



SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi,
dan Teknik Informatika

<https://ejurnal.itats.ac.id/snestik> dan <https://snestik.itats.ac.id>



Informasi Pelaksanaan :

SNESTIK V - Surabaya, 26 April 2025

Fakultas Teknik Elektro dan Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:

DOI : 10.31284/p.snestik.2025.7370

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043 Email
: snestik@itats.ac.id

Implementasi Hak Akses untuk Meningkatkan Keamanan Manajemen Hotel ABC Berbasis Database MySQL

Wahyu Nisfu Melati Sukma, Rikha Maisya Kotalima, Hisyam Abiansyah Gazani,
Anindo Saka Fitri, Agung Brastama Putra

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan
Nasional “Veteran” Jawa Timur

e-mail: 22082010230@student.upnjatim.ac.id

ABSTRACT

Hotel management systems require effective and secure data management to protect sensitive information such as guest data, transactions, and other personal information. This research implements a MySQL-based access rights mechanism to improve the security of the hotel management system. The design of access rights is developed based on the roles of hotel staff, including managers, receptionists, and guests, each of which is given access rights according to their operational needs. Implementation was done using SQL commands such as GRANT and REVOKE through the CMD terminal to ensure appropriate access rights management. The test results show that the implementation of structured access rights can reduce the risk of security breaches, improve operational efficiency, and strengthen user confidence in the system. This research makes a significant contribution to the development of database-based management systems with a focus on data security.

Keywords: MySQL, access privileges, data security

ABSTRAK

Sistem manajemen hotel memerlukan pengelolaan data yang efektif dan aman untuk melindungi informasi sensitif seperti data tamu, transaksi, dan informasi pribadi lainnya. Penelitian ini mengimplementasikan mekanisme hak akses berbasis MySQL guna meningkatkan keamanan sistem manajemen hotel. Desain hak akses dikembangkan berdasarkan peran staf hotel, meliputi manajer, resepsionis, dan tamu, yang masing-masing diberikan hak akses sesuai kebutuhan operasionalnya. Implementasi dilakukan menggunakan perintah SQL seperti GRANT dan REVOKE melalui terminal CMD untuk memastikan pengelolaan hak akses yang sesuai. Hasil pengujian menunjukkan bahwa penerapan hak akses yang terstruktur dapat mengurangi risiko pelanggaran keamanan, meningkatkan efisiensi operasional, dan memperkuat kepercayaan pengguna terhadap sistem. Penelitian ini memberikan kontribusi signifikan terhadap pengembangan sistem manajemen berbasis database dengan fokus pada keamanan data.

Kata kunci: MySQL, hak akses, keamanan data

PENDAHULUAN

Dalam era digital saat ini, keamanan informasi menjadi perhatian utama bagi banyak organisasi, termasuk industri perhotelan [1]. Dengan meningkatnya ancaman terhadap data, penerapan mekanisme kontrol akses yang efektif menjadi sangat penting untuk melindungi informasi dari akses yang tidak sah [2]. Dalam pengelolaan sistem basis data, pengaturan hak akses memegang peranan penting dalam menjaga keamanan dan integritas data [3]. Penerapan hak akses yang tepat pada perancangan database hotel dapat meningkatkan keamanan dari aktivitas yang tidak diinginkan [4]. Oleh karena itu, sistem otorisasi akses terbatas perlu diterapkan untuk memastikan bahwa hanya pihak yang berwenang yang memiliki akses ke data sensitif [5]. Hal ini tidak hanya mengurangi risiko penyalahgunaan data tetapi juga membantu dalam memenuhi regulasi privasi yang berlaku [6].

Sistem database MySQL menyediakan berbagai fitur untuk mengatur hak akses pengguna, seperti perintah GRANT dan REVOKE [7]. Pengaturan ini memungkinkan administrator untuk memberikan atau mencabut hak akses berdasarkan kebutuhan pengguna, sehingga hanya pihak yang berwenang yang dapat mengakses data tertentu [8]. Dokumentasi resmi MySQL (2024) juga menjelaskan pengaturan kontrol akses secara komprehensif, mulai dari tingkat database, tabel, kolom, hingga prosedur yang spesifik, yang sangat penting dalam lingkungan multi-user seperti sistem hotel [9].

Penelitian menunjukkan bahwa penerapan hak akses yang tepat dapat secara signifikan mengurangi risiko kebocoran data dan serangan siber, yang merupakan tantangan utama dalam pengelolaan informasi di sektor perhotelan [10]. Beberapa penelitian lain juga telah membahas pentingnya kontrol akses pada sistem berbasis MySQL, seperti studi oleh Firmansyah et al. (2021) yang menerapkan Role-Based Access Control (RBAC) untuk meningkatkan keamanan data dalam sistem manajemen [11]. Penelitian lain oleh Syahputra dan Lestari (2021) menunjukkan bahwa konfigurasi hak akses yang tepat mampu mengurangi potensi serangan siber dalam sistem basis data [12]. Implementasi hak akses yang cermat tidak hanya melindungi data tetapi juga meningkatkan kepercayaan pelanggan terhadap sistem manajemen hotel [13].

Meski sudah terdapat sejumlah penelitian terkait, sebagian besar masih berfokus pada implementasi teknis secara umum atau belum secara spesifik diterapkan dalam konteks operasional hotel. Penelitian ini memiliki fokus yang berbeda karena secara khusus mengeksplorasi penerapan hak akses dalam sistem manajemen Hotel ABC berbasis MySQL, serta menguji efektivitasnya dalam meningkatkan efisiensi dan keamanan data. Dengan demikian, penelitian ini bertujuan untuk memberikan rekomendasi implementasi hak akses yang efektif guna meningkatkan keamanan dan efisiensi dalam manajemen hotel serta memberikan

kontribusi signifikan terhadap pengembangan sistem manajemen berbasis database dengan fokus pada keamanan data.

METODE

Pada penelitian ini akan menggunakan pendekatan eksperimental yaitu suatu metode yang memungkinkan peneliti untuk menerapkan dan menguji langsung suatu perlakuan atau kebijakan terhadap objek yang diteliti[14]. Pendekatan eksperimental efektif digunakan dalam pengujian sistem informasi karena dapat mengidentifikasi dampak langsung dari penerapan fitur terhadap keamanan atau efisiensi sistem[15].

1. Analisis Kebutuhan: Mengidentifikasi jenis data yang dikelola oleh sistem manajemen hotel dan pihak yang memerlukan akses ke data tersebut.
2. Desain Hak Akses: Membuat desain hierarki hak akses berdasarkan peran staf hotel, seperti manajer, resepsionis, dan staf housekeeping.
3. Implementasi di MySQL melalui Command Line (CMD):
 - a. Menggunakan perintah SQL untuk membuat database dan tabel.
 - b. Menentukan hak akses menggunakan perintah GRANT dan REVOKE melalui terminal CMD.
 - c. Menerapkan kontrol akses dengan mendefinisikan user roles sesuai dengan hierarki.
4. Pengujian Keamanan: Menguji efektivitas hak akses dengan melakukan simulasi berbagai skenario, termasuk upaya akses tidak sah.



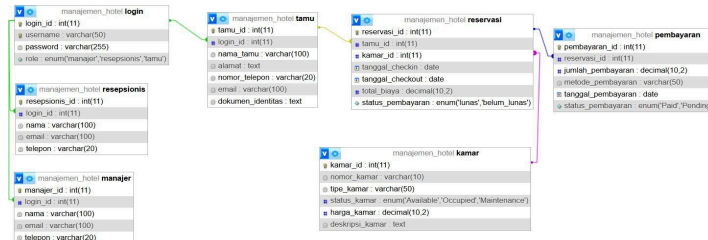
Gambar 1. Alur penelitian

HASIL DAN PEMBAHASAN

1. Analisis Kebutuhan
 - a. Manajer: Membutuhkan akses penuh untuk mengelola laporan pendapatan, memantau status kamar, dan mengelola data reservasi, tamu, dan pembayaran.
 - b. Resepsionis: Membutuhkan akses untuk membaca dan memperbarui data tamu, kamar, dan reservasi, tetapi tidak memiliki hak untuk menghapus data atau mengubah status pembayaran.
 - c. Tamu: Membutuhkan akses terbatas untuk melihat dan mengelola reservasi mereka sendiri, tanpa hak untuk mengakses data tamu lain.
2. Desain Hak Akses
 - a. Manajer hotel memiliki hak akses penuh ke semua data, termasuk informasi tamu, reservasi, pembayaran, dan laporan. Manajer dapat membaca, menambah, memperbarui, dan menghapus data apa pun. Tugas utamanya adalah mengelola laporan pendapatan hotel serta memantau status kamar,

- seperti yang terisi, kosong, atau dalam perbaikan.
- b. Resepsionis memiliki hak akses untuk membaca data kamar, tamu, dan reservasi, serta dapat menambah atau memperbarui data reservasi. Resepsionis juga dapat melihat status pembayaran namun tidak dapat mengubahnya atau menghapus data. Tugas resepsionis meliputi melayani check-in dan check-out tamu serta mencatat pembayaran untuk reservasi.
 - c. Tamu hanya memiliki akses untuk melihat data reservasi mereka sendiri, melakukan reservasi atau pembatalan jika diperlukan, dan tidak dapat melihat atau mengubah data tamu lain. Tugas mereka adalah membuat reservasi kamar dan melihat informasi tagihan atau status reservasi yang relevan.
3. Implementasi di MySQL melalui Command Prompt (CMD) :
- a. Membuat database dan tabel

Pada Command Prompt dibuat terlebih dahulu database nya bernama menggunakan CREATE DATABASE manajemen_hotel. Lalu dilanjutkan untuk membuat tabel - tabel dari user beserta aktivitasnya. Menggunakan CREATE TABLE login, CREATE TABLE reservasi, dan seterusnya. Desain tabel dan relationship dapat dilihat pada gambar 2.



Gambar 2. Desain tabel relationship

- b. Menentukan Hak Akses

Hak akses diberikan kepada setiap user sesuai dengan kebutuhannya. Manajer diberikan hak akses penuh termasuk mencabut hak akses, maka perintah hak akses untuk manajer akan diberikan secara keseluruhan pada setiap aktivitas dan setiap user. Resepsionis diberikan hak akses untuk melakukan pengelolaan reservasi tamu serta melihat data kamar dan pengunjung. Tamu diberikan batasan hak akses hanya dapat menentukan proses reservasinya sendiri dan melakukan pembayaran.

- c. Menerapkan kontrol akses

Perintah menambahkan dan mencabut hak akses menggunakan perintah GRANT dan REVOKE seperti dibawah ini :

- a) Manajer

```

MariaDB [manajemen_hotel]> GRANT ALL PRIVILEGES ON manajemen_hotel.* TO 'manajer'@'localhost';
Query OK, 0 rows affected (0.005 sec)
    
```

Manajer pada gambar 2 diberikan hak akses penuh dengan menggunakan perintah GRANT ALL PRIVILEGES ON manajemen_hotel.* TO 'manajer'@'localhost'.

- b) Resepsionis

```
MariaDB [manajemen_hotel]> GRANT SELECT, INSERT, UPDATE ON manajemen_hotel.tamu TO 'resepionis'@'localhost';
Query OK, 0 rows affected (0.002 sec)

MariaDB [manajemen_hotel]> GRANT SELECT, INSERT, UPDATE ON manajemen_hotel.reservasi TO 'resepionis'@'localhost';
Query OK, 0 rows affected (0.003 sec)

MariaDB [manajemen_hotel]> GRANT SELECT ON manajemen_hotel.kamar TO 'resepionis'@'localhost';
Query OK, 0 rows affected (0.000 sec)

MariaDB [manajemen_hotel]> GRANT SELECT ON manajemen_hotel.pembayaran TO 'resepionis'@'localhost';
Query OK, 0 rows affected (0.002 sec)
```

Resepionis pada gambar 3 diberikan hak akses yang terbatas dengan menggunakan perintah GRANT SELECT, INSERT, UPDATE ON manajemen_hotel.tamu TO 'resepionis'@'localhost' , GRANT SELECT, INSERT, UPDATE ON manajemen_hotel.reservasi TO 'resepionis'@'localhost', GRANT SELECT ON manajemen_hotel.kamar TO 'resepionis'@'localhost', GRANT SELECT ON manajemen_hotel.pembayaran TO 'resepionis'@'localhost'.

c) Tamu

```
MariaDB [manajemen_hotel]> GRANT SELECT, INSERT, UPDATE ON manajemen_hotel.reservasi TO 'tamu'@'localhost';
Query OK, 0 rows affected (0.002 sec)
```

Gambar 5. Memberi hak akses kepada tamu

Tamu pada gambar 5 diberikan hak akses hanya dapat melihat dan mengelola reservasinya sendiri menggunakan perintah GRANT SELECT, INSERT, UPDATE ON manajemen_hotel.reservasi TO 'tamu'@'localhost'.

d) Revoke

```
MariaDB [manajemen_hotel]> REVOKE CREATE ON manajemen_hotel.* FROM 'resepionis'@'localhost';
Query OK, 0 rows affected (0.001 sec)
```

Gambar 6. Mencabut/menghapus hak akses

Pada gambar 6 mencabut hak akses menggunakan REVOKE DELETE ON manajemen_hotel.* FROM 'resepionis'@'localhost'.

4. Pengujian Hak Akses

Pada gambar tersebut ketika resepsionis ingin melakukan perintah DELETE pembayaran menampilkan sintaks error. Artinya hak akses untuk resepsionis yang tidak mengizinkan untuk menghapus data pembayaran berjalan dengan baik.

Pengujian keamanan dilakukan untuk memastikan bahwa hak akses yang telah ditetapkan bekerja sesuai dengan hierarki peran yang dirancang. Berikut ini simulasi dari setiap user :

a. Simulasi hak akses manajer

```
MariaDB [manajemen_hotel]> SELECT * FROM kamar;
```

kamar_id	nomor_kamar	tipe_kamar	status_kamar	harga_kamar	deskripsi_kamar
1	101	Standard	Available	500000.00	Kamar dengan fasilitas standar
2	102	Deluxe	Occupied	750000.00	Kamar dengan fasilitas deluxe
3	103	Suite	Maintenance	1200000.00	Kamar suite dengan fasilitas premium

```
3 rows in set (0.001 sec)
```

Gambar 7. Manajer sebelum menambahkan data kamar

Gambar 7 tersebut menunjukkan data kamar lama yang belum ada data kamar baru di hotel. Dapat dilihat masih terdapat tiga kamar saja pada database tabel kamar tersebut.

```
MariaDB [manajemen_hotel]> SELECT * FROM kamar;
```

kamar_id	nomor_kamar	tipe_kamar	status_kamar	harga_kamar	deskripsi_kamar
1	101	Standard	Available	500000.00	Kamar dengan fasilitas standar
2	102	Deluxe	Occupied	750000.00	Kamar dengan fasilitas deluxe
3	103	Suite	Maintenance	1200000.00	Kamar suite dengan fasilitas premium
4	202	Deluxe	Available	750000.00	NULL

4 rows in set (0.000 sec)

Gambar 8. Manajer sesudah menambahkan data kamar

Gambar tersebut merupakan data kamar yang baru dimana terdapat kamar baru yang ingin ditambahkan atau disewakan. Maka pada tabel database kamar bertambah menjadi empat kamar karena telah ditambahkan oleh manajer.

b. Simulasi hak akses resepsionis

```
MariaDB [manajemen_hotel]> SELECT * FROM tamu;
```

tamu_id	login_id	nama_tamu	alamat	nomor_telepon	email	dokumen_identitas
4	3	Mela	Jl. Merpati No. 15, Surabaya	081223344556	mela123@gmail.com	KTP
5	4	Rikha	Jl. Kenanga No. 23, Surabaya	081334455667	rikha@gmail.com	KTP
6	5	Hisyam	Jl. Angrek No. 20, Sidoarjo	081556688997	hisyam321@gmail.com	KTP

3 rows in set (0.004 sec)

Gambar 9. resepsionis membaca data sebelum ada tamu baru

Gambar 9 diatas adalah data reservasi tamu yang dimiliki oleh resepsionis adalah data yang lama. Data tersebut berjumlah 3 orang tamu yang telah melakukan reservasi ke resepsionis di hotel.

```
MariaDB [manajemen_hotel]> SELECT * FROM tamu;
```

tamu_id	login_id	nama_tamu	alamat	nomor_telepon	email	dokumen_identitas
4	3	Mela	Jl. Merpati No. 15, Surabaya	081223344556	mela123@gmail.com	KTP
5	4	Rikha	Jl. Kenanga No. 23, Surabaya	081334455667	rikha@gmail.com	KTP
6	5	Hisyam	Jl. Angrek No. 20, Sidoarjo	081556688997	hisyam321@gmail.com	KTP
8	6	Manaya	Jl. Kamboja No. 20, Surabaya	0813399228856	manaya123@gmail.com	KTP

4 rows in set (0.000 sec)

Gambar 10. resepsionis membaca data sebelum ada tamu baru

Gambar 10 tersebut adalah data baru resepsionis setelah ada tamu yang telah melakukan reservasi. Tamu bertambah satu menjadi empat orang yang telah melakukan reservasi kamar.

c. Simulasi hak akses tamu

```
MariaDB [manajemen_hotel]> SELECT * FROM reservasi;
```

reservasi_id	tamu_id	kamar_id	tanggal_checkin	tanggal_checkout	total_biaya	status_pembayaran
9	4	3	2025-01-10	2025-01-15	3750000.00	lunas

1 row in set (0.001 sec)

Gambar 11. Data pembayaran reservasi tamu

Gambar 11 tersebut untuk tamu hanya bisa melihat data pembayaran reservasinya sendiri. Data pada tabel tersebut menampilkan bahwa tamu telah melakukan pelunasan terhadap kamar yang telah ia reservasi. Setiap tamu tidak dapat melihat reservasi ataupun pembayaran milik tamu yang lain.

5. Pengujian Hak Akses Tidak Sah

```
C:\xampp\mysql\bin>mysql -u resepsionis -p
Enter password: *****
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 390
Server version: 10.4.32-MariaDB mariadb.org binary distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SELECT * FROM pembayaran;
ERROR 1046 (3D000): No database selected
MariaDB [(none)]> USE manajemen_hotel;
Database changed
MariaDB [manajemen_hotel]> SELECT * FROM pembayaran;
```

pembayaran_id	reservasi_id	jumlah_pembayaran	metode_pembayaran	tanggal_pembayaran	status_pembayaran
5	14	1000000.00	Transfer	2025-01-09	Paid
6	15	2250000.00	Kartu Kredit	2025-01-14	Pending

2 rows in set (0.001 sec)

```
MariaDB [manajemen_hotel]> DELETE FROM pembayaran WHERE pembayaran_id = 5;
ERROR 1142 (42000): DELETE command denied to user 'resepsionis'@'localhost' for table 'manajemen_hotel`.`pembayaran`
MariaDB [manajemen_hotel]>
```

Gambar 12. Hak akses tidak sah resepsionis

Pengujian ini bertujuan untuk memastikan juga bahwa pada pihak manajemen hotel tidak melakukan kecurangan ataupun tindakan yang tidak diinginkan lainnya. Resepsionis tidak dapat melakukan tindakan diluar hak akses yang diberikan yaitu tidak

diberikan hak akses untuk menghapus data atau riwayat pembayaran reservasi. Dilihat pada gambar 12, resepsionis tidak dapat menghapus data atau riwayat pembayaran reservasi. Ditandai dengan munculnya sintaks error ketika memasukkan perintah DELETE.

KESIMPULAN

Penelitian ini menunjukkan bahwa implementasi hak akses berbasis MySQL dalam sistem manajemen Hotel ABC secara efektif meningkatkan keamanan data. Dengan mendesain struktur hak akses sesuai peran pengguna seperti manajer, resepsionis, dan tamu, sistem berhasil membatasi akses berdasarkan kebutuhan operasional masing-masing peran. Hasil pengujian membuktikan bahwa penggunaan perintah seperti GRANT dan REVOKE dapat menjaga integritas data serta mencegah akses tidak sah. Namun demikian, penelitian ini masih memiliki keterbatasan, seperti belum mengintegrasikan sistem dengan metode keamanan tambahan seperti autentikasi dua faktor atau audit log yang lebih kompleks. Untuk pengembangan ke depan, disarankan agar dapat dikembangkan lebih lanjut dengan mengkombinasikan hak akses database dengan pendekatan keamanan lainnya guna meningkatkan proteksi data secara menyeluruh.

DAFTAR PUSTAKA

- [1] Maulina, L. (2023). Revitalisasi Industri Perhotelan Dengan Inovasi Teknologi: Meningkatkan Keunggulan Bersaing Dan Pengalaman Pelanggan. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, 7(1), 504-519.
- [2] Yamin, A. F., Rachmawati, A., Pratama, R. A., & Wijaya, J. K. (2024). Perlindungan Data Pribadi Dalam Era Digital: Tantangan Dan Solusi. *Meraja journal*, 7(2), 138-155.
- [3] Harahap, S. W., Anisa, A., Pane, S. N., & Purba, M. A. R. (2023). DATABASE MANAGEMENT SYSTEM PT SIERAD PRODUCE Tbk DI MEDAN. *Jurnal Ilmiah Sains Teknologi Dan Informasi*, 1(3), 20-26.
- [4] Ahmadar, M., Perwito, P., & Taufik, C. (2021). Perancangan Sistem Informasi Penjualan Berbasis Web pada Rahayu Photo Copy dengan Database MySQL. *Dharmakarya: Jurnal Aplikasi Ipteks Untuk Masyarakat*, 10(4), 284-289.
- [5] Joko, T. (2023). Penerapan Hak Akses pada Perancangan Database Akademik untuk Meningkatkan Keamanan Data. *Indonesian Journal of Machine Learning and Computer Science*, 3(1), 50-59.
- [6] SoftwareSeni. (n.d.). *Hotel management systems: Meningkatkan efisiensi manajemen hotel di era digital*. SoftwareSeni. Retrieved January 10, 2025, from <https://www.softwareseni.co.id/blog/hotel-management-systems>
- [7] Ujung, A. M., & Nasution, M. I. P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *Jurnal Sistem Informasi Dan Informatika*, 1(2), 44-47.
- [8] BPTSI Universitas Aisyiyah Yogyakarta. (n.d.). *Membatasi hak akses user MySQL pada level basis data, tabel, kolom, dan baris*. Universitas Aisyiyah Yogyakarta. Retrieved January 11, 2025, from <https://bptsi.unisayogya.ac.id/membatasi-hak-akses-user-mysql-pada-level-basis-data-tabel-kolom-dan-baris/>
- [9] Oracle Corporation. (2024). *MySQL 8.0 Reference Manual: Access Control and Account Management*. <https://dev.mysql.com/doc/refman/8.0/en/access-control.html>
- [10] 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.
- [11] Firmansyah, D., Hartono, B., & Prasetyo, A. (2021). *Penggunaan Role-Based Access Control pada Database MySQL untuk Keamanan Data*. *Jurnal Informatika*, 8(2), 115-122.

- [12] Syahputra, R., & Lestari, M. (2021). *Evaluasi Implementasi Hak Akses pada Sistem Database dalam Mengurangi Ancaman Siber*. Jurnal Sistem Informasi dan Keamanan, 7(2), 90–99.
- [13] Khairi, A. S. (2024). Implementasi Role Based Access Control dalam Pengelolaan Hak Akses Koperasi Berbasis Mobile. Jurnal Teknik Informatika Unika ST. Thomas (JTIUST), 9(1).
- [14] Fadlan, M., Bintari, E. D., & Tasya, A. (2023). Pengamanan Basis Data Dengan Algoritma Transposisi Rail Fence. Jurnal Sistem Informasi dan Sistem Komputer, 8(2), 66-72.
- [15] Di Juni, P., Hasan, M. A., Sitompul, Y. S. P., Alexander, J., Hidayat, I., & Bilbo, R. M. (2025). AUDIT KEAMANAN BASIS DATA MENGGUNAKAN SQL SERVER AUDIT UNTUK DETEKSI AKTIVITAS TIDAK SAH. JATI (Jurnal Mahasiswa Teknik Informatika), 9(2), 2896-2903.