Prosiding Seminar Nasional Keguruan dan Pendidikan
Universitas Muhammadiyah Muara Bungo
Volume (4) Agustus 2026
https://ejournal.ummuba.ac.id/index.php/SNKP/hm
e-ISSN: 3109-6166

Tinjauan Literatur: Integrasi Deep Learning Dan Algoritma Berbasis Isolasi Pada Deteksi Anomali Query SQL

Literature Review: Integration of Deep Learning and Isolation-Based Algorithms in SQL Query Anomaly Detection

Raka Maulana Bintang[1], Tining Haryanti[2], Muhamad Amirul Haq[3]
[1] Universitas Muhammadiyah Surabaya
Corresponding author: rakamaulana.2005@gmail.com

ABSTRAK

Keamanan database SQL menghadapi ancaman siber yang semakin dinamis, seperti SQL Injection, penyalahgunaan hak akses, dan serangan zero-day yang sulit dideteksi menggunakan sistem berbasis tanda tangan (signature-based detection). Berbagai penelitian telah mengembangkan metode deteksi anomali berbasis Deep Learning dan algoritma berbasis isolasi untuk meningkatkan adaptivitas sistem keamanan database. Literature review ini bertujuan menganalisis perkembangan metode, efektivitas algoritma, serta tren integrasi Deep Learning dan algoritma berbasis isolasi dalam deteksi anomali query SQL. Metode yang digunakan adalah systematic literature review terhadap artikel terindeks periode 2022–2026 yang dianalisis berdasarkan metode, objek penelitian, serta keterbatasan pendekatan yang digunakan. Hasil tinjauan menunjukkan bahwa Isolation Forest unggul dalam efisiensi dan deteksi unsupervised, namun masih terbatas dalam menangkap pola query yang memiliki hubungan fitur non-linear. Sebaliknya, model Deep Learning seperti CNN dan LSTM mampu melakukan ekstraksi fitur sintaksis secara otomatis, meskipun membutuhkan sumber daya komputasi yang lebih besar. Tren penelitian menunjukkan adanya pergeseran menuju model hibrida yang menggabungkan kemampuan representasi fitur dan mekanisme isolasi data. Tinjauan ini menyimpulkan bahwa integrasi kedua pendekatan memiliki potensi dalam membangun sistem deteksi anomali query SQL yang lebih adaptif dan efisien.

Kata Kunci: Deep Learning, Isolation Forest, Query SQL, Deteksi Anomali, Tinjauan Literatur

Korespondensi: Raka Maulana Bintang. Universitas Muhammadiyah Surabaya. Jalan Raya Sutorejo No.59, Surabaya. Email: rakamaulana.2005@gmail.com Mobile: 0881027795533

LATAR BELAKANG

Keamanan basis data (database security) menjadi salah satu aspek penting dalam sistem informasi modern karena database SQL digunakan secara luas pada sektor perbankan, kesehatan, pendidikan, pemerintahan, hingga e-commerce untuk menyimpan dan mengelola data yang bersifat sensitif. Peningkatan penggunaan aplikasi berbasis web menyebabkan database semakin rentan terhadap berbagai ancaman siber seperti SQL Injection (SQLi), penyalahgunaan hak akses (insider threat), serta serangan zero-day yang terus berkembang. Pendekatan keamanan tradisional seperti firewall, validasi input, dan sistem deteksi berbasis tanda tangan (signature-based detection) masih memiliki keterbatasan karena hanya mampu mengenali pola serangan yang telah diketahui sebelumnya dan kurang adaptif terhadap pola serangan baru yang bersifat dinamis (Crespo-Martínez et al., 2023; Dadiyala et al., 2025).

Sebagai alternatif, pendekatan anomaly detection berkembang sebagai mekanisme keamanan yang berfokus pada identifikasi perilaku yang menyimpang dari pola normal. Dalam konteks database SQL, anomali dapat berupa pola akses tidak biasa, struktur kueri yang mencurigakan, maupun operasi yang tidak sesuai dengan konteks penggunaan sistem. Pendekatan ini dianggap lebih adaptif karena tidak sepenuhnya bergantung pada basis aturan serangan yang telah didefinisikan sebelumnya. Penelitian S. Li et al. (2022) menunjukkan bahwa deteksi anomali berbasis konteks mampu mengenali serangan tersembunyi (stealthy anomaly) dengan mempertimbangkan hubungan semantik antaroperasi database, sehingga lebih efektif dibanding pendekatan yang hanya mengandalkan deviasi statistik sederhana.

Salah satu metode yang banyak digunakan dalam deteksi anomali adalah algoritma berbasis isolasi, khususnya Isolation Forest (iForest). Metode ini bekerja dengan membangun pohon isolasi secara acak, di mana data anomali cenderung terisolasi lebih cepat dibanding data normal. Pendekatan tersebut memiliki keunggulan berupa efisiensi komputasi, kemampuan bekerja pada data berdimensi tinggi, serta sifat unsupervised yang tidak memerlukan data berlabel. Pengembangan terhadap iForest juga terus dilakukan, seperti Deep Isolation Forest (DIF) yang menggabungkan

DOI : https://doi.org/10.52060/snkp.2026.4497

representasi neural network untuk menangani pola anomali kompleks (Xu, Pang, Wang, & Wang, 2023), OptIForest yang mengoptimalkan struktur pohon isolasi (Xiang et al., 2023), serta metode interpretabilitas DIFFI untuk menjelaskan kontribusi fitur dalam proses deteksi anomali (Carletti, Terzi, & Susto, 2023). Meskipun demikian, iForest masih menghadapi keterbatasan dalam mengenali hubungan fitur yang bersifat non-linear dan anomali yang memiliki pola kompleks.

Di sisi lain, perkembangan Deep Learning memberikan pendekatan baru dalam deteksi anomali query SQL melalui kemampuan ekstraksi fitur otomatis dari representasi teks dan struktur sintaksis query. Model seperti CNN, LSTM, BiLSTM, autoencoder, hingga Transformer telah banyak diterapkan untuk mendeteksi SQLi dengan tingkat akurasi yang tinggi. Kakisim (2024) melalui pendekatan multi-view consensus berbasis BiLSTM-CNN memperoleh akurasi hingga 99,96%, sedangkan Lu, Fei, & Liu (2023) menggunakan semantic learning berbasis BERT untuk meningkatkan kemampuan generalisasi terhadap serangan zero-day. Selain itu, X. Li (2025) menunjukkan bahwa integrasi CNN-LSTM dengan optimasi NSGA-II mampu meningkatkan efisiensi komputasi sekaligus mempertahankan performa deteksi query anomali. Walaupun menghasilkan akurasi tinggi, model Deep Learning umumnya memerlukan sumber daya komputasi besar, data pelatihan yang memadai, serta memiliki kompleksitas model yang relatif tinggi.

Perkembangan penelitian terbaru menunjukkan adanya kecenderungan menuju model hibrida yang menggabungkan kemampuan representasi fitur dari Deep Learning dengan mekanisme isolasi data pada algoritma berbasis Isolation Forest. Pendekatan tersebut bertujuan memanfaatkan keunggulan masing-masing metode, yaitu kemampuan Deep Learning dalam menangkap pola non-linear dan efisiensi deteksi tanpa supervisi dari metode berbasis isolasi. Penelitian Deep Isolation Forest oleh Xu et al. (2023) menunjukkan bahwa integrasi representasi neural mampu meningkatkan kemampuan Isolation Forest dalam mendeteksi anomali kompleks, sedangkan X. Li (2025) menunjukkan bahwa integrasi CNN-LSTM dengan optimasi NSGA-II mampu mempertahankan akurasi tinggi sekaligus meningkatkan efisiensi komputasi pada deteksi query anomali. Selain itu, pendekatan multi-view dan model hybrid berbasis Deep Learning juga mulai dikembangkan untuk meningkatkan kemampuan generalisasi terhadap variasi serangan SQL (Kakisim, 2024). Meskipun demikian, penelitian terkait integrasi Deep Learning dan algoritma berbasis isolasi masih tersebar pada berbagai domain dan belum banyak dirangkum secara khusus dalam konteks deteksi anomali query SQL maupun keamanan database.

Berdasarkan kondisi tersebut, diperlukan suatu tinjauan literatur yang mampu merangkum perkembangan metode deteksi anomali query SQL secara lebih sistematis, khususnya pada integrasi Deep Learning dan algoritma berbasis isolasi. Kajian sebelumnya masih cenderung berfokus pada evaluasi model machine learning atau SQL injection detection secara umum tanpa secara spesifik membahas hubungan antara representasi Deep Learning dan mekanisme isolasi data dalam keamanan database (Adeyinka Ayodeji Mustapha et al., 2024). Oleh karena itu, penelitian ini melakukan systematic literature review terhadap artikel ilmiah periode 2022–2026 untuk mengidentifikasi perkembangan metode, membandingkan efektivitas pendekatan Deep Learning dan algoritma berbasis isolasi, serta menganalisis tren integrasi keduanya pada deteksi anomali query SQL. Tinjauan ini diharapkan dapat memberikan pemahaman yang lebih terstruktur mengenai arah perkembangan penelitian sekaligus menjadi landasan bagi pengembangan sistem keamanan database yang lebih adaptif dan efisien di masa mendatang.

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan metode Systematic Literature Review (SLR) untuk menganalisis perkembangan metode deteksi anomali query SQL berbasis Deep Learning dan algoritma berbasis isolasi secara sistematis dan terstruktur. Pendekatan SLR dipilih karena memungkinkan identifikasi, evaluasi, dan sintesis hasil penelitian terdahulu secara komprehensif sehingga dapat memberikan gambaran yang objektif mengenai perkembangan topik penelitian(Kitchenham & Charters, 2007). Proses review dilakukan melalui tahapan identifikasi literatur, seleksi artikel, ekstraksi data, serta sintesis hasil penelitian berdasarkan tema dan metode yang digunakan.

DOI : https://doi.org/10.52060/snkp.2026.4497

Prosiding Seminar Nasional Keguruan dan Pendidikan
Universitas Muhammadiyah Muara Bungo
Volume (4) Agustus 2026
https://ejournal.ummuba.ac.id/index.php/SNKP/hm
e-ISSN: 3109-6166

Sampel dan Populasi

Populasi dalam penelitian ini adalah seluruh artikel ilmiah yang membahas deteksi anomali, keamanan database, SQL Injection, Deep Learning, serta algoritma berbasis isolasi pada periode 2022–2026. Sampel penelitian berupa 20 artikel ilmiah yang dipilih menggunakan teknik purposive sampling berdasarkan kriteria inklusi dan eksklusi yang telah ditentukan (Kitchenham & Charters, 2007).

Kriteria inklusi meliputi: (1) artikel diterbitkan pada periode 2022–2026, (2) terindeks Scopus atau jurnal nasional yang relevan, (3) membahas metode deteksi anomali atau keamanan database yang berkaitan dengan query SQL maupun SQL Injection, serta (4) menyediakan informasi metode dan evaluasi performa. Artikel yang tidak relevan dengan keamanan query SQL atau tidak memiliki hasil evaluasi yang jelas dikeluarkan dari proses seleksi.

Pencarian literatur dilakukan melalui basis data Scopus, IEEE Xplore, Springer, ACM Digital Library, dan Google Scholar menggunakan kombinasi kata kunci "SQL injection detection", "query anomaly detection", "deep learning SQL", "database anomaly detection", dan "isolation forest anomaly detection". Artikel yang terpilih kemudian dianalisis berdasarkan metode yang digunakan, metrik performa, kelebihan, keterbatasan, serta arah penelitian selanjutnya.

Hasil Penelitian

1. Karakteristik Literatur yang Ditinjau

Berdasarkan proses pencarian dan seleksi literatur, diperoleh 20 artikel yang memenuhi kriteria inklusi dan dianalisis lebih lanjut. Artikel yang ditinjau dipublikasikan pada periode 2022–2026 dan mayoritas berasal dari jurnal internasional terindeks Scopus. Fokus penelitian didominasi oleh deteksi SQL Injection (SQLi), anomaly detection pada database, serta intrusion detection berbasis machine learning dan deep learning. Sebagian besar penelitian menggunakan dataset publik maupun data simulasi untuk mengevaluasi performa model melalui metrik akurasi, precision, recall, F1-score, dan AUC.

Karakteristik	(N)	(%)
Tahun Publikasi		
2022	3	15
2023	10	50
2024	2	10
2025	4	20
2026	1	5
Indeksasi		
Scopus Q1	11	55
Scopus Q2	4	20
Scopus Q3/Q4	2	10
Nasional/Conference	3	15

Table 1. Karakteristik Literatur yang Ditinjau

Tabel 1 menunjukkan bahwa penelitian terkait deteksi anomali query SQL mengalami peningkatan pada periode 2023–2025, dengan dominasi publikasi pada jurnal Scopus Q1. Hal ini menunjukkan bahwa topik keamanan database dan deteksi anomali menjadi perhatian penting dalam penelitian keamanan siber modern.

2. Klasifikasi Metode Deteksi Anomali

Analisis terhadap 20 artikel menunjukkan bahwa metode yang digunakan dapat diklasifikasikan ke dalam empat kelompok utama, yaitu pendekatan berbasis algoritma isolasi, Deep Learning, model hibrida, serta machine learning klasik.

Pendekatan	(N)	(%)

DOI : https://doi.org/10.52060/snkp.2026.4497

Prosiding Seminar Nasional Keguruan dan Pendidikan
Universitas Muhammadiyah Muara Bungo
Volume (4) Agustus 2026
https://ejournal.ummuba.ac.id/index.php/SNKP/hm
e-ISSN: 3109-6166

Pendekatan	(N)	(%)
Isolatin-Based	3	15
Deep Learning	7	35
Hybrid	8	40
Classical Machine Learning	2	10

Table 2. Distribusi Pendekatan Metode

Pendekatan hibrida merupakan metode yang paling dominan dengan proporsi 40%, diikuti oleh Deep Learning sebesar 35%. Temuan ini menunjukkan bahwa penelitian terbaru cenderung menggabungkan beberapa metode untuk memperoleh performa deteksi yang lebih baik dibandingkan penggunaan model tunggal. Sementara itu, metode berbasis isolasi seperti Isolation Forest tetap digunakan karena memiliki efisiensi komputasi tinggi dan tidak membutuhkan data berlabel.

3. Ringkasan Literatur Yang Ditinjau

Ringkasan artikel yang dianalisis disajikan pada Tabel 3. Tabel ini memuat penulis dan tahun, metode yang digunakan, hasil utama, serta keterbatasan masing-masing penelitian

No	Penulis	Metode	Hasil Utama	Keterbatasan
1	Li (2025)	CNN-LSTM + NSGA-II	Akurasi 99,3%, efisiensi +27%	Kompleksitas tinggi
2	Dadiyala dkk. (2025)	Isolation Forest	Akurasi 85%	Kurang optimal untuk sistem kritis
3	Xu dkk. (2023)	Deep Isolation Forest	AUC hingga 0,99	Komputasi lebih tinggi
4	Carletti dkk. (2023)	DIFFI	Interpretasi 10× lebih cepat dari SHAP	Terbatas pada IF
5	Xiang dkk. (2023)	OptIForest	Unggul pada 17 dataset	Implementasi kompleks
6	Bella dkk. (2024)	Deep Neural Decision Forest	94–98,84%	Sedikit di bawah SOTA
7	Sarhan dkk. (2023)	Zero-Shot Learning	Z-DR realistis	Sensitif distribusi fitur
8	Ahmed dkk. (2025)	Hybrid DT-XGB-CNN	>99%	Biaya komputasi tinggi
9	Demirel dkk. (2023)	ZSL + CNN	TPR 99,29%	Tidak klasifikasi tipe
10	Kakismi (2024)	MVC-BiCNN	99,96%	Kompleksitas tinggi
11	Casmiry dkk. (2026)	Hybrid CNN-LSTM	99,85%	Masih ada FN
12	Lu dkk. (2023)	synBERT	Zero-day 94,35%	Model besar
13	Menaka dkk. (2025)	CNN + RF	95,67%	Di bawah SOTA
14	Alghawazi dkk. (2023)	RNN Autoencoder	94%	Akurasi rendah
15	Sun dkk. (2023)	TextCNN+BiLSTM+BERT	F1 >99,57%	Sangat kompleks
16	Zhang dkk. (2022)	DNN+TF-IDF	96,16%	Di bawah SOTA
17	Triloka dkk. (2022)	SVM+NLP	99,77%	Black-box
18	Crespo-Martinez dkk. (2023)	ML NetFlow	>97%	Deteksi biner
19	Lo dkk. (2025)	Lightweight MHSA	98,98%	Terbatas SQLi
20	Li dkk. (2022)	Trans-DAS	F1 0,896–0,981	False positive

Table 3. Ringkasan Literatur Deteksi Anomali Query SQL

DOI : https://doi.org/10.52060/snkp.2026.4497

4. Perbandingan Performa Metode

Berdasarkan hasil analisis, model Deep Learning hibrida menunjukkan performa paling tinggi dibanding pendekatan lainnya. MVC-BiCNN yang dikembangkan oleh Kakisim (2024) mencapai akurasi 99,96%, sedangkan Hybrid CNN-LSTM dengan Chi-square feature selection memperoleh akurasi 99,85% (Casmiry, Sinde, & Mduma, 2026). Seleain itu, CNN-LSTM dengan optimasi NSGA-II yang dikembangkan X. Li (2025) mampu mempertahankan akurasi 99,3% sekaligus meningkatkan efisiensi komputasi sebesar 27%.

Di sisi lain, model berbasis semantic learning seperti synBERT (Lu et al., 2023) menunjukkan kemampuan generalisasi yang baik terhadap serangan zero-day dengan tingkat keberhasilan mencapai 94,35%. Hal ini menunjukkan bahwa pemanfaatan struktur sintaksis dan semantik query memberikan kontribusi penting terhadap peningkatan performa deteksi.

Sementara itu, pendekatan Isolation Forest konvensional masih memiliki akurasi yang lebih rendah, yaitu sekitar 85% (Dadiyala et al., 2025). Namun, pengembangan seperti Deep Isolation Forest (Xu et al., 2023) berhasil meningkatkan performa hingga AUC 0,99 dengan memanfaatkan representasi neural network.

Dari sisi efisiensi komputasi, model lightweight berbasis self-attention yang dikembangkan Lo, Hwang, & Tai (2025) hanya memiliki 69.269 parameter namun tetap mencapai akurasi 98,98%. Temuan ini menunjukkan bahwa desain arsitektur yang efisien memungkinkan implementasi model deteksi pada edge device maupun lingkungan dengan sumber daya terbatas.

5. Tren Penelitian dan Research Gap

Tren penelitian menunjukkan pergeseran yang jelas dari pendekatan single-model menuju model hibrida. Pada periode 2022–2023, penelitian dominan menggunakan model Deep Learning tunggal seperti CNN, LSTM, DNN, maupun Transformer untuk mendeteksi SQL injection dan anomali database (Lu et al., 2023; Sun, Du, & Li, 2023; Zhang et al., 2022). Memasuki periode 2024–2025, mayoritas penelitian mulai mengombinasikan beberapa teknik guna meningkatkan akurasi, efisiensi, serta kemampuan generalisasi model. Pendekatan tersebut terlihat pada penggunaan hybrid CNN-LSTM dengan optimasi NSGA-II (X. Li, 2025), multi-view consensus berbasis BiLSTM-CNN (Kakisim, 2024), serta pengembangan Deep Isolation Forest yang menggabungkan representasi neural network dengan mekanisme isolasi (Xu et al., 2023). Pergeseran ini menunjukkan bahwa penelitian terkini tidak lagi hanya berfokus pada peningkatan akurasi, tetapi juga pada efisiensi komputasi dan kemampuan deteksi terhadap anomali yang lebih kompleks.

Research gap yang teridentifikasi meliputi: (1) masih terbatasnya penelitian yang secara langsung mengintegrasikan mekanisme isolasi seperti Isolation Forest dengan kemampuan ekstraksi fitur berbasis CNN dalam konteks deteksi anomali akses atau query database SQL; (2) sebagian besar penelitian masih berfokus pada deteksi SQL Injection atau intrusion detection secara umum, sehingga deteksi anomali akses database yang mencakup pola perilaku pengguna, insider threat, dan aktivitas tidak wajar lainnya belum banyak dieksplorasi (Dadiyala et al., 2025; X. Li, 2025); (3) terbatasnya evaluasi menggunakan dataset real-world yang mencerminkan kondisi lingkungan produksi sesungguhnya; serta (4) minimnya penelitian yang mempertimbangkan implementasi model yang efisien dan adaptif untuk deployment pada sistem dengan keterbatasan sumber daya atau kebutuhan deteksi real-time (Lo et al., 2025). Temuan tersebut menunjukkan adanya peluang pengembangan model integratif berbasis CNN dan Isolation Forest untuk membangun sistem deteksi anomali akses database SQL yang lebih adaptif, efisien, dan relevan terhadap kebutuhan keamanan database modern.

PEMBAHASAN

Deep Learning dalam Deteksi Anomali Query SQL

Pendekatan Deep Learning berkembang pesat dalam deteksi anomali dan SQL Injection karena mampu melakukan ekstraksi fitur secara otomatis dari struktur dan representasi query tanpa memerlukan feature engineering manual yang kompleks. Model berbasis CNN, LSTM, BiLSTM, dan Transformer banyak digunakan karena mampu menangkap pola sintaksis maupun hubungan semantik pada query SQL. Penelitian Zhang et al. (2022) melalui Deep Neural Network-Based SQL Injection Detection Method menunjukkan bahwa model DNN dengan TF-IDF dan dropout

DOI : https://doi.org/10.52060/snkp.2026.4497

mencapai akurasi 96,16%, lebih baik dibanding beberapa metode machine learning klasik. Perkembangan selanjutnya ditunjukkan oleh Lu et al. (2023) melalui A Semantic Learning-Based SQL Injection Attack Detection Technology yang menggunakan synBERT berbasis semantic learning dan memperoleh akurasi 99,74% dengan kemampuan generalisasi terhadap serangan zero-day sebesar 94,35%.

Peningkatan performa juga terlihat pada penggunaan model hybrid berbasis Deep Learning. Sun et al. (2023) dalam Deep Learning-Based Detection Technology for SQL Injection Research and Implementation menggabungkan TextCNN, BiLSTM, attention mechanism, dan transfer learning berbasis BERT sehingga menghasilkan F1-score lebih dari 99,57%. Demikian pula Kakisim (2024) melalui pendekatan multi-view consensus berbasis BiLSTM-CNN memperoleh akurasi 99,96% dengan false positive dan false negative yang sangat rendah. Temuan tersebut menunjukkan bahwa Deep Learning memiliki kemampuan tinggi dalam menangkap pola query yang kompleks, termasuk hubungan non-linear dan struktur sintaksis yang sulit dikenali metode tradisional.

Meskipun demikian, tingginya akurasi Deep Learning sering diikuti peningkatan kompleksitas komputasi. Model berbasis BERT atau arsitektur multi-layer membutuhkan sumber daya komputasi besar serta data pelatihan yang memadai. Hal ini menjadi tantangan ketika model akan diterapkan pada sistem real-time atau lingkungan dengan sumber daya terbatas. Lo et al. (2025) mencoba menjawab masalah tersebut melalui lightweight multi-head self-attention dengan jumlah parameter yang jauh lebih kecil namun tetap mencapai akurasi 98,98%. Dengan demikian, tantangan utama Deep Learning bukan hanya meningkatkan akurasi, tetapi juga menjaga efisiensi dan skalabilitas implementasi.

Algoritma Berbasis Isolasi dalam Deteksi Anomali Database

Selain Deep Learning, algoritma berbasis isolasi menjadi pendekatan penting dalam deteksi anomali karena sifatnya yang unsupervised dan efisien secara komputasi. Isolation Forest bekerja dengan prinsip bahwa data anomali lebih mudah terisolasi dibanding data normal melalui pembentukan pohon isolasi secara acak. Dadiyala et al. (2025) melalui Enhancing Security of Databases Through Anomaly Detection in Structured Workloads menunjukkan bahwa Isolation Forest mencapai akurasi 85% dan mengungguli beberapa metode seperti Random Forest, Gradient Boosting, serta One-Class SVM pada beban kerja database terstruktur. Keunggulan utama metode ini terletak pada kesederhanaan implementasi, kemampuan menangani data berdimensi tinggi, serta tidak memerlukan data berlabel.

Pengembangan lebih lanjut dilakukan untuk mengatasi keterbatasan Isolation Forest standar dalam mengenali pola non-linear. Xu et al. (2023) melalui Deep Isolation Forest for Anomaly Detection memperkenalkan Deep Isolation Forest (DIF) yang menggabungkan representasi neural network dengan mekanisme isolasi sehingga memperoleh nilai AUC hingga 0,99 pada berbagai tipe data. Sementara itu, Xiang et al. (2023) melalui OptIForest: Optimal Isolation Forest for Anomaly Detection menunjukkan bahwa optimasi struktur pohon isolasi dapat meningkatkan performa dibanding iForest konvensional. Dari sisi interpretabilitas, Carletti et al. (2023) melalui DIFFI memperlihatkan bahwa feature importance pada Isolation Forest dapat dijelaskan lebih cepat dibanding metode seperti SHAP.

Walaupun memiliki efisiensi tinggi, metode berbasis isolasi tetap memiliki keterbatasan. Isolation Forest standar umumnya melakukan partisi linear sehingga kurang efektif dalam mengenali anomali yang memiliki pola hubungan kompleks atau konteks semantik tertentu. Oleh karena itu, penggunaan Isolation Forest secara tunggal sering menghasilkan performa yang lebih rendah dibanding model Deep Learning modern.

Integrasi CNN dan Isolation Forest sebagai Arah Pengembangan

Hasil literature review menunjukkan bahwa penelitian terbaru bergerak menuju pendekatan hibrida yang mengombinasikan beberapa teknik untuk memperoleh keseimbangan antara akurasi dan efisiensi. X. Li (2025) melalui Optimizing Neural Networks for Anomalous Query Detection in Databases Using the NSGA-II Algorithm menunjukkan bahwa hybrid CNN-LSTM dengan optimasi NSGA-II mampu meningkatkan efisiensi komputasi sebesar 27% tanpa menurunkan performa deteksi. Sementara itu, Xu et al. (2023) membuktikan bahwa integrasi representasi neural network dengan Isolation Forest dapat meningkatkan kemampuan deteksi terhadap anomali kompleks.

Temuan tersebut mendukung gagasan bahwa integrasi CNN dan Isolation Forest memiliki potensi kuat untuk sistem deteksi anomali akses database SQL. CNN mampu berperan sebagai ekstraktor fitur sintaksis dan pola query yang kompleks, sedangkan Isolation Forest berfungsi sebagai mekanisme deteksi anomali yang ringan dan tidak bergantung pada data berlabel. Kombinasi keduanya berpotensi menghasilkan sistem yang tidak hanya akurat, tetapi juga adaptif

DOI : https://doi.org/10.52060/snkp.2026.4497

terhadap pola serangan baru dan efisien untuk implementasi real-time. Oleh karena itu, integrasi CNN dan Isolation Forest menjadi salah satu arah penelitian yang relevan dan masih terbuka untuk dikembangkan lebih lanjut.

KESIPULAN

Berdasarkan hasil Systematic Literature Review terhadap 20 artikel ilmiah periode 2022–2026, dapat disimpulkan bahwa pendekatan Deep Learning dan algoritma berbasis isolasi memiliki karakteristik yang saling melengkapi dalam deteksi anomali query maupun akses database SQL. Model Deep Learning seperti CNN, LSTM, BiLSTM, dan Transformer menunjukkan performa tinggi dalam mengenali pola sintaksis, hubungan non-linear, serta karakteristik serangan yang kompleks, namun memerlukan sumber daya komputasi yang besar dan kompleksitas model yang tinggi. Sebaliknya, algoritma berbasis isolasi seperti Isolation Forest unggul dalam efisiensi komputasi, kemampuan bekerja secara unsupervised, serta implementasi yang relatif sederhana, meskipun masih memiliki keterbatasan dalam memahami hubungan fitur dan konteks semantik yang kompleks.

Hasil tinjauan juga menunjukkan adanya pergeseran tren penelitian dari penggunaan model tunggal menuju pendekatan hibrida yang menggabungkan kemampuan representasi fitur Deep Learning dengan mekanisme deteksi anomali berbasis isolasi. Pendekatan tersebut terbukti mampu meningkatkan akurasi, efisiensi, serta kemampuan generalisasi terhadap berbagai jenis serangan, termasuk zero-day attack.

Meskipun demikian, penelitian yang secara khusus mengintegrasikan CNN dengan Isolation Forest pada konteks deteksi anomali akses maupun query database SQL masih relatif terbatas. Selain itu, penggunaan dataset real-world dan pengembangan model yang adaptif untuk implementasi real-time juga masih menjadi tantangan. Oleh karena itu, integrasi CNN dan Isolation Forest memiliki potensi sebagai arah penelitian selanjutnya untuk membangun sistem deteksi anomali database SQL yang lebih adaptif, efisien, dan relevan terhadap kebutuhan keamanan database modern.

REFERENCES

Adeyinka Ayodeji Mustapha, Anayo Sylvester Udeh, Thomas Anafeh Ashi, Odunayo Sekinat Sobowale, Mayowa Jesse Akinwande, & Aminat Olaide Oteniara. (2024). Comprehensive review of machine learning models for sql injection detection in e-commerce. *World Journal of Advanced Research and Reviews*, *23*(1), 451–465. doi:10.30574/wjarr.2024.23.1.2004

Carletti, M., Terzi, M., & Susto, G. A. (2023). Interpretable Anomaly Detection with DIFFI: Depth-based Isolation Forest Feature Importance. Retrieved from http://arxiv.org/abs/2007.11117

Casmiry, E. N., Sinde, R. S., & Mduma, N. M. (2026). A Hybrid Deep Learning Model for SQL Injection Attack Detection. *IEEE Access*, *14*, 6450–6463. doi:10.1109/access.2026.3651991

Crespo-Martínez, I. S., Campazas-Vega, A., Guerrero-Higueras, Á. M., Riego-DelCastillo, V., Álvarez-Aparicio, C., & Fernández-Llamas, C. (2023). SQL injection attack detection in network flow data. *Computers and Security*, *127*. doi:10.1016/j.cose.2023.103093

Dadiyala, C., Qureshi, F., Bhattad, K. A., Thakur, S., Sheikh, N. T. S., & Singh, K. A. K. (2025). Enhancing Security of Databases through Anomaly Detection in Structured Workloads. *Journal of ICT Research and Applications*, *18*(3), 196–214. doi:10.5614/itbj.ict.res.appl.2025.18.3.2

Kakisim, A. G. (2024). A deep learning approach based on multi-view consensus for SQL injection detection. *International Journal of Information Security*, *23*(2), 1541–1556. doi:10.1007/s10207-023-00791-y

Kitchenham, & Charters. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*.

Li, S., Yin, Q., Li, G., Li, Q., Liu, Z., & Zhu, J. (2022). *Unsupervised Contextual Anomaly Detection for Database Systems*. In *Proceedings of the ACM SIGMOD International Conference on Management of Data* (pp. 788–802). Association for Computing Machinery. doi:10.1145/3514221.3517861

DOI : https://doi.org/10.52060/snkp.2026.4497

Li, X. (2025). Optimizing neural networks for anomalous query detection in databases using the NSGA-II algorithm. *Journal of Engineering and Applied Science*, *72*(1). doi:10.1186/s44147-025-00790-x

Lo, R. T., Hwang, W. J., & Tai, T. M. (2025). SQL Injection Detection Based on Lightweight Multi-Head Self-Attention. *Applied Sciences (Switzerland)*, *15*(2). doi:10.3390/app15020571

Lu, D., Fei, J., & Liu, L. (2023). A Semantic Learning-Based SQL Injection Attack Detection Technology. *Electronics (Switzerland)*, *12*(6). doi:10.3390/electronics12061344

Sun, H., Du, Y., & Li, Q. (2023). Deep Learning-Based Detection Technology for SQL Injection Research and Implementation. *Applied Sciences (Switzerland)*, *13*(16). doi:10.3390/app13169466

Xiang, H., Zhang, X., Hu, H., Qi, L., Dou, W., Dras, M., … Xu, X. (2023). *OptIForest: Optimal Isolation Forest for Anomaly Detection*. Retrieved from https://github.com/xiagll/OptIForest.

Xu, H., Pang, G., Wang, Y., & Wang, Y. (2023). Deep Isolation Forest for Anomaly Detection. doi:10.1109/TKDE.2023.3270293

Zhang, W., Li, Y., Li, X., Shao, M., Mi, Y., Zhang, H., & Zhi, G. (2022). Deep Neural Network-Based SQL Injection Detection Method. *Security and Communication Networks*, *2022*. doi:10.1155/2022/4836289

DOI : https://doi.org/10.52060/snkp.2026.4497