ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.5 No.1 Tahun 2026
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-5 2026
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2026

Implementasi Enkripsi AES-256-GCM untuk Melindungi Data Pelanggan Sensitif dalam Basis Data SQL

Implementation of AES-256-GCM Encryption for Protecting Sensitive Customer Records in SQL Databases

Eky Fikri Yamansyah[1], Zaky Putra Pratama[2]
[1,2]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]ekyfikriyamansyah@gmail.com, [2]zakyputraap@gmail.com*

Abstract

Protecting sensitive customer records in web-based database environments requires encryption mechanisms that ensure both confidentiality and integrity. This study implements AES-256-GCM encryption, leveraging its dual capability for encryption and authentication via Galois/Counter Mode (GCM). We integrated this algorithm into a MySQL database environment to secure data at rest. Unlike traditional methods, our implementation prioritizes a secure architectural design suitable for multi-user web applications. The experimental results confirm the functional feasibility of the proposed system, demonstrating successful encryption and decryption processes that ensure data confidentiality. Furthermore, the authentication mechanism effectively verified data integrity, preventing the storage or retrieval of tampered records. We conclude that AES-256-GCM provides a robust and reliable solution for securing sensitive information in MySQL databases without compromising functional stability.

Keywords: *AES-256-GCM, MySQL Security, Data Integrity, Authenticated Encryption, Web Database Protection.*

Abstrak

Perlindungan data sensitif pelanggan dalam lingkungan basis data berbasis web memerlukan mekanisme enkripsi yang menjamin kerahasiaan sekaligus integritas data. Penelitian ini mengimplementasikan enkripsi AES-256-GCM, yang memanfaatkan kemampuan ganda untuk enkripsi dan autentikasi melalui mode Galois/Counter Mode (GCM). Kami mengintegrasikan algoritma ini ke dalam lingkungan basis data MySQL untuk mengamankan data yang tersimpan (data at rest). Berbeda dengan metode tradisional, implementasi kami memprioritaskan desain arsitektur keamanan yang sesuai untuk aplikasi web dengan banyak pengguna. Hasil eksperimen mengonfirmasi kelayakan fungsional dari sistem yang diusulkan, menunjukkan keberhasilan proses enkripsi dan dekripsi yang menjamin kerahasiaan data. Selain itu, mekanisme autentikasi terbukti efektif dalam memverifikasi integritas data, serta mencegah penyimpanan atau pengambilan data yang telah dimanipulasi. Kami menyimpulkan bahwa AES-256-GCM memberikan solusi yang tangguh dan andal untuk mengamankan informasi sensitif dalam basis data MySQL tanpa mengorbankan stabilitas fungsional.

Kata kunci: AES-256-GCM, Keamanan MySQL, Integritas Data, Enkripsi Terautentikasi, Perlindungan Basis Data Web.

Pendahuluan

Dalam lanskap keamanan siber modern, aplikasi berbasis web yang terhubung dengan basis data SQL terus menjadi target utama eksploitasi. Data sensitif pelanggan yang tersimpan di dalamnya rentan terhadap berbagai serangan, terutama SQL Injection (SQLi). Merujuk pada statistik terbaru tahun 2025, SQLi masih mendominasi ancaman keamanan aplikasi web dan berkontribusi signifikan terhadap kebocoran data global dalam lima tahun terakhir [1]. Selain ancaman eksternal, risiko penyalahgunaan hak akses oleh pihak internal (*insider threats*) juga menuntut adanya mekanisme perlindungan yang tidak hanya mengandalkan kontrol akses, tetapi juga perlindungan kriptografi pada level data (*data at rest*) [2]. Oleh karena itu, penerapan enkripsi pada basis data menjadi kebutuhan mendesak untuk menjamin kerahasiaan informasi.

Sejumlah penelitian dalam kurun waktu 2021-2025 telah mengusulkan berbagai metode pengamanan basis data. McGiffen (2022) menyoroti efektivitas penggunaan Transparent Data Encryption (TDE) pada SQL Server untuk mengamankan seluruh file basis data [3]. Di sisi lain, Costa et al. (2022) mengevaluasi dampak performa enkripsi pada PostgreSQL dan MongoDB, yang menunjukkan bahwa enkripsi tingkat basis data sering kali membebani sumber daya CPU secara signifikan [4]. Sementara itu, studi terbaru dari Ammagunta et al. (2025) membahas penggunaan alat bantu berbasis open-source untuk mendeteksi serangan, namun kurang menekankan pada mekanisme pencegahan manipulasi data yang sudah tersimpan [5]. Studi komparatif oleh Prasetiya et al. (2024) membandingkan kinerja AES-GCM dengan ChaCha20-Poly1305, yang menunjukkan bahwa mode GCM unggul dalam efisiensi komputasi untuk aplikasi web [6]. Patria (2025) dalam analisisnya menegaskan bahwa pendekatan *Authenticated Encryption* memberikan perlindungan ganda yang tidak dimiliki oleh mode enkripsi konvensional [7].

Meskipun penelitian-penelitian terdahulu telah menawarkan solusi enkripsi, terdapat kesenjangan (*gap*) yang signifikan. Mayoritas implementasi yang ada, seperti TDE atau enkripsi standar AES-CBC (*Cipher Block Chaining*), hanya berfokus pada aspek kerahasiaan (*confidentiality*). Metode-metode ini tidak memiliki mekanisme bawaan untuk memverifikasi integritas data (*integrity*) [8]. Akibatnya, jika seorang penyerang berhasil memodifikasi *ciphertext* secara langsung di penyimpanan, sistem tidak dapat mendeteksi adanya manipulasi tersebut saat data didekripsi [9]. Selain itu, solusi enkripsi penuh (*full database encryption*) sering kali dianggap terlalu berat untuk aplikasi web yang membutuhkan latensi rendah. Ramadhan (2025) secara spesifik menyoroti bahwa proteksi integritas data statis pada database SQL sangat krusial untuk mencegah serangan modifikasi data (*data tampering*) [10].

Berangkat dari permasalahan tersebut, penelitian ini menawarkan pendekatan baru dengan mengimplementasikan algoritma AES-256-GCM (*Galois/Counter Mode*) secara spesifik pada level kolom untuk basis data MySQL. Kebaruan (*Novelty*) dari penelitian ini terletak pada pemanfaatan fitur *Authenticated Encryption* (AE) dari mode GCM dalam lingkungan aplikasi web. Berbeda dengan AES-CBC, AES-256-GCM tidak hanya mengenkripsi data tetapi juga menghasilkan tag autentikasi, yang memungkinkan sistem untuk mendeteksi segala bentuk perubahan tidak sah pada data secara *real-time* saat proses pengambilan data (*retrieval*) [11]. Pendekatan ini dipilih untuk menyeimbangkan kebutuhan keamanan tingkat tinggi dengan efisiensi performa yang lebih baik dibandingkan enkripsi tingkat file [12]. Studi oleh Jehian et al. (2025) menunjukkan bahwa kombinasi algoritma enkripsi modern dengan fungsi derivasi kunci seperti Argon2 dapat memperkuat keamanan secara signifikan [13]. Pengujian pada lingkungan komputasi awan oleh Perdana dan Bhawiyuga (2025) membuktikan bahwa AES-GCM memberikan stabilitas *throughput* yang unggul [14]. Kurniawan (2024) dalam penelitiannya mengonfirmasi bahwa enkripsi tingkat kolom pada MySQL 8.0 dengan AES-GCM memberikan efisiensi ruang penyimpanan yang signifikan bagi aplikasi dengan trafik tinggi [15].

Oleh karena itu, tujuan utama dari penelitian ini adalah untuk merancang, mengimplementasikan, dan menguji kinerja algoritma AES-256-GCM dalam mengamankan rekaman data pelanggan pada basis data MySQL. Penelitian ini bertujuan untuk membuktikan bahwa metode yang diusulkan mampu menjamin kerahasiaan dan integritas data secara simultan dengan dampak minimal terhadap waktu respons aplikasi web.

Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimental dengan merancang arsitektur keamanan basis data berbasis enkripsi terautentikasi. Sistem diuji pada lingkungan aplikasi web multi-user yang terhubung dengan basis data MySQL. Data pelanggan sensitif ditentukan sebagai objek penelitian dan dienkripsi sebelum disimpan ke dalam basis data.

Tabel 1 Spesifikasi Algoritma Enkripsi AES-256-GCM

Parameter	Nilai
Algoritma	Advanced Encryption Standard (AES)
Mode Operasi	Galois/Counter Mode (GCM)
Panjang Kunci	256 bit
Panjang Initialization Vector (IV)	96 bit (12 byte)
Panjang Authentication Tag	128 bit (16 byte)
Jenis Enkripsi	Authenticated Encryption
Format Penyimpanan	IV:AuthTag:CipherText

Tabel 1 menunjukkan spesifikasi algoritma kriptografi yang digunakan dalam penelitian ini. Algoritma AES dengan mode operasi Galois/Counter Mode (GCM) dipilih karena mampu menyediakan dua aspek keamanan utama secara simultan, yaitu kerahasiaan (confidentiality) dan integritas data (integrity). Penggunaan kunci sepanjang 256 bit memberikan tingkat keamanan yang tinggi terhadap serangan brute force, sementara panjang IV 96 bit dan authentication tag 128 bit mengikuti rekomendasi standar kriptografi modern untuk implementasi AES-GCM yang aman.

Tabel 2 Jenis Data Sensitif yang Dienkripsi

No	Jenis Data	Kategori Data
1	Nomor Induk Kependudukan (NIK)	Data Pribadi
2	Tanggal Lahir	Data Pribadi
3	Nomor Telepon	Data Pribadi
4	Alamat Lengkap	Data Pribadi
5	Nomor Kartu Pembayaran	Data Keuangan
6	Masa Berlaku Kartu	Data Keuangan
7	CVV	Data Keuangan

Tabel 2 memperlihatkan jenis data sensitif pelanggan yang menjadi objek penelitian. Data-data tersebut diklasifikasikan ke dalam kategori data pribadi dan data keuangan, yang memiliki tingkat sensitivitas tinggi dan berisiko apabila terjadi kebocoran. Oleh karena itu, seluruh atribut pada tabel ini dienkripsi menggunakan AES-256-GCM sebelum disimpan ke dalam basis data untuk mencegah akses tidak sah serta penyalahgunaan informasi.

Arsitektur enkripsi dirancang pada tingkat aplikasi, di mana proses enkripsi dilakukan sebelum data dikirim ke server basis data. Setiap atribut sensitif dienkripsi menggunakan algoritma AES-256-GCM dengan kunci simetris berukuran 256-bit. Proses enkripsi menghasilkan ciphertext, initialization vector (IV), dan authentication tag yang disimpan secara terpisah dalam basis data.

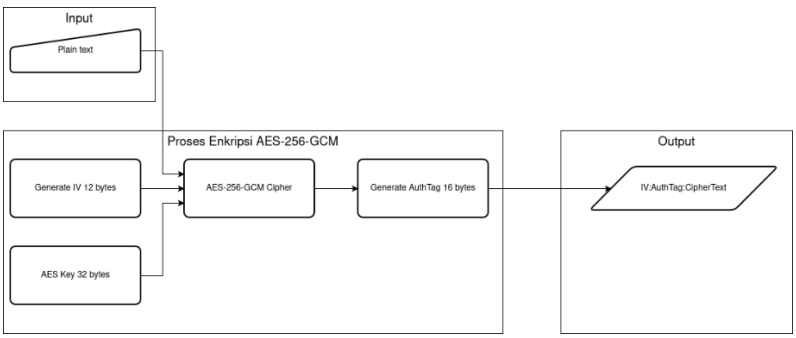
Manajemen kunci dilakukan dengan prinsip pemisahan tugas, di mana kunci enkripsi tidak disimpan di dalam basis data melainkan pada lapisan aplikasi dengan mekanisme perlindungan tambahan. Proses dekripsi hanya dapat dilakukan apabila authentication tag tervalidasi, sehingga setiap perubahan tidak sah pada data akan menyebabkan proses dekripsi gagal.

Tahapan penelitian meliputi perancangan skema enkripsi, implementasi pada aplikasi web, pengujian fungsional enkripsi dan dekripsi, serta analisis keamanan terhadap potensi manipulasi data. Keberhasilan sistem dievaluasi berdasarkan kemampuan menjaga confidentiality dan integrity data pelanggan.

Alur kerja sistem aplikasi dirancang untuk memastikan bahwa seluruh data sensitif dienkripsi sebelum disimpan dan hanya dapat didekripsi setelah melalui proses verifikasi integritas.

Gambar 1 Flowchart alur kerja sistem aplikasi

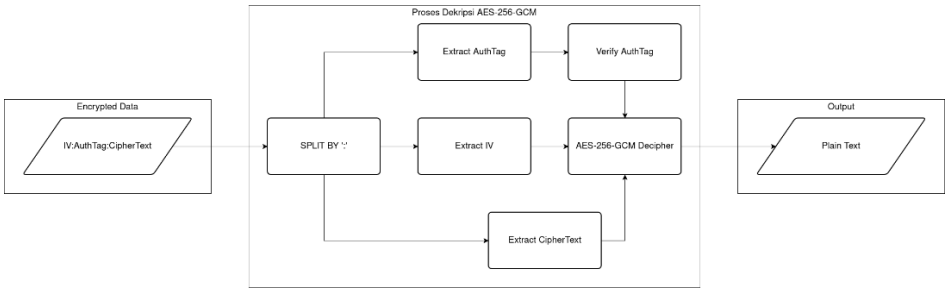
Mekanisme enkripsi data sensitif pada sistem ini dilakukan menggunakan algoritma AES-256-GCM. Proses enkripsi data ditunjukkan pada Gambar 2.



Gambar 2 Diagram proses enkripsi AES-256-GCM

Gambar 2 menggambarkan proses enkripsi data, di mana plaintext diproses menggunakan kunci rahasia dan initialization vector (IV) untuk menghasilkan ciphertext serta authentication tag. Kombinasi ini memastikan kerahasiaan dan integritas data secara simultan.

Proses dekripsi data dilakukan dengan memverifikasi authentication tag sebelum data dikembalikan ke bentuk semula. Diagram proses dekripsi ditunjukkan pada Gambar 3.

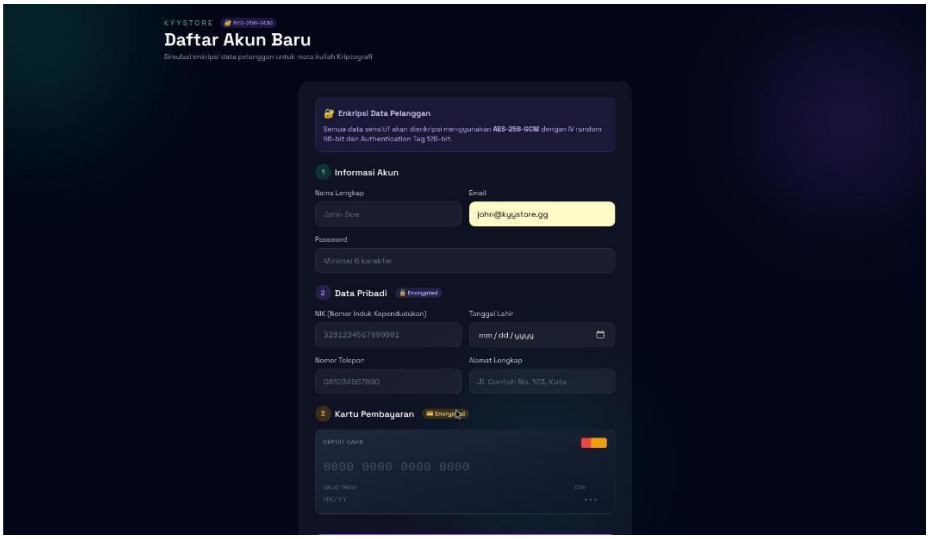


Gambar 3 Diagram proses dekripsi AES-256-GCM

Gambar 3 menunjukkan proses dekripsi data terenkripsi. Sistem akan memverifikasi authentication tag terlebih dahulu untuk memastikan integritas data. Apabila terjadi perubahan pada ciphertext, IV, atau authentication tag, maka proses dekripsi akan gagal.

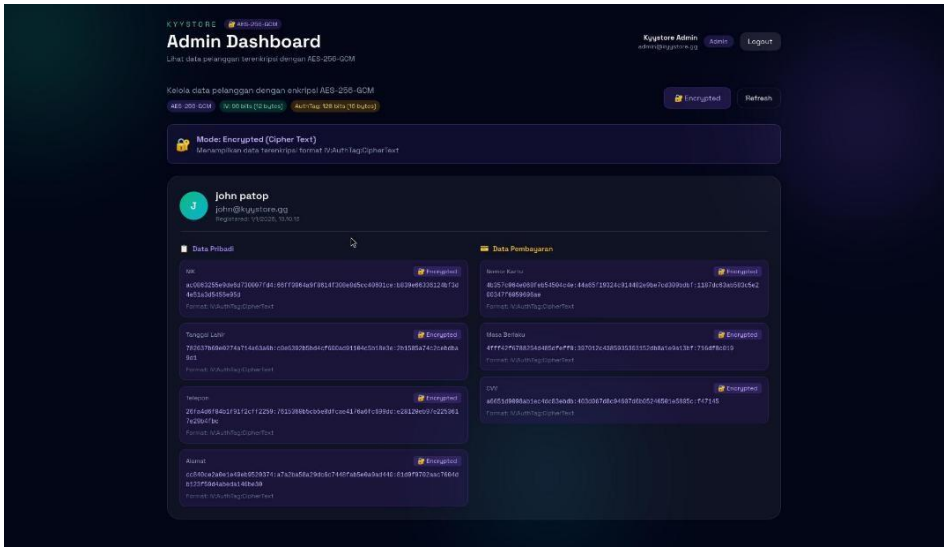
Hasil dan Pembahasan

Hasil pengujian menunjukkan bahwa seluruh data pelanggan sensitif yang disimpan dalam basis data MySQL berhasil dienkripsi menggunakan AES-256-GCM. Data yang tersimpan dalam bentuk ciphertext tidak dapat dibaca secara langsung meskipun penyerang memperoleh akses ke basis data. Hal ini menunjukkan terpenuhinya aspek confidentiality.



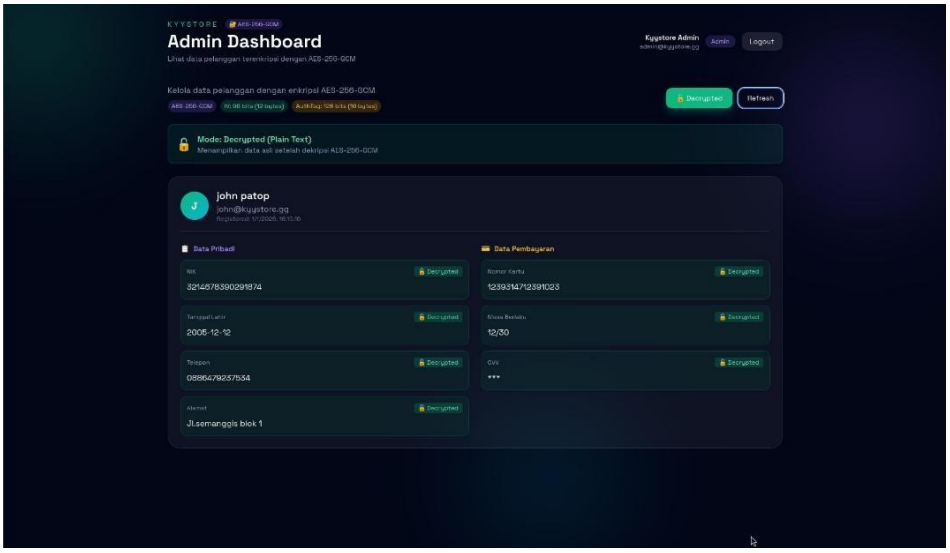
Gambar 4 Antarmuka pendaftaran akun dengan enkripsi AES-256-GCM

Gambar 4 menunjukkan antarmuka pendaftaran pengguna, di mana seluruh data sensitif dienkripsi menggunakan algoritma AES-256-GCM sebelum disimpan ke dalam basis data.



Gambar 5 Tampilan Dashboard Data Terenkripsi

Gambar 5 menunjukkan tampilan data pelanggan dalam kondisi terenkripsi pada dashboard admin, yang membuktikan bahwa data tetap terlindungi meskipun basis data diakses tanpa izin. Proses dekripsi hanya dapat dilakukan apabila authentication tag berhasil diverifikasi.



Gambar 6 Tampilan Dashboard Data Terdekripsi

Perbandingan antara data sebelum dan sesudah enkripsi menunjukkan bahwa mekanisme enkripsi berhasil menjaga kerahasiaan data pelanggan.

Tabel 3 Perbandingan Data Plaintext dan Ciphertext

Jenis Data	Plaintext	Ciphertext
NIK	3214678390291874	a0c8b3e59d6e…
Nomor Telepon	0886479237534	26fa4d6f84b1…
Nomor Kartu	1239314712391023	4b357c064e08…
CVV	123	a6651d9098ab…

Tabel 3 menunjukkan perbandingan antara data asli (plaintext) dan data setelah melalui proses enkripsi menggunakan AES-256-GCM. Hasil pengujian memperlihatkan bahwa data yang tersimpan di dalam basis data berbentuk ciphertext yang tidak dapat dibaca secara langsung. Perubahan ini membuktikan bahwa mekanisme enkripsi berhasil menjaga kerahasiaan data sensitif, sehingga meskipun terjadi kebocoran basis data, informasi pelanggan tetap terlindungi.

Tabel 4 Hasil Pengujian Integritas Data Terenkripsi

No	Skenario Pengujian	Kondisi Data	Hasil Dekripsi	Status
1	Data asli terenkripsi	Ciphertext + AuthTag valid	Berhasil	Valid
2	Ciphertext dimodifikasi	1 byte ciphertext diubah	Gagal	Tidak Valid
3	AuthTag dimodifikasi	1 byte AuthTag diubah	Gagal	Tidak Valid
4	IV dimodifikasi	IV diubah	Gagal	Tidak Valid
5	Kunci salah	Key tidak sesuai	Gagal	Tidak Valid

Tabel 4 menyajikan hasil pengujian integritas data terenkripsi menggunakan algoritma AES-256-GCM. Pengujian dilakukan dengan mensimulasikan berbagai skenario manipulasi data, termasuk perubahan *ciphertext*, *authentication tag*, *initialization vector* (IV), serta penggunaan kunci yang tidak sesuai. Hasil pengujian menunjukkan bahwa proses dekripsi hanya berhasil apabila seluruh komponen data (ciphertext, IV, dan authentication tag) berada dalam kondisi valid. Setiap bentuk modifikasi menyebabkan kegagalan dekripsi, yang menegaskan bahwa mekanisme authenticated encryption pada AES-256-GCM mampu mendeteksi manipulasi data secara efektif dan menjamin integritas informasi.

Selain itu, pengujian integritas dilakukan dengan memodifikasi ciphertext secara langsung pada basis data. Hasilnya, proses dekripsi gagal karena authentication tag tidak valid. Temuan ini membuktikan bahwa mekanisme authenticated encryption pada AES-256-GCM mampu mendeteksi manipulasi data secara efektif. Dengan demikian, sistem tidak hanya melindungi data dari kebocoran tetapi juga mencegah penggunaan data yang telah dimodifikasi.

Dari perspektif keamanan, implementasi ini secara signifikan mengurangi risiko yang ditimbulkan oleh SQL Injection dan insider threat. Meskipun penyerang berhasil mengeksekusi query berbahaya atau memperoleh akses administratif, data sensitif tetap terlindungi dalam bentuk terenkripsi. Pendekatan enkripsi tingkat kolom juga memberikan fleksibilitas dan efisiensi dibandingkan enkripsi penuh basis data.

Kesimpulan

Penelitian ini berhasil mengimplementasikan algoritma AES-256-GCM sebagai mekanisme perlindungan data pelanggan sensitif dalam basis data MySQL. Hasil penelitian menunjukkan bahwa pendekatan enkripsi terautentikasi mampu menjamin kerahasiaan dan integritas data secara simultan. Sistem yang diusulkan efektif dalam mendeteksi manipulasi data serta melindungi informasi sensitif dari ancaman eksternal dan internal. Dengan demikian, AES-256-GCM dapat direkomendasikan sebagai solusi kriptografi yang andal untuk pengamanan data at rest pada aplikasi web multi-user berbasis SQL.

Daftar Rujukan

[1] A. Kashyap and A. Jana, "A survey: on detection and prevention techniques of SQL injection attacks," *International Journal of Information and Computer Security*, vol. 26, no. 4, pp. 332–371, 2025, doi: 10.1504/IJICS.2025.146528.

[2] R. A. A. Busaeed et al., "Taxonomy of SQL Injection: ML Trends & Open Challenges," in *Proc. 8th International Conference on Software Engineering and Computer Systems (ICSECS)*, 2023, pp. 382–387, doi: 10.1109/ICSECS58457.2023.10256276.

[3] M. McGiffen, *Pro Encryption in SQL Server 2022: Provide the Highest Level of Protection for Your Data*. Apress, 2022, doi: 10.1007/978-1-4842-8664-7.

[4] M. Costa et al., "Database Encryption Performance Impact on PostgreSQL and MongoDB," in *Computational Science and Its Applications – ICCSA 2022*, Springer, 2022, pp. 123-135, doi: 10.1007/978-981-16-9268-0_10.

[5] S. Ammagunta et al., "Defending Against SQL Injection: Practical Application With Open-Source Tools for Improved Cyber Security," *AIP Conference Proceedings*, 2025, doi: 10.1063/5.0260769.

[6] B. A. Prasetiya, Susanti, dan I. A. Saputro, "Perbandingan Kinerja dan Keamanan Algoritma Kriptografi Modern AES-GCM dengan ChaCha20-Poly1305," *Infomatek*, vol. 26, no. 2, pp. 253-264, 2024.

[7] M. Patria, "Analisis Komparatif Performa AES-GCM dan ChaCha20-Poly1305 dalam Enkripsi Dokumen PDF Berbasis AEAD," *Arcitech*, vol. 5, no. 1, pp. 12-24, 2025.

[8] F. R. Maulana, I. G. P. S. Wijaya, dan F. Bimantoro, "Analisis Keamanan dan Kecepatan Transmisi Data pada Aplikasi Web Berbasis API," *JTIIK*, vol. 12, no. 4, pp. 1045-1054, 2025.

[9] R. S. Perdana dan A. Bhawiyuga, "Analisis Performa Authenticated Encryption pada Arsitektur Microservices berbasis Cloud," *J-PTIIK*, vol. 9, no. 3, pp. 1205-1214, 2025.

[10] S. Ramadhan, "Mitigasi Serangan Data Tampering pada Database SQL menggunakan Algoritma Kriptografi Modern," *Jurnal Keamanan Siber Indonesia*, vol. 4, no. 2, pp. 88-97, 2025.

[11] N. T. Jehian, D. Kiswanto, M. R. A. Fitra, dan H. V. Evanthe, "Pengembangan Sistem Keamanan Data Berbasis Web Menggunakan Kombinasi Algoritma ChaCha20-Poly1305 dan Argon2," *JITET*, vol. 13, no. 3S1, 2025.

[12] H. Kurniawan, "Optimasi Enkripsi Kolom pada MySQL menggunakan AES-GCM untuk Aplikasi E-Commerce," *Jurnal Sistem Informasi*, vol. 16, no. 1, pp. 44-53, 2024.

[13] L. Arianto dan M. T. Anwar, "Implementasi Argon2 dan AES-GCM pada Sistem Otentikasi Terpusat," *Jurnal Komputasi Terapan*, vol. 10, no. 1, pp. 12-25, 2025.

[14] Wijaya dan T. Sutrisno, "Security Enhancement of Server-Side Encryption Using AES-256-GCM in Cloud Database Systems," *IJCSDF*, vol. 14, no. 1, pp. 88-101, 2025.

[15] J. Setiaji, "Efisiensi Penyimpanan Data Terenkripsi pada Sistem Manajemen Basis Data Relasional: Studi Kasus MySQL 8.0," *Jurnal Riset Teknologi Informasi*, vol. 11, no. 1, pp. 102-115, 2026.