Systematic Literature Review: SQL Injection Detection Vulnerability Using Machine Learning

[1]Agnes Rahayu, [2]Eva Yulyanti, [3]Muhammad Ghalib

[1,2,3] Program Studi Magister Ilmu Komputer Universitas Budi Luhur

Jl. Ciledug Raya No.99, Petukangan Utara, Kec. Pesanggrahan, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12260

E-mail: rahayuagnes.ar@gmail.com[1], evayulyanti02@gmail.com[2], muhammadghalibb18@gmail.com [3]

(Received: Nopember 2024, Revised: Februari 2025, Accepied: April 2025)

Abstract — SQL Injection (SQLI) is a security attack on databases that exploits loopholes or vulnerabilities in improperly monitored user input in web applications and is an important aspect of information system security. Research and development continues to be carried out using more effective methods to detect and prevent SQLI, including the use of Machine Learning algorithms such as Random Forest, Naïve Bayes, Support Vector Machine, Neutral Network, Knearest, Decision Tree and others. The focus of this research is to compare the performance results of each algorithm. This research compares the performance of each algorithm in detecting SQLI vulnerabilities against a set of related metrics. The results of the analysis based on the literature study show that Random Forest and Support Vector Machine (SVM) have superior value.

Keywords: SQL Injection, injection vulnerability detection, Machine Learning, Support Vector Machine, Random Forest.

Abstrak — SQL Injection (SQLI) adalah serangan keamanan pada database yang mengeksploitasi celah atau kerentanan pada input pengguna yang tidak dipantau dengan benar dalam aplikasi web dan merupakan aspek penting dalam keamanan sistem informasi. Penelitian dan pengembangan terus dilakukan menggunakan metode yang lebih efektif untuk mendeteksi dan mencegah SQLI, termasuk penggunaan algoritma Machine Learning seperti Random Forest, Naïve Bayes, Support Vector Machine, Neutral Network, Knearest, Decision Tree dan lainnya. Fokus penelitian ini adalah melakukan perbandingan terhadap hasil kinerja dari masing-masing algoritma. Penelitian ini membandingkan kinerja setiap algoritma dalam mendeteksi kerentanan SQLI terhadap serangkaian metrik terkait. Hasil analisis berdasarkan studi literatur menunjukan bahwa Random Forest dan Support Vector Machine (SVM) memiliki nilai kinerja yang unggul.

Kata Kunci: SQL Injection, injection vulnerability detection, Machine Learning, Support Vector Machine, Random Forest.

I. PENDAHULUAN

Keamanan aplikasi web adalah aspek penting untuk memastikan integritas dan keberlanjutan sebuah sistem informasi. Salah satu ancaman paling serius terhadap keamanan aplikasi web adalah *SQL Injection (SQLI). SQL Injection* adalah sebuah aksi *hacking* yang dilakukan di aplikasi *client* dengan cara memodifikasi perintah *SQL* yang ada di memori aplikasi *client, SQL Injection* merupakan teknik eksploitasi aplikasi berbasis yang di dalamnya menggunakan basis data untuk penyimpanan data [1]

Dalam beberapa tahun terakhir, pendekatan berbasis *Machine Learning (ML)* telah muncul sebagai alternatif yang menjanjikan untuk mendeteksi dan memitigasi serangan *SQLI*. Dengan menggunakan teknik *ML*, sistem keamanan dapat belajar mengenali pola mencurigakan dalam *Query SQL*, sehingga memungkinkan sistem mendeteksi dan mencegah serangan sebelum menyebabkan kerusakan.

Penelitian sebelumnya telah menyelidiki berbagai metode *Machine Learning* untuk mendeteksi *SQLI*, termasuk *Random Forest*, *Naive Bayes*, *K-Nearest Neighbors (KNN)*, *Neutral Network*, dan *Support Vector Machine (SVM).* Eksperimen dalam literatur telah mampu membandingkan kinerja masing-masing metode ini dalam mendeteksi serangan *SQLI* menggunakan kumpulan data terkait yang berisi sampel *Query SQL* yang aman dan berpotensi berbahaya.

Tinjauan literatur menyajikan hasil penelitian sebelumnya yang dilakukan di bidang ini. Identifikasi berbagai pendekatan, teknik, dan strategi yang digunakan untuk mendeteksi *SQLI* menggunakan Algoritma *Machine Learning* yang umum digunakan *seperti Random Forest, Naive Bayes, KNN, Neural Networks, SVM, etc.*

Tujuan dari tinjauan literatur ini adalah untuk memberikan pemahaman komprehensif tentang kemajuan dan tantangan dalam deteksi *SQLI* menggunakan algooritma *Machine Learning*. Memahami kontribusi yang ada dan mengidentifikasi area untuk penelitian lebih lanjut guna mengarahkan upaya masa depan menuju pengembangan solusi keamanan yang lebih efektif dan mudah beradaptasi dalam menghadapi ancaman *SQLI* yang semakin kompleks.

P-ISSN 1858-2680
E-ISSN 2723-4673

II. TINJAUAN PUSTAKA

Objek penelitian berfokus pada topik *SQL Injection* yang digunakan dalam mendeteksi serangan *SQLI* pada aplikasi *web* menggunakan algoritma *Machine Learning*. Penelitian ini menggunakan pendekatan *Systematic Literature Review (SLR).* Fokus utama akan diberikan pada perbandingan kinerja beberapa algoritma *Machine Learning*, termasuk *Random Forest, Naive Bayes, KNN, Neural Network, SVM*, dan lainnya dalam mendeteksi *SQLI*.

Research question yang dibuat pada penelitian ini merupakan pertanyaan yang dirumuskan berdasarkan kebutuhan dari topik penelitian. Perumusan *Research Question (RQ)* tentang perbandingan kinerja setiap algoritma *Machine Learning* dalam mendeteksi kerentanan *SQLI* harus fokus pada 5 elemen yang dikenal sebagai berikut:

PICOC, yaitu:

1. *Population* (P), kelompok sasaran untuk investigasi (misalnya orang, perangkat lunak, dll.)
2. *Intervention* (I), menentukan aspek investigasi atau masalah yang menarik bagi peneliti.
3. *Comparison* (C), aspek investigasi yang akan dibandingkan dengan intervensi
4. *Outcomes* (O), efek dari intervensi.
5. *Context* (C), latar atau lingkungan investigasi. [8]

Pertanyaan Penelitian (*Research Questions)*

Research Questions digunakan untuk membantu memberikan gambaran cakupan dan batasan SLR, dapat menggunakan metode PICOC tersaji pada Tabel 1.

Tabel 1. PICOC

Population (P)	Studi yang berkaitan dengan *SQL Injection, Detection Vulnerability, Machine Learning*
Intervention (I)	Mendeteksi sebuah kerentanan pada database dengan algoritma *Machine Learning*
Comparison (C)	*Machine Learning* dengan algoritma *RF, KNN, Naves Bayes, SVM, Neutral Network* dan lainnya dibandingkan untuk menemukan hasil yang lebih efektif
Outcomes (O)	Hasil perbandingan dengan tingkat performa yang lebih baik untuk mendeteksi *SQLI* dengan *Machine Learning*.
Context (C)	Penggunaan Algoritma dalam konteks deteksi kerentanan *SQL Injection*

Proses pencarian artikel diperoleh dari beberpa sumber diantaranya menggunakan situs Google Scholar, Scopus preview, dan ScienceDirect.com dengan bantuan *software Publish or Perish (PoP),* pada pencarian peniliti menggunakan kata kunci "*SQL injection, injection vulnerability detection, machine learning*", *"random forest ", "support vector machine"* untuk memudahkan dalam menemukan jurnal yang signifikan

Tabel 2. Pertanyaan Penelitian

#	**Pertanyaan Penelitian**
RQ1	Apa saja metrik evaluasi yang digunakan dalam penelitian terkait untuk menilai deteksi kerentanan *SQLI* menggunakan *Machine Learning*?
RQ2	Bagaimana perbandingan kinerja antara berbagai algoritma yang digunakan?
RQ3	Kesimpulan umum dari literatur yang telah dipublikasikan tentang deteksi kerentanan *SQL Injection* menggunakan pendekatan *Machine Learning*, termasuk kelebihan, kelemahan?

Pemilihan penelitian berdasarkan *Quality Asssassment* dengan tujuan untuk membantu peneliti memilih jurnal yang berkualitas. Adapun kriteria yang cocok untuk *QA* adalah:

1. Artikel yang digunakan dengan kriteria rentang waktu tahun 2020 - 2024
2. Data diperoleh dari sumber Google Scholar, Scopus preview, dan ScienceDirect.com

Data yang digunakan yaitu mengenai *SQL Injection, injection vulnerability detection, Machine Learning Algorithm* seperti *Support Vector Machine*, dan *Random Forest,etc*.

NO	Penulis, Tahun	QA1	QA2	QA3	Hasil
1	Mahmoud Khalid Baklizi *et al.*, 2024	YA	YA	YA	DITERIMA
2	Ahmed Abadulla Ashlam *et al.*, 2022	YA	YA	YA	DITERIMA
3	Edwin Peralta-Garcia *et al.*, 2024	YA	YA	YA	DITERIMA
4	Wubetu Barud Demilie *et al.*, 2022	YA	YA	YA	DITERIMA
5	Prince Roy *et al.*, 2022	YA	YA	YA	DITERIMA
6	Md. Maruf Hassan *et al.*,	YA	YA	YA	DITERIMA

P-ISSN 1858-2680
E-ISSN 2723-4673

2022

III. METODOLOGI PENELITIAN

Metode yang lebih efektif untuk mendeteksi dan mencegah *SQLI*, termasuk penggunaan algoritma *Machine Learning* seperti *Random Forest, Naïve Bayes, Support Vector Machine, Neutral Network, Knearest, Decision Tree*

IV. HASIL DAN PEMBAHASAN

Literature Review dilakukan pada Mei 2024, pencarian awal dilakukan menggunakan perangkat lunak *Publish or Perish (PoP)* pada *platform* Google Scholar berdasarkan tahun publikasi dengan rentang waktu 2020-2024. Hasil pencarian menggunakan *keywords "SQL injection, injection vulnerability detection, machine learning"* pada *PoP* ditampilkan sebanyak 200 jurnal, kemudian dilakukan penyaringan secara manual dan terdapat 4 yang terpilih, selanjutnya pada *keyword "Web attack, machine learning"* pada *PoP* ditampilkan sebanyak 200 jurnal, dilakukan penyaringan secara manual dan terdapat 1 yang terpilih, dan *"SQLI attack, machine learning", PoP* menampilkan sebanyak 200 jurnal, kemudian terdapat 1 yang dipilih. Penelitian ini menargetkan sebanyak 6 jurnal untuk dilakukan *literature review* pada jurnal yang relevan. *Literature* yang digunakan hanya *paper* jurnal, proses seleksi studi penelitian dilakukan juga dengan melihat judul, abstrak, hasil, serta kesimpulan dan diperoleh hasil studi utama yang akan digunakan untuk dianalisis lebih lanjut.

Tabel 4. Penyaringan Pencarian

No	Jurnal terpilih berdasarkan *keyword*	Jumlah
1	*SQL injection, injection vulnerability detection, machine learning*	4
2	*Web attack, machine learning*	1
3	*SQLI attack, machine learning*	1
	Jurnal Terpilih**:**	**6**

Berdasarkan tabel diatas dapat dilihat bahwa hasil seleksi yang dilakukan berdasarkan *keyword* terdapat sebanyak 6 jurnal yang terpilih sesuai dengan topik *SQL Injection* dengan *Machine Learning Algorithm*, kemudian seluruh informasi yang didapatkan akan di analisis.Seluruh jurnal di dalam penelitian ini menggunakan algoritma *Machine Learning* dengan melakukan pengujian dan perbandingan beberapa metode seperti *Support Vector Machines (SVMs), K-Nearest Neighbor (KNN), Naive Bayes (NB), Random Forest (RF), Neural Network* dan lainnya sebagai metode klasifikasi yang telah teruji di beberapa penelitian sebelumnya, metode-metode ini mampu menghasilkan kinerja yang baik dengan akurasi yang tinggi.

Tabel 5. Pembahasan dan hasil *Literature Review*

No	Penulis dan Tahun	Penerbit	Judul	Pembahasan	Hasil
1	Mahmoud Khalid Bakliz i *et al*., 2024	iJOE	*Web Attack Intrusion Detection System Using Machine Learning Techniques*	Penelitian ini mengevaluasi efektivitas terhadap tiga algoritma *Machine Learning*, yaitu *Random Forest s (RF*), *K-Nearest Neighbor (KNN),* dan *Naive Bayes (NB),* dalam mendeteksi serangan web menggunakan dataset *IDS Canadian Institute for Cyber Security (CIC-IDS2017).*	*RF* unggul 99,78% untuk tingkat akurasi. *KNN* unggul 99,49% dalam fase pengujian. Namun, baik *RF* maupun *KNN* mencapai tingkat presisi dan *recall* rata-rata 100%. Kesimpulannya, *RF* dan *KNN* diidentifikasi sebagai algoritma yang paling efektif untuk mendeteksi serangan web *IDS* berdasarkan penelitian ini.

P-ISSN 1858-2680
E-ISSN 2723-4673

2	Ahmed Abadulla Ashlam *et al*., 2022	IC_ASET	*A Novel Approach Exploiting Machine Learning to Detect SQLI Attacks*	Jurnal ini membahas pengungkapan peningkatan serangan *SQL injection* (*SQLI*) dalam lingkungan distribusi aplikasi Teknologi Informasi (TI) dan ketersediaan informasi tentang kerentanan secara terbuka di web. Berbagai algoritma *Machine Learning* telah diterapkan untuk mendeteksi serangan seperti *SVM, DT, KNeighbours, AdaBoost, RF*	Hasilnya *SVM* memiiki nilai akurasi tertinggi 94%. Kemudian dilakukan komparasi, sebuah model baru kombinasi *SVM* dan *SVM* PALOSDM, juga dikembangkan. Hasilnya menunjukkan bahwa pendekatan yang diusulkan berhasil meningkatkan tingkat akurasi deteksi dari 94% menjadi 99%
3	Edwin Peralta-Garcia *et al*., 2024	MDPI	*Detecting Structured Query Language Injections in Web Microservices Using Machine Learning*	Penelitian bertujuan untuk mengevaluasi efektivitas beberapa algoritma *Machine Learning* dalam mendeteksi *SQLI* pada layanan web mikro menggunakan dataset publik. Algoritma *Machine Learning* yang dibandingkan adalah *Random Forest*, decision tree, dan support vector machine (*SVM*).	Hasil evaluasi menunjukkan bahwa *Random Forest* memiliki kinerja terbaik, dengan presisi dan akurasi mencapai 99%, *recall* sebesar 97%, dan skor F1 sebesar 98%. *SVM* memiliki akurasi, presisi, dan skor F1 sebesar 98%, dengan *recall* 97%. Sementara *Decision tree* memiliki presisi 92%, *Recall* 86%, dan skor F1 97%,
4	Wubetu Barud Demilie *et al*., 2022	Springer Open	*Detection and prevention of SQLI attacks and developing compressive framework using Machine Learning and hybrid techniques*	Penelitian ini bertujuan untuk mendeteksi dan mencegah *SQLI* serta melakukan evaluasi dengan algoritma *Machine Learning* termasuk *Naive Bayes (NB), Decision Trees (DT), Support Vector Machine (SVM), Random Forest s (RF), Logistic Regression (LR),* dan *Neural Networks Based on Multilayer Perceptron (MLP),* serta pendekatan hibrida	Hasil evaluasi kinerja menunjukkan bahwa pendekatan kombinasi antara (*ANN* dan *SVM*) lebih unggul dibandingkan pendekatan *ML* lainnya dalam menunjukkan akurasi yang lebih baik dalam presisi (98,87% dan 99,20%), *recall* (99,13% dan 99,47%), skor f1 (99,00% dan 99,33%), dan set pengujian (98,70% dan 99,40%) masing-masing dibandingkan dengan pendekatan *ML* lainnya. Namun, waktu pengujian mereka terlalu tinggi yaitu 15,33 milidetik
5	Prince Roy *et al*., 2022	ICAAIC	*SQL Injection Attack Detection by Machine Learning Classifier*	Penelitian membahas kerentanan *SQLI* dalam sistem berbasis web, penelitian menggunakan berbagai metode *Machine Learning*, seperti *Logistic Regression*, *AdaBoost*, *Random Forest*, *Naive* Bayes, dan *XGBoost Classifier*, untuk mengidentifikasi dan	Hasilnya, setelah menganalisis kinerja klasifikasi, disimpulkan bahwa kinerja terbaik dalam semua parameter diberikan oleh *Naïve Bayes*. Akurasi (98,33%), Skor F1 (97,00%), Sensitivitas (100%), Spesifisitas (97,71%), Presisi (94,19%),

P-ISSN 1858-2680
E-ISSN 2723-4673

				mendeteksi serangan *SQL Injection*	diberikan oleh *Naïve Bayes* (97,00%). *Logistic Regression* memberikan akurasi sebesar 92,73%, *Adaboost* memberikan akurasi sebesar 90,35%, *XGBoost* memberikan akurasi sebesar 89,64%, dan *Random Forest* memberikan akurasi sebesar 92,14%.
6	Md. Maruf Hassan *et al*., 2022	IJEEI	*SQL Injection Vulnerability Detection Using Deep Learning : A Feature-based Approach*	Penelitian ini berfokus pada deteksi *SQLI* dalam aplikasi web. Menggunakan *Machine Learning* untuk mendeteksi *SQLI* dengan algoritma *SVM,* Naïve Bayes dan *Random Forest*	Hasil perbandingan algoritma menunjukan bahwa *RF* memiliki akurasi 97,33%, *SVM* 94,66%, *Naive Bayes* 84,49%. Sedangkan *Neutral Network (NN)* yang diusulkan pada penelitian ini berhasil mencapai akurasi tertinggi yaitu sebesar 98,04%.

I. PENUTUP

A.Kesimpulan

Hasil *RQ*1, metrik evaluasi yang digunakan adalah *precision, acuracy, f1 score*, waktu komputasi dan lainnya. Hasil *RQ*2, perbandingan memberikan wawasan tentang efektivitas relatif setiap algoritma dalam mendeteksi kerentanan *SQLI*. Perbandingan dilakukan berdasarkan nilai kinerja terbaik dalam metrik evaluasi, jika hasil evaluasi menunjukkan bahwa suatu algoritma lebih akurat dan memiliki nilai skor tinggi pada metrik lain maka dinilai lebih baik dan kemungkinan besar algoritma ini lebih efektif dalam mendeteksi kerentanan *SQLI*. Hasil *RQ*3, kesimpulan umum mengenai cara menggunakan *machine learning* untuk mendeteksi kerentanan *SQL injection* yaitu memiliki kelebihan dalam hal deteksi kerentanan, kemampuan akses terhadap banyak data, dan otomatis. Sedangkan kelemahan dalam penggunaan *ML* salah satunya adalah model yang kompleks sehingga sulit untuk difahami.

Hasil studi *literature* terhadap topik penelitian deteksi kerentanan *SQL injection* dengan menggunakan algoritma *machine learning* seperti *RF, SVM, NN, DT, etc* dan kegiatan identifikasi, evaluasi, serta interpretasi semua bukti penelitian untuk menjawab pertanyaan penelitian tertentu. Berdasarkan jurnal yang telah di pilih untuk dilakukan *SLR*, bahwa pada proses penilaian kinerja deteksi kerentanan *SQLI* terdapat dua algoritma dengan nilai kinerja terbaik yaitu *Random Forest* dengan nilai tertinggi sebesar 99,78% pada jurnal berjudul *"Web Attack Intrusion Detection System Using Machine Learning Techniques*" dan untuk *Support Vector Machine* sebesar 94% kemudian dilakukan dilakukan komparasi, sebuah model baru kombinasi *SVM* dan *SVM* PALOSDM dikembangkan. Hasilnya, tingkat akurasi bertambah sebanyak 5% menjadi 99% dalam penelitian berjudul "*A Novel Approach Exploiting Machine Learning to Detect SQLI Attacks".*

B.Saran

1. Disarankan Hasil studi *literature* terhadap topik penelitian deteksi kerentanan *SQL injection* dengan menggunakan algoritma *machine learning* seperti *RF, SVM, NN, DT, etc diperlukan pengembangan dan ditingkatkan lagi dalam hal kemajuan tek nologi.*

2.Kurangnya publikasi dalam memberi sumber pada penelitian ini disaran agar lebih berkonsultasi ke pakar agar menjadi sempurna

Daftar Pustaka

[1] Bastian, A., Sujadi, H., & Abror, L. (2020). Analisis keamanan aplikasi data pokok Pendidikan (DAPODIK) menggunakan penetration testing dan *SQL injection*. INFOTECH *journal*, 6(2), 65-70.

P-ISSN 1858-2680
E-ISSN 2723-4673

[2] Baklizi, M. K., Atoum, I., Alkhazaleh, M., Kanaker, H., Abdullah, N., Al-Wesabi, O. A., & Otoom, A. A. (2024). Web Attack Intrusion Detection System Using *Machine Learning Techniques*. *International Journal of Online & Biomedical Engineering*, 20(3).

[3] [Hassan, M. M., Ahmad, R. B., & Ghosh, T. (2021). *SQL injection vulnerability detection using deep learning: a feature-based approach. Indonesian Journal of Electrical Engineering and Informatics* (IJEEI), 9(3), 702-718.

[4] Roy, P., Kumar, R., & Rani, P. (2022, May). *SQL injection attack detection by Machine Learning classifier. In 2022 International Conference on Applied Artificial Intelligence and Computing* (ICAAIC) (pp. 394-400). IEEE.

[5] Demilie, W. B., & Deriba, F. G. (2022). *Detection and prevention of SQLI attacks and developing compressive framework using Machine Learning and hybrid techniques. Journal of Big Data,* 9(1), 124.

[6] 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.

[7] Ashlam, A. A., Badii, A., & Stahl, F. (2022, March). *A novel approach exploiting Machine Learning to detect SQLI attacks. In 2022 5th International Conference on Advanced Systems and Emergent Technologies* (IC_ASET) (pp. 513-517). IEEE.

[8] R. S. Wahono, "*Literature Review*: Pengantar dan Metode," di romisatriawahono.net, 2016. [Online]. Tersedia: http://romisatriawahono.net.

P-ISSN 1858-2680
E-ISSN 2723-4673