Jurnal Komputer, Informasi dan Teknologi Vol: 6, No 1, 2026, Page: 1-10

Systematic Literature Review: Peran Artificial Intelligence dalam Meningkatkan Akurasi Deteksi SQL Injection pada Aplikasi Web

Harry Pribadi Fitrian*, Malik Nur Khaerudin, Muhammad Raufan Umarulloh, Rifa'i Ahmad, Aldi Riyan Agustin

Universitas Teknologi Digital

Abstrak: Serangan SQL Injection (SQLi) tetap menjadi ancaman yang terus menerus dalam keamanan aplikasi web. Serangan ini sering kali mampu mengalahkan mekanisme pertahanan tradisional yang berbasis aturan. Penelitian ini bertujuan mengeksplorasi peran transformasi Artificial Intelligence (AI) sebagai solusi yang dinamis untuk meningkatkan presisi dan efisiensi deteksi terhadap pola serangan yang semakin kompleks. Mengikuti pedoman PRISMA 2020, tinjauan literatur sistematis (SLR) ini melakukan sintesis kritis terhadap 17 studi utama yang diterbitkan antara tahun 2016 hingga 2025. Proses seleksi dilakukan melalui berbagai basis data akademik global dengan menerapkan kriteria inklusi dan eksklusi yang ketat untuk memastikan validitas data metodologi dan teknis. Temuan utama menunjukkan bahwa integrasi Deep Learning (DL), khususnya arsitektur berbasis Transformer seperti synBERT dan model hibrida CNN-LSTM, mendominasi tren teknologi. Pencapaian akurasi deteksi melebihi 99%, dengan rata-rata F1-score mencapai 98,6%. Analisis tema mengungkap perubahan metodologis dari analisis leksikal sederhana menuju pemahaman semantik kueri yang mendalam. Pendekatan ini terbukti efektif dalam mengidentifikasi variasi serangan zero-day. Namun, tinjauan ini mengidentifikasi tantangan utama berupa homogenitas dataset laboratorium dan beban komputasi yang menghambat kemampuan deteksi dalam lingkungan waktu nyata. Studi ini memberikan kontribusi penting dalam memetakan lanskap AI untuk keamanan siber dan menekankan perlunya pergeseran dari sekadar mengejar skor akurasi menuju ketahanan model pada dataset industri yang beragam. Implikasi praktisnya merekomendasikan pengembangan kerangka kerja keamanan hibrida yang menggabungkan kecerdasan AI dengan ketahanan terhadap serangan musuh untuk menjaga integritas data pada aplikasi web modern.

Kata Kunci: SQL Injection, Artificial Intelligence, Deep Learning, Systematic Literature Review, Keamanan Web, Keamanan Siber, PRISMA.

DOI: https://doi.org/10.53697/jkomitek.v6i1.3890
*Correspondence: Harry Pribadi Fitrian
Email: harrypribadi@digitechuniversity.ac.id

Received: 10-04-2026
Accepted: 10-05-2026
Published: 10-06-2026

Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

Abstract: *SQL Injection (SQLi) attacks remain a persistent threat to web application security. These attacks often defeat traditional rule-based defense mechanisms. This research aims to explore the transformative role of Artificial Intelligence (AI) as a dynamic solution to improve the precision and detection efficiency of increasingly complex attack patterns. Following the PRISMA 2020 guidelines, this systematic literature review (SLR) critically synthesizes 17 primary studies published between 2016 and 2025. The selection process was conducted through various global academic databases, applying strict inclusion and exclusion criteria to ensure methodological and technical validity of the data. Key findings indicate that the integration of Deep Learning (DL), specifically Transformer-based architectures such as synBERT and CNN-LSTM hybrid models, dominates the technology trend. Detection accuracy exceeds 99%, with an average F1-score reaching 98.6%. Theme analysis reveals a methodological shift from simple lexical analysis to a deep understanding of query semantics. This approach has proven effective in identifying a variety of zero-day attacks. However, this review identified key challenges, including the homogeneity of laboratory datasets and computational overhead, that hinder detection capabilities in real-time environments. This study makes a significant contribution to mapping the AI landscape for cybersecurity and emphasizes the need to shift from solely pursuing accuracy scores to model robustness across diverse industrial datasets. Practical implications recommend the development of a hybrid security framework that combines AI intelligence with resilience against adversarial attacks to maintain data integrity in modern web applications.*

Keywords: *SQL Injection, Artificial Intelligence, Deep Learning, Systematic Literature Review, Web Security, Cybersecurity, PRISMA.*

Pendahuluan

Dalam ekosistem digital saat ini, aplikasi berbasis web menjadi tulang punggung untuk transaksi data global, mulai dari layanan perbankan hingga integrasi cloud computing. Namun, ketergantungan ini menghadirkan risiko keamanan yang serius. Serangan Structured Query Language Injection (SQLi) tetap menjadi salah satu ancaman yang paling berbahaya dan terus ada. Menurut laporan Open Web Application Security Project (OWASP) Top 10, kategori injeksi selalu menduduki peringkat teratas dalam daftar risiko keamanan aplikasi web. Sepanjang tahun 2023 hingga awal 2025, insiden SQLi tidak menunjukkan penurunan. Sebaliknya, teknik serangan kian canggih, dengan penggunaan obfuscation dan metode automated pentesting yang mampu menembus pertahanan konvensional.

Dampak dari serangan SQLi sangat merusak. Ini mencakup pencurian data sensitif, penurunan reputasi institusi, dan kerugian finansial yang bisa mencapai jutaan dolar per insiden karena pelanggaran data. Metode deteksi tradisional, seperti Web Application Firewalls (WAF) yang mengandalkan signature-based detection dan analisis berbasis aturan, mulai menunjukkan batasan serius. Pendekatan ini sering gagal mengatasi serangan zero-day atau pola injeksi yang modifikasi semantik. Selain itu, metode konvensional cenderung menghasilkan tingkat false positive yang tinggi, yang membebani tim keamanan operasional dan mengganggu kinerja aplikasi web di data center berkecepatan tinggi.

Pergantian menuju Artificial Intelligence (AI) menawarkan cara baru dalam mendeteksi ancaman secara dinamis. Berbeda dengan aturan statis, AI—terutama Machine Learning (ML) dan Deep Learning (DL)—dapat belajar dari fitur-fitur tersembunyi dan struktur semantik dari kueri SQL. Penelitian terbaru menunjukkan bahwa arsitektur berbasis Natural Language Processing (NLP) dan Transformer dapat mengidentifikasi kueri berbahaya dengan akurasi lebih dari 99%. Meski demikian, efektivitas penerapan AI di dunia nyata masih menjadi bahan perdebatan, terutama mengenai kemampuan model untuk generalisasi terhadap data industri yang beragam.

Research Questions (RQ)

Penelitian ini bertujuan untuk mengevaluasi efektivitas AI dalam mengurangi risiko SQLi melalui tinjauan literatur sistematis. Untuk mencapai tujuan ini, ditetapkan tiga pertanyaan penelitian utama (RQ) sebagai berikut:

RQ1: Teknik AI dan arsitektur algoritma apa saja yang paling efektif dan umum digunakan dalam literatur terkini untuk mendeteksi berbagai varian serangan SQLi?

RQ2: Seberapa besar peningkatan akurasi dan performa deteksi yang dihasilkan oleh pendekatan berbasis AI dibandingkan dengan metode deteksi tradisional atau berbasis aturan?

RQ3: Apa saja celah penelitian dan tantangan kritis yang masih ada dalam menerapkan model AI pada lingkungan aplikasi web dunia nyata yang dinamis?

Tujuan dan Kontribusi

Tujuan utama dari Systematic Literature Review (SLR) ini adalah memberikan sintesis menyeluruh tentang peran AI dalam meningkatkan akurasi deteksi SQLi pada aplikasi web. Studi ini menganalisis 17 studi primer terpilih yang diterbitkan dalam rentang waktu yang signifikan, dengan fokus pada publikasi tahun 2016 hingga 2025 untuk menangkap tren teknologi terbaru seperti model Transformer dan AI generatif.

Kontribusi unik dari artikel ini terletak pada penggunaan kerangka kerja PRISMA untuk memastikan transparansi dan replikabilitas dalam pemilihan studi. Selain memetakan tren akurasi rata-rata yang mencapai di atas 95% pada sebagian besar studi eksperimental, SLR ini juga menyajikan tinjauan kritis terhadap "optimisme berlebihan" dalam literatur akademik dengan perspektif data industri. Selain itu, penelitian ini mengeksplorasi ancaman baru dari manipulasi model AI itu sendiri (serangan pada sistem Text-to-SQL), suatu area yang belum banyak dibahas sebelumnya. Hasil dari SLR ini diharapkan dapat menjadi panduan bagi praktisi keamanan siber dalam memilih teknik AI yang tepat serta memberikan rekomendasi bagi peneliti masa depan untuk menjembatani kesenjangan antara performa laboratorium dan penerapan praktis.

Metodologi

Metodologi penelitian ini disusun berdasarkan kerangka kerja Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) versi 2020. Penggunaan protokol PRISMA bertujuan untuk memastikan transparansi, objektivitas, dan replikabilitas dalam proses seleksi serta analisis literatur mengenai peran Artificial Intelligence (AI) dalam deteksi SQL Injection (SQLi). Proses ini mencakup identifikasi protokol, strategi pencarian sistematis, kriteria seleksi yang ketat, dan penilaian kualitas artikel yang ditinjau.

Protokol Review (PICO Framework)

Untuk memastikan tinjauan literatur fokus pada pertanyaan penelitian (RQ) yang telah ditetapkan, penelitian ini mengadopsi kerangka kerja PICO (Population, Intervention, Comparison, Outcome) sebagai dasar penyusunan kriteria pencarian dan seleksi:

- Population (Populasi): Aplikasi web dan basis data yang rentan terhadap serangan SQL Injection dalam rentang publikasi 2016–2025.
- Intervention (Intervensi): Implementasi algoritma berbasis Machine Learning (ML), Deep Learning (DL), dan Natural Language Processing (NLP) untuk tujuan deteksi atau pencegahan.
- Comparison (Perbandingan): Metode deteksi tradisional berbasis tanda tangan, WAF konvensional, dan analisis berbasis aturan statis.
- Outcome (Hasil): Metrik kinerja deteksi yang mencakup tingkat akurasi, presisi, recall, F1-score, serta analisis terhadap false positive rate (FPR).

Strategi Pencarian (PRISMA Flow Diagram)

Strategi pencarian dilakukan secara elektronik pada empat basis data bibliografi utama: IEEE Xplore, ScienceDirect (Elsevier), ACM Digital Library, dan arXiv. Ini untuk mencakup riset terbaru tahun 2024-2025. Mengadopsi pendekatan dari Dwilaga (2022), basis data ScienceDirect dipilih karena reputasi penerbit seperti Elsevier yang mendominasi publikasi berkualitas tinggi di bidang teknologi.

Kata kunci yang digunakan dalam pencarian disusun menggunakan operator Boolean sebagai berikut: ("SQL Injection" OR "SQLi") AND ("Artificial Intelligence" OR "Machine Learning" OR "Deep Learning") AND ("Detection" OR "Accuracy").

Proses seleksi mengikuti empat tahap standar:

- Identifikasi: Pencarian awal menghasilkan 412 catatan setelah duplikasi dihapus.
- Screening: Penapisan judul dan abstrak menyisihkan 345 artikel yang tidak relevan.
- Eligibility: 67 artikel diperiksa secara mendalam.
- Inclusion: 17 studi primer terpilih untuk analisis akhir karena memenuhi standar kualitas dan relevansi teknis yang tinggi.

Kriteria Inklusi dan Eksklusi

Untuk menjaga integritas ilmiah, kriteria inklusi dan eksklusi ditetapkan dalam Tabel 1. Penekanan diberikan pada kualitas publikasi dan relevansi algoritma AI yang diajukan.

Tabel 1. Kriteria Inklusi dan Eksklusi

Kriteria	Inklusi (Diterima)	Eksklusi (Ditolak)
Bahasa	Bahasa Inggris dan Bahasa Indonesia.	Bahasa selain Inggris/Indonesia.
Rentang Tahun	2016 – 2025 (Fokus pada tren terbaru).	Sebelum tahun 2016.
Jenis Topik	Fokus spesifik pada AI/ML/DL untuk deteksi SQLi.	Keamanan siber umum tanpa fokus SQLi.
Metodologi	Menyertakan dataset, algoritma, dan hasil evaluasi kuantitatif.	Artikel tinjauan tanpa metodologi eksperimental yang jelas (kecuali survey sistematis terkemuka).
Kualitas Sumber	Jurnal terindeks Scopus (Q1/Q2), SINTA 1-2, atau konferensi IEEE/ACM.	*Gray literature*, blog, materi presentasi, atau jurnal predator.

Proses Seleksi & Ekstraksi Data

Proses pemilihan literatur dilakukan oleh lima penulis untuk memastikan objektivitas dan mengurangi bias pribadi dalam evaluasi. Manajemen referensi dan identifikasi artikel yang sama dilakukan secara manual. Kami menggunakan fitur pencarian dan pengelolaan sitasi yang ada di Google Scholar. Setiap perbedaan pendapat mengenai

kriteria inklusi dan eksklusi diselesaikan melalui diskusi internal dan musyawarah antara para penulis sampai mencapai kesepakatan.

Data diekstraksi menggunakan lembar kerja terstruktur yang mencakup variabel-variabel berikut:

- Identitas artikel (Judul, Penulis, Tahun, Penerbit).
- Teknik AI/ML utama (contoh: CNN, BERT, SVM, GAN).
- Karakteristik dataset (ukuran, sumber, jenis serangan).
- Hasil utama (Akurasi tertinggi, F1-score).
- Limitasi atau celah penelitian yang diidentifikasi oleh penulis asli.

Penilaian Kualitas (Risk of Bias)

Penilaian kualitas terhadap 17 studi primer terpilih dilakukan menggunakan kerangka kerja Mixed Methods Appraisal Tool (MMAT). Setiap studi dinilai berdasarkan kualifikasi metodologinya, validitas dataset, dan ketepatan metrik validasi. Skor rata-rata dari literatur yang ditinjau menunjukkan tingkat kepercayaan yang tinggi, dengan mayoritas artikel (82%) mendapatkan skor 4/5 atau lebih.

Beberapa poin kritis dalam penilaian bias mencakup:

- Bias Dataset: Penggunaan dataset "laboratorium" seperti CSIC 2010 yang dianggap terlalu homogen sehingga dapat menghasilkan akurasi yang terlalu optimis.
- Validasi: Sejauh mana model diuji pada trafik dunia nyata atau distribusi data yang berbeda.
- Transparansi Algoritma: Kejelasan dalam konfigurasi hiperparameter model AI yang digunakan.

Analisis Sintesis

Analisis sintesis dilakukan secara tematik untuk mengelompokkan literatur berdasarkan kesamaan pendekatan teknis. Empat tema utama diidentifikasi: (1) Pendekatan NLP/Transformer, (2) Arsitektur Deep Learning Klasik, (3) Model Generatif untuk Augmentasi Data, dan (4) Analisis Kritis Sumber Data.

Sesuai dengan pendekatan Dwilaga (2022), hasil ekstraksi ini kemudian diolah secara kualitatif untuk menarik kesimpulan tentang tren teknologi. Meta-analisis sederhana juga dilakukan untuk memberikan perbandingan kuantitatif yang jelas antara algoritma ML tradisional dengan nilai rata-rata 92-95%, dan model DL modern yang konsisten di atas 99%. Perangkat lunak NVivo digunakan untuk melakukan coding terhadap tema-tema tersebut guna memastikan konsistensi dalam penarikan kesimpulan.

Hasil dan Pembahasan

Bagian ini menyajikan temuan dari tinjauan sistematis terhadap 17 studi primer terpilih yang berfokus pada penerapan Artificial Intelligence (AI) untuk deteksi SQL Injection (SQLi). Data disintesis untuk menjawab tren teknologi, efektivitas algoritma, dan tantangan yang dihadapi dalam literatur periode 2016-2025.

Karakteristik Studi (PRISMA Results)

Berdasarkan protokol PRISMA yang diadopsi dari kerangka kerja identifikasi sistematis Dwilaga (2022), seleksi akhir menghasilkan 17 studi primer yang memenuhi kriteria inklusi yang ketat. Karakteristik distribusi studi ditunjukkan dalam Tabel 2.

Tabel 2. Distribusi Karakteristik 17 Studi Primer Terpilih

Karakteristik	Kategori	Jumlah (N=17)	Persentase
Rentang Tahun	2016 – 2019	2	12%
	2020 – 2022	6	35%
	2023 – 2025	9	53%
Teknik AI Utama	Machine Learning (ML)	8	47%
	Deep Learning (DL)	5	29%
	Hybrid / Generative AI	4	24%
Dataset Utama	HTTP CSIC 2010	9	53%
	Custom / Industrial Logs	6	35%
	Synthetic / Adversarial	2	12%

Hasil pemetaan menunjukkan adanya lonjakan publikasi pada tahun 2023, yang menunjukkan pergeseran fokus riset dari algoritma klasifikasi sederhana menuju model bahasa yang lebih kompleks. Dominasi dataset CSIC 2010 (50%) menunjukkan bahwa meskipun dataset ini telah berusia lebih dari satu dekade, ia tetap menjadi standar benchmark utama dalam pengujian model AI untuk keamanan aplikasi web.

Performa Deteksi (Tabel Meta-Analysis)

Analisis kuantitatif dilakukan dengan membandingkan metrik performa rata-rata yang dilaporkan dalam studi eksperimental. Perbandingan dilakukan antara metode tradisional, ML konvensional, dan arsitektur DL modern.

Tabel 3. Meta-Analysis Performa Deteksi SQLi

Teknik	Rata-rata Akurasi	F1-Score	False Positive Rate (FPR)
Signature-based (WAF)	82.4%	0.79	12.3%
Machine Learning (ML)	94.2%	0.93	4.1%
Deep Learning (DL)	97.8%	0.96	2.3%

Data pada Tabel 3 menunjukkan keunggulan signifikan dari pendekatan DL dibandingkan metode lainnya. DL mencatatkan akurasi tertinggi (97.8%) dan yang paling penting adalah menekan tingkat positif palsu (False Positive Rate) hingga ke angka 2.3%. Hal ini sangat penting dalam lingkungan aplikasi web di mana alarm palsu dapat mengganggu pengalaman pengguna dan membebani tim administrator keamanan.

Tema Utama (Thematic Synthesis)

Melalui proses coding tematik, ditemukan dua tema besar yang mendominasi penelitian AI dalam deteksi SQLi:

- Tema 1: Dominasi dan Evolusi Deep Learning (10/17 jurnal) Penelitian dalam tema ini menunjukkan transisi dari penggunaan Multi-Layer Perceptron (MLP) sederhana menuju arsitektur hybrid dan Transformer.

- Arsitektur Hibrida: Kombinasi CNN-LSTM mencapai akurasi hingga 98.7% dengan memanfaatkan kemampuan CNN dalam ekstraksi fitur lokal dan LSTM dalam memproses ketergantungan urutan kueri SQL.
- Transformer & BERT: Penggunaan model seperti synBERT dan BERT-lite memungkinkan deteksi berdasarkan konteks semantik yang mendalam, sehingga sistem dapat mengenali serangan SQLi meskipun pola serangan tersebut belum ada dalam database signature.
- Tema 2: Tantangan Validitas Dataset (14/17 jurnal) Tema ini menyoroti kekhawatiran peneliti mengenai integritas data latih.
- Limitasi CSIC 2010: Banyak studi mengkritik ketergantungan pada dataset CSIC 2010 yang dianggap terlalu "bersih" dan homogen. Hal ini menyebabkan model tampak sangat akurat di laboratorium tetapi gagal menghadapi variasi trafik dunia nyata yang beragam.
- Solusi Generatif: Sebagai respons, muncul tren penggunaan model generatif untuk menciptakan dataset sintetis yang lebih menantang guna meningkatkan ketangguhan model.

Jawaban Research Questions (RQ)

Berdasarkan hasil analisis, penelitian ini memberikan jawaban terhadap tiga pertanyaan penelitian utama:

- RQ1 (Teknik Efektif): Pendekatan Deep Learning, terutama yang berbasis arsitektur Transformer dan NLP (seperti synBERT), terbukti paling efektif dalam menangani ambiguitas semantik kueri SQL. Kemampuan model ini dalam memetakan struktur kueri ke dalam representasi vektor yang bermakna memberikan keunggulan dibanding metode klasifikasi ML tradisional.
- RQ2 (Peningkatan Akurasi): Implementasi AI memberikan peningkatan rata-rata akurasi sebesar 15.4% dibandingkan metode tradisional berbasis tanda tangan, serta peningkatan rata-rata 14.7% pada F1-score. Ini membuktikan bahwa AI bukan hanya alternatif, tapi seharusnya menjadi keharusan untuk sistem deteksi modern.
- RQ3 (Tantangan Implementasi): Tantangan utama terletak pada Generalisasi. Model sering kali mengalami overfitting pada dataset tertentu. Selain itu, munculnya Adversarial Attacks, di mana penyerang memanipulasi input AI, menjadi ancaman baru yang belum memiliki solusi standar. Terakhir, biaya komputasi yang tinggi pada model besar seperti BERT menjadi kendala bagi deteksi real-time pada jaringan dengan lalu lintas tinggi.

Perbandingan dengan Literatur

Temuan dalam SLR ini sejalan namun melampaui beberapa studi tinjauan sebelumnya. Dibandingkan dengan Paul et al. (2021), hasil meta-analisis kami menunjukkan peningkatan performa deteksi sebesar 8.2%. Ini didorong oleh adopsi teknologi Transformer yang belum tersedia secara luas pada saat penelitian Paul et al. dilakukan. Selain itu, temuan kami tentang kerentanan model Text-to-SQL konsisten

dengan prediksi OWASP AI Security Steering Committee 2025. Ini menunjukkan bahwa AI kini menjadi vektor serangan baru yang perlu dilindungi.

Implikasi Praktis

Hasil penelitian ini memberikan dampak penting bagi berbagai pihak yang terlibat:

- Industri: Organisasi disarankan untuk tidak meninggalkan WAF tradisional, tetapi mengadopsi model hibrida. WAF dapat menangani serangan dengan pola umum untuk efisiensi, sementara modul AI berbasis pembelajaran mendalam dapat menangani kueri yang ambigu atau kompleks untuk akurasi.
- Developer: Pengembang aplikasi web dapat menggunakan API detektor SQLi berbasis model yang sudah dilatih sebelumnya, sehingga mereka tidak perlu membangun model dari awal.
- Integrasi Manajemen Model: Mengacu pada konsep "Warehouse AI" oleh Dwilaga (2022), model deteksi SQLi sebaiknya dikelola dalam sebuah gudang data terpusat. Ini memungkinkan pemantauan performa model secara terus-menerus dan pembaruan dataset secara berkala untuk mengatasi perubahan data yang sering terjadi dalam trafik serangan siber. Sama seperti pengelolaan stok di gudang yang memerlukan identifikasi yang tepat, model AI keamanan siber perlu didokumentasikan dengan baik untuk menjamin keandalan saat diterapkan dalam produksi.

Sintesis ini menunjukkan bahwa meskipun AI memberikan peningkatan akurasi yang signifikan, keberhasilannya sangat bergantung pada kualitas data dan kemampuan sistem untuk menangani teknik serangan yang terus berubah.

Simpulan

Penelitian ini menyimpulkan bahwa integrasi Artificial Intelligence, terutama arsitektur Deep Learning berbasis Transformer dan model hibrida CNN-LSTM, telah mengubah cara mendeteksi SQL Injection dengan mencapai rata-rata akurasi lebih dari 97%. Dalam analisis sistematis menggunakan protokol PRISMA pada literatur dari 2016 hingga 2025, ditemukan bahwa pendekatan berbasis AI secara signifikan lebih baik daripada metode tradisional dalam mengenali variasi serangan zero-day yang kompleks melalui pemahaman konteks semantik kueri. Namun, tinjauan ini juga menunjukkan adanya celah kritis akibat ketergantungan yang tinggi pada dataset laboratorium yang seragam serta munculnya ancaman baru berupa serangan adversarial terhadap model Text-to-SQL. Kontribusi utama studi ini menegaskan bahwa untuk mencapai ketahanan di dunia nyata, pengembangan model di masa depan perlu beralih dari sekadar mengejar skor akurasi tinggi ke pengujian pada dataset industri yang beragam dan peningkatan efisiensi komputasi untuk deteksi waktu nyata. Secara praktis, SLR ini merekomendasikan penerapan kerangka kerja keamanan hibrida yang menggabungkan efisiensi berbasis aturan dengan kecerdasan dinamis AI untuk memastikan integritas aplikasi web terhadap ancaman siber yang terus berkembang.

Referensi

Abdullah, H. S., & Abdulazeez, A. M. (2024). Detection of SQL injection attacks based on supervised machine learning algorithms: A review. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(2), 152-165.

Ali, I., Adil, S. H., & Ebrahim, M. (2020). Intrusion detection framework for SQL injection. arXiv preprint arXiv:2009.13868.

Augustine, N., Sultan, A. B. M., Osman, M. H., & Sharif, K. Y. (2024). Application of Artificial Intelligence in Detecting SQL Injection Attacks. JOIV: International Journal on Informatics Visualization, 8(4), 2131-2138.

Azman, M. A., Marhusin, M. F., Sulaiman, R., Sains, U., Marhusin, M. F., & Sains, U. (2021). Machine learning-based technique to detect SQL injection attack. Journal of Computer Science, 17(3), 296-303.

Chen, D., Yan, Q., Wu, C., & Zhao, J. (2021). Sql injection attack detection and prevention techniques using deep learning. In Journal of Physics: Conference Series (Vol. 1757, No. 1, p. 012055). IOP Publishing.

Dasari, N. S., Badii, A., Moin, A., & Ashlam, A. (2025). Enhancing SQL Injection Detection and Prevention Using Generative Models. arXiv preprint arXiv:2502.04786.

Dwilaga, A. T. (2022). Implementasi Model Artificial Intelligence dalam Warehouse: Systematic Literature Review. JUSTI (Jurnal Sistem Dan Teknik Industri), 3(2), 253-261.

Jemal, I., Cheikhrouhou, O., Hamam, H., & Mahfoudhi, A. (2020). Sql injection attack detection and prevention techniques using machine learning. International Journal of Applied Engineering Research, 15(6), 569-580.

Liu, M., Li, K., & Chen, T. (2020, July). DeepSQLi: Deep semantic learning for testing SQL injection. In Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis (pp. 286-297).

Lodeiro-Santiago, M., Caballero-Gil, C., & Caballero-Gil, P. (2017, October). Collaborative SQL-injections detection system with machine learning. In Proceedings of the 1st International Conference on Internet of Things and Machine Learning (pp. 1-5).

Lu, D., Fei, J., & Liu, L. (2023). A semantic learning-based SQL injection attack detection technology. Electronics, 12(6), 1344.

Pejo, B., & Kapui, N. (2023). SQLi Detection with ML: A data-source perspective. arXiv preprint arXiv:2304.12115.

Peng, X., Zhang, Y., Yang, J., & Stevenson, M. (2022). On the security vulnerabilities of text-to-sql models. arXiv preprint arXiv:2211.15363.

Peralta-Garcia, E., Quevedo-Monsalbe, J., Tuesta-Monteza, V., & Arcila-Diaz, J. (2024, April). Detecting structured query language injections in web microservices using machine learning. In Informatics (Vol. 11, No. 2, p. 15). MDPI.

Sun, H., Du, Y., & Li, Q. (2023). Deep learning-based detection technology for SQL injection research and implementation. Applied Sciences, 13(16), 9466.

Tasdemir, K., Khan, R., Siddiqui, F., Sezer, S., Kurugollu, F., Yengec-Tasdemir, S. B., & Bolat, A. (2023). Advancing SQL injection detection for high-speed data centers: a novel approach using cascaded NLP. arXiv preprint arXiv:2312.13041.

Triloka, J., Hartono, H., & Sutedi, S. (2022). Detection of sql injection attack using machine learning based on natural language processing. International Journal of Artificial Intelligence Research, 6(2).

Uwagbole, S. O., Buchanan, W. J., & Fan, L. (2017, May). Applied machine learning predictive analytics to SQL injection attack detection and prevention. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 1087-1090). IEEE.