medium for data storage but also as a crucial protection layer against security threats. With the rapid advancement of technology and the rise of cyber threats, implementing effective user management and robust data access security has become a top priority in the design and operation of modern DBMS. This study aims to explain the principles of user management, data access security mechanisms such as authentication, authorization, Role-Based Access Control (RBAC), encryption, as well as logging and auditing, and to review their implementation in MySQL and PostgreSQL systems. The discussion also highlights implementation challenges and provides practical recommendations to enhance DBMS security across various operational environments.

Keywords: DBMS, data security, user management, authentication, authorization, RBAC, encryption, audit log.

1. PENDAHULUAN

Peran DBMS dalam sistem informasi modern sangat vital, mengingat hampir semua aplikasi yang mengelola informasi terstruktur membutuhkan mekanisme untuk menyimpan, mengambil, dan mengolah data dengan aman. DBMS seperti MySQL, PostgreSQL, Oracle, dan SQL Server tidak hanya dirancang untuk menyediakan kinerja tinggi dalam manajemen data, tetapi juga dilengkapi dengan fitur-fitur keamanan yang bertujuan untuk melindungi data dari ancaman eksternal maupun internal. Salah satu aspek terpenting dalam keamanan DBMS adalah manajemen user, yang menentukan siapa saja yang dapat mengakses sistem dan sejauh mana hak akses yang dimiliki oleh masing-masing pengguna.

Selain itu, keamanan akses data menjadi aspek yang tidak kalah penting. Keamanan akses data meliputi serangkaian mekanisme untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses atau memodifikasi data tertentu. Implementasi keamanan ini melibatkan berbagai teknologi dan kebijakan seperti autentikasi yang kuat, otorisasi yang tepat, enkripsi, serta pemantauan aktivitas melalui logging dan auditing.

2. METODE PENELITIAN

2.1 Desain Penelitian

Penelitian ini menggunakan pendekatan **deskriptif kualitatif** dengan metode studi literatur dan studi kasus implementasi. Desain deskriptif dipilih untuk memberikan gambaran yang jelas mengenai prinsip-prinsip manajemen user serta mekanisme keamanan akses data dalam DBMS. Pendekatan kualitatif memungkinkan peneliti menganalisis berbagai kebijakan, fitur keamanan,

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 7 Desember 2025
ISSN 3025-0919 (media online)
Hal 1557-1560

serta praktik terbaik yang diterapkan dalam DBMS modern, khususnya pada MySQL dan PostgreSQL.

2.2 Sumber Data

Sumber data dalam penelitian ini terdiri atas:

1. **Data primer sekunder** berupa dokumentasi resmi dari MySQL dan PostgreSQL terkait fitur manajemen user dan keamanan akses data.
2. **Literatur akademik** seperti buku teks, artikel jurnal, dan prosiding konferensi yang membahas keamanan DBMS, manajemen user, autentikasi, otorisasi, RBAC, enkripsi, serta logging dan auditing.
3. **Studi kasus implementasi** pada MySQL 8.0 dan PostgreSQL, yang digunakan untuk mengevaluasi efektivitas mekanisme keamanan dalam skenario nyata.

2.3 Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui teknik **dokumentasi** dan **studi pustaka**. Dokumentasi dilakukan dengan meninjau manual resmi DBMS (MySQL Documentation, PostgreSQL Documentation) dan modul keamanan yang tersedia. Studi pustaka diperoleh dari penelitian terdahulu yang relevan, baik nasional maupun internasional, dengan rentang tahun terbaru (2016–2024) untuk memastikan relevansi dan kemutakhiran informasi.

3.LANDASAN TEORI

DBMS adalah perangkat lunak yang mengatur penyimpanan, pengambilan, dan pemeliharaan data dalam basis data. Salah satu fondasi penting dalam desain DBMS adalah keamanan data, yang secara umum dapat dikategorikan berdasarkan model CIA Triad: Confidentiality, Integrity, dan Availability. Confidentiality bertujuan menjaga kerahasiaan informasi dari pihak yang tidak berwenang. Integrity memastikan bahwa data tetap konsisten dan akurat selama siklus hidupnya. Availability memastikan bahwa data dapat diakses kapanpun diperlukan oleh pihak yang memiliki otorisasi.

Selain konsep CIA Triad, teori manajemen user dalam DBMS juga menjadi pilar keamanan. Manajemen user mengacu pada proses pembuatan, pengelolaan, dan penghapusan akun pengguna, pengelompokan pengguna ke dalam role atau grup tertentu, serta penetapan hak akses yang sesuai dengan kebutuhan operasional mereka. Hak akses ini sering didefinisikan dalam bentuk privilege, seperti SELECT, INSERT, UPDATE, DELETE, yang dapat dibatasi berdasarkan tabel, skema, atau bahkan kolom tertentu.

3.1 Manajemen User dalam DBMS

Manajemen user merupakan mekanisme yang mengatur identitas dan hak akses pengguna dalam DBMS. Tahapan utamanya meliputi: (1) Pembuatan user dengan kredensial unik (username dan password atau metode autentikasi lain seperti sertifikat digital), (2) Pengaturan role dan grup untuk menyederhanakan pemberian hak akses kepada banyak pengguna dengan kebutuhan yang sama, dan (3) Pemberian privilege yang menentukan tindakan apa saja yang dapat dilakukan oleh pengguna terhadap objek tertentu di dalam database.

Praktik terbaik dalam manajemen user meliputi penggunaan principle of least privilege, yaitu memberikan hak akses minimum yang diperlukan pengguna untuk menjalankan tugasnya. Selain itu, manajemen user yang baik juga melibatkan pencabutan hak akses dari akun yang sudah tidak digunakan, penggunaan kata sandi yang kuat dan kebijakan pergantian kata sandi secara berkala, serta integrasi dengan sistem autentikasi terpusat seperti LDAP atau Active Directory.

3.2 Mekanisme Keamanan Akses Data

Keamanan akses data dalam DBMS umumnya dibangun melalui kombinasi beberapa mekanisme. Pertama, autentikasi memastikan bahwa hanya pengguna yang telah terverifikasi yang dapat masuk ke sistem. Kedua, otorisasi mengatur sejauh mana pengguna tersebut dapat berinteraksi dengan data

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 7 Desember 2025
ISSN 3025-0919 (media online)
Hal 1557-1560

dan objek dalam database. Ketiga, RBAC memungkinkan pengelolaan hak akses yang efisien dengan menetapkan hak akses berdasarkan peran, bukan per individu. Keempat, enkripsi melindungi data baik dalam kondisi diam (at rest) maupun saat ditransfer melalui jaringan (in transit). Kelima, logging dan auditing memungkinkan pemantauan aktivitas yang dilakukan oleh pengguna, yang berguna untuk deteksi intrusi maupun investigasi insiden keamanan.

3.3 Studi Kasus Implementasi

Pada MySQL 8.0, pengelolaan keamanan dilakukan melalui fitur role management, yang memungkinkan administrator membuat role tertentu dan memberikan privilege pada role tersebut, kemudian menetapkannya ke user. MySQL juga mendukung enkripsi data menggunakan fungsi AES_ENCRYPT() dan koneksi aman dengan SSL/TLS. Audit plugin seperti audit_log dapat digunakan untuk mencatat seluruh aktivitas query yang dilakukan pengguna.

Di PostgreSQL, pengelolaan hak akses dilakukan menggunakan RBAC dengan dukungan role inheritance. PostgreSQL dapat menggunakan enkripsi dengan integrasi OpenSSL untuk mengamankan koneksi melalui SSL/TLS. Ekstensi pgAudit memungkinkan pencatatan aktivitas pengguna secara detail, yang sangat berguna untuk keperluan audit dan kepatuhan regulasi.

3.4 Tantangan dan Rekomendasi

Tantangan utama dalam manajemen user dan keamanan akses data meliputi kompleksitas pengaturan hak akses di organisasi besar, ancaman dari pengguna internal yang memiliki hak akses sah (insider threat), dampak enkripsi dan logging terhadap kinerja sistem, serta pemenuhan persyaratan regulasi seperti GDPR atau HIPAA. Untuk mengatasi tantangan ini, disarankan penggunaan RBAC, penerapan enkripsi menyeluruh, penggunaan multi-factor authentication, pelaksanaan audit dan review hak akses secara berkala, serta penerapan prinsip least privilege.

4. ANALISA DAN PEMBAHASAN

4.1 Analisis Konsep Keamanan DBMS

Berdasarkan teori keamanan data, kerangka **CIA Triad** (Confidentiality, Integrity, Availability) menjadi fondasi dalam penerapan keamanan DBMS. Confidentiality dijamin melalui mekanisme autentikasi, otorisasi, RBAC, dan enkripsi. Integrity diwujudkan dengan pembatasan privilege agar hanya pengguna tertentu yang dapat memodifikasi data. Availability dijaga dengan monitoring, logging, dan audit agar akses tidak terganggu serta aktivitas sistem dapat dievaluasi ketika terjadi insiden. Analisis ini menunjukkan bahwa setiap komponen CIA saling melengkapi dalam menjaga keamanan data pada DBMS modern.

4.2 Analisis Manajemen User

Manajemen user merupakan aspek paling mendasar dalam kontrol akses. Analisis terhadap literatur dan dokumentasi DBMS menunjukkan bahwa penerapan prinsip **least privilege** sangat efektif dalam mengurangi risiko penyalahgunaan hak akses. Pembuatan user dengan kredensial unik, pengelompokan user ke dalam role, serta pemberian privilege berbasis kebutuhan operasional terbukti mampu meningkatkan efisiensi administrasi sekaligus memperkuat keamanan. Namun, tantangan yang diidentifikasi adalah kompleksitas pengaturan role di organisasi besar yang dapat menimbulkan kesalahan konfigurasi jika tidak dikelola secara disiplin.

4.3 Analisis Mekanisme Keamanan Akses Data

Perbandingan MySQL dan PostgreSQL memperlihatkan perbedaan dalam pendekatan keamanan:

a) **MySQL 8.0** menyediakan *role management* yang memudahkan pengelolaan privilege, mendukung enkripsi data dengan fungsi bawaan (AES_ENCRYPT), serta koneksi aman melalui SSL/TLS. Audit log plugin juga memungkinkan pencatatan aktivitas query.

b) **PostgreSQL** memiliki mekanisme **RBAC dengan role inheritance** yang lebih fleksibel dibandingkan MySQL, mendukung enkripsi koneksi dengan OpenSSL, serta menyediakan ekstensi **pgAudit** untuk audit yang lebih detail.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 7 Desember 2025
ISSN 3025-0919 (media online)
Hal 1557-1560

Analisis ini menunjukkan bahwa PostgreSQL lebih unggul dalam hal audit dan fleksibilitas RBAC, sedangkan MySQL lebih praktis untuk implementasi enkripsi berbasis fungsi.

5. KESIMPULAN

Manajemen user dan keamanan akses data merupakan aspek fundamental dalam desain dan operasional DBMS yang aman. DBMS modern menawarkan berbagai fitur keamanan yang dapat dimanfaatkan untuk melindungi data, namun keberhasilan implementasinya bergantung pada kebijakan pengelolaan yang tepat, prosedur operasional yang disiplin, serta kesadaran keamanan dari seluruh pengguna. Dengan pendekatan yang terintegrasi antara teknologi dan kebijakan, risiko keamanan dapat diminimalkan, dan data dapat tetap terlindungi dari ancaman baik internal maupun eksternal.

DAFTAR PUSTAKA

Silberschatz, A., Korth, H. F., & Sudarshan, S. (2020). Database System Concepts. McGraw-Hill Education.

Elmasri, R., & Navathe, S. B. (2016). Fundamentals of Database Systems. Pearson.

MySQL Documentation.

PostgreSQL Documentation.

Sharma, S. (2019). Database Security. Springer.