JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 5, No. 1, Januari 2026, pp. 326 - 339
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/169

Machine Learning Performance Comparison for Web Application Security Threat Detection: A Systematic Review

Divala Zahra Oktavia*[1], Dwi Alvin Hidayat[2], Desy Natalia[3], Satria Krisna Prabantara[4], Arief Arfriandi[5]
[1,2,3,4,5] Fakultas Teknik, Universitas Negeri Semarang
Jl. Taman Siswa Sekaran, Gunungpati Semarang 50229, Semarang, Jawa Tengah, Indonesia
e-mail: divalazahra12@students.unnes.ac.id*[1], dwihidayat285@students.unnes.ac.id[2], desynataliaa17@students.unnes.ac.id[3], satriaprabantara19@students.unnes.ac.id[4], arfriandi@mail.unnes.ac.id[5]

ARTICLE INFO

Article History:

Received: 15-11-2025
Revised: 06-12-2025
Accepted: 28-12-205
Published: 21-01-2026

ABSTRACT

The increasing use of web-based applications across various sectors has led to a growing risk of cyber threats, including phishing, DDoS attacks, SQL Injection, cross-site scripting (XSS), and other forms of intrusion. Traditional detection methods, which are often static, frequently fail to identify newly emerging, dynamic attack patterns. To overcome these limitations, machine learning has emerged as a more adaptive approach that can learn behavioral patterns, detect anomalies, and automatically identify potential threats. This study conducts a Systematic Literature Review (SLR) to investigate the application of machine learning in enhancing web application security and to evaluate the performance of several algorithms commonly used in prior research. The SLR is structured using the PICOC framework, which includes population, intervention, comparison, outcome, and context. The analysis reveals that machine learning techniques are widely applied across various aspects of web security, including phishing detection, malicious URL classification, mitigation of DDoS impacts, and network intrusion detection. Algorithms such as Random Forest, XGBoost, and Support Vector Machine (SVM) consistently demonstrate strong performance, achieving high accuracy across diverse datasets and attack scenarios. Additionally, supporting techniques such as ADASYN, feature selection, and natural language processing-based methods further improve model effectiveness. Overall, the findings of this study highlight that machine learning not only accelerates and improves the precision of threat detection but also adapts to evolving attack patterns, making it a critical component in strengthening the security of modern web applications.

Keywords: *Web Applications, Threat Detection, Cybersecurity, Machine Learning, Systematic Literature Review (SLR).*

Abstrak

Pemanfaatan aplikasi berbasis web yang semakin meluas di berbagai sektor menyebabkan meningkatnya risiko terhadap ancaman siber, termasuk serangan *Phising*, DDoS, injeksi SQL, XSS, serta intrusi. Berbagai

DOI: https://doi.org/10.51903/dhayjg79

p-ISSN : 2803-1507 e-ISSN : 2803-1531

metode deteksi tradisional yang bersifat statis sering kali tidak mampu mengidentifikasi pola serangan baru yang bersifat dinamis. Untuk mengatasi keterbatasan tersebut, *machine learning* muncul sebagai pendekatan yang lebih adaptif karena mampu mempelajari pola perilaku, mendeteksi anomali, dan melakukan deteksi ancaman secara otomatis. Penelitian ini melakukan tijauan sistematis literatur *(Systematic Literature Review*/SLR) untuk meneliti penggunaan *machine learning* dalam mengingkatkan keamanan aplikasi web dan mengevaluasi performa beberapa algoritma yang digunakan. SLR dilaksanakan dengan menggunakan kerangka PICOC, yang mencakup populasi, intervensi, perbandingan, hasil, konteks. Hasil analisis menunjukkan bahwa *machine learning* digunakan untuk berbagai aspek keamanan web, seperti deteksi *Phising*, penentuan URL berbahaya, pengurangan dampak serangan DDoS, serta identifikasi intrusi jaringan. Algoritma seperti *Random Forest*, XGBoost, dan SVM terbukti memiliki kinerja yang stabil dengan tingkat akurasi yang tinggi. Selain itu, teknik pendukung seperti ADASYN, *feature selection*, dan metode berbasis pemrosesan bahasa alami turut meningkatkan efektivitas model. Secara keseluruhan, hasil penelitian ini menegaskan bahwa *machine learning* dapat mempercepat dan meningkatkan ketepatan deteksi ancaman serta memberikan adaptasi terhadap pola serangan yang terus berubah, sehingga menjadi komponen penting dalam memperkuat keamanan aplikasi web.

Kata Kunci: *Aplikasi Web, Deteksi Ancaman, Keamanan Siber, Machine Learning, Systematic Literature Review (SLR).*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong penggunaan aplikasi web secara luas di berbagai sektor seperti layanan publik, pendidikan, *e-commerce*, dan keuangan. Namun, peningkatan penggunaan ini turut memperbesar risiko terhadap ancaman siber, termasuk *SQL Injection, Cross-Site Scripting (XSS), Denial of Service (DoS/DDoS)*, serta *phishing*, yang semakin berkembang dengan pola serangan yang dinamis sehingga sulit ditangani menggunakan metode tradisional berbasis aturan [1].

Machine learning (ML), sebagai bagian dari kecerdasan buatan, menawarkan pendekatan adaptif yang mampu mempelajari pola data, mengenali aktivitas mencurigakan, serta melakukan deteksi ancaman secara otomatis tanpa aturan statis [2]. Dalam konteks keamanan siber, ML digunakan untuk membedakan antara aktivitas normal dan aktivitas berbahaya melalui analisis perilaku sistem maupun struktur permintaan web. Penelitian sebelumnya telah menunjukkan bahwa algoritma seperti SVM, *Random Forest*, *Neural Network*, dan model *deep learning* mampu meningkatkan akurasi dan efisiensi dalam mendeteksi berbagai jenis serangan pada aplikasi web [3], [4].

Walaupun telah terdapat banyak studi mengenai keamanan siber berbasis ML, kajian secara sistematis yang secara khusus membahas peran ML dalam keamanan aplikasi web masih terbatas. Oleh karena itu, penelitian ini melakukan *Systematic Literature Review* (SLR) untuk meninjau kontribusi ML dalam peningkatan keamanan aplikasi web dan mengevaluasi performa algoritma yang digunakan. Penelitian ini berfokus pada dua pertanyaan utama, yaitu bagaimana ML diterapkan dalam mendeteksi ancaman pada aplikasi web, serta bagaimana performa dan efektivitas berbagai pendekatan ML dalam mencegah serangan. Hasil kajian ini diharapkan dapat memberikan gambaran menyeluruh mengenai tren penelitian terkini serta menjadi acuan dalam pengembangan sistem keamanan aplikasi web yang lebih cerdas, adaptif, dan responsif terhadap ancaman modern.

Berbeda dengan penelitian terdahulu yang umumnya berfokus pada satu jenis ancaman atau satu pendekatan tertentu, seperti deteksi malicious website berbasis convolutional neural network oleh Alsaedi et al. [5], analisis serangan phishing pada media sosial oleh Dewanto et al. [6], serta studi eksperimental identifikasi *SQL Injection* menggunakan *Damn Vulnerable Web Application* (DVWA) oleh Wiandani et al. [7], penelitian ini menyajikan kajian yang lebih komprehensif dalam konteks keamanan aplikasi web. Selain itu, beberapa studi mutakhir, seperti yang dilakukan oleh Wang et al. melalui pendekatan dynamic command perturbation [8], menyoroti aspek kerentanan sistem, namun belum memberikan pemetaan terstruktur terkait performa model *machine learning* berdasarkan jenis serangan aplikasi web. Oleh karena itu, kontribusi utama penelitian ini terletak pada systematic literature review terhadap publikasi periode 2021–2025 dengan fokus pada perbandingan performa algoritma *machine learning* dan *deep learning* berdasarkan jenis ancaman aplikasi web, meliputi phishing, *SQL Injection*, Cross-Site Scripting (XSS), *Distributed Denial of Service* (DDoS), dan intrusion detection. Selain itu, penelitian ini mengidentifikasi kesenjangan riset yang masih terbuka, khususnya terkait keterbatasan dataset yang merepresentasikan trafik aplikasi web modern, minimnya integrasi pendekatan *machine learning* dengan praktik keamanan aplikasi web, serta kurangnya

p-ISSN : 2803-1507 e-ISSN : 2803-1531

evaluasi ketahanan model terhadap skenario serangan yang dinamis. Dengan demikian, SLR ini tidak hanya merangkum penelitian terdahulu, tetapi juga memberikan arah pengembangan riset *machine learning* yang lebih terstruktur dan aplikatif dalam domain keamanan aplikasi web.

2. TINJAUAN PUSTAKA

2.1. *Keamanan Web*

Keamanan aplikasi web merupakan aspek penting dalam pengembangan sistem berbasis web karena aplikasi modern banyak menggunakannya untuk transaksi, penyimpanan data sensitif, dan layanan berbasis internet. Meningkatnya ancaman terhadap aplikasi web sejalan dengan kemajuan teknologi dan jumlah pengguna. Agar sistem tetap menjaga keandalan dan integritas sistemnya, maka diperlukan metode untuk mendeteksi dan mencegah serangan yang terus berkembang. Pengelolaan sistem keamanan web *(web security system)* memegang peranan vital bagi integritas data serta kepercayaan pengelola dan pengguna platform. Banyak pengguna lebih memperhatikan desain dan konten untuk menarik perhatian. Namun, jika salah satu pengelola atau pengguna mengabaikan aspek keamanan, maka pengguna yang akan dirugikan karena seseorang dapat mencuri informasi penting dari situs web dan bahkan merusak tampilannya. Melindungi komputer, aplikasi, dan jaringan dari sebuah situs web merupakan elemen kunci dalam menjaga keamanannya, karena hal ini memastikan bahwa informasi yang tersimpan tetap terlindungi.

Aplikasi web saat ini menjadi fokus utama bagi serangan siber karena perannya penting dalam berbagai layanan publik, e-commerce, pendidikan, dan sektor keuangan. Kelemahan yang terdapat pada lapisan aplikasi sering kali dimanfaatkan menggunakan cara-cara seperti *SQL Injection*, XSS, CSRF, serta rekayasa sosial (*Phising*). Metode tradisional rule-based dan signature-based cenderung lambat dalam beradaptasi dengan jenis serangan yang baru, sehingga hal ini mendorong penggunaaan pendekatan yang berbasis data dan pembelajaran mesin yang lebih responsif [5].

2.2. *Jenis Ancaman Keamanan pada Aplikasi Web*

Aplikasi web memiliki berbagai titik kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mendapatkan akses ilegal, merubah informasi, atau mengganggu layanan. Untuk menciptakan pemahaman fundamental mengenai risiko yang paling kritis, diperlukan klasifikasi terkait jenis ancaman yang sering menyerang aplikasi berbasis web. Adapun ancaman keamanan yang umum ditemukan pada aplikasi web meliputi hal-hal berikut:

2.2.1. *Phising*

Praktik phishing melibatkan penyamaran pelaku sebagai pihak terpercaya guna memanipulasi korban agar menyerahkan informasi sensitif seperti kredensial akun atau data pribadi. Serangan ini umumnya dilakukan melalui email, pesan singkat, atau situs web palsu yang dibuat menyerupai situs resmi. Dampak dari *phishing* dapat berupa kerugian finansial, pencurian identitas, hingga kebocoran data, sehingga edukasi dan kesadaran masyarakat dalam mengenali ciri-ciri *phishing* menjadi sangat penting. Dalam konteks hukum di Indonesia, *phishing* diatur dalam UU Nomor 19 Tahun 2016 sebagai perubahan dari UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Namun, ketentuan yang ada dinilai belum memberikan rumusan yang jelas sehingga menimbulkan kekaburan hukum. Pada praktiknya, *phishing* dilakukan dengan membuat situs palsu yang menyerupai situs resmi, kemudian mengarahkan korban untuk memasukkan data pribadi seperti *username*, *password*, atau informasi keuangan. Data yang diperoleh tersebut kemudian digunakan secara ilegal dan merugikan korban. Pasal yang relevan, seperti Pasal 28 dan Pasal 35, belum sepenuhnya mencakup unsur manipulasi dan penipuan dalam *phishing* secara utuh. Oleh karena itu, diperlukan perumusan konsep *phishing* yang lebih tegas serta revisi pada Pasal 35 agar penegakan hukum terhadap pelaku dapat dilakukan dengan lebih efektif [6].

2.2.2. *Injection attacks*

Injection attacks menempati jajaran ancaman keamanan aplikasi *web* yang paling berisiko karena kemampuannya dalam memanipulasi logika sistem melalui penyisipan kode berbahaya. Di antara berbagai varian injection, *SQL Injection* (SQLi) dan Command Injection menjadi fokus utama karena menyerang logika aplikasi serta hubungan dengan basis data atau sistem backend sebuah celah yang jika dimanfaatkan dapat menimbulkan konsekuensi berat terhadap kerahasiaan, integritas, dan ketersediaan data.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Pada serangan *SQL Injection*, penyerang memanfaatkan masukan pengguna yang tidak melalui proses sanitasi atau validasi dengan benar—baik melalui form, URL, maupun parameter lainnya. Dengan kondisi tersebut, penyerang dapat menyisipkan perintah SQL berbahaya sehingga aplikasi mengeksekusi query yang memungkinkan akses tidak sah untuk membaca, mengubah, atau menghapus data dalam database. Studi menggunakan aplikasi rentan seperti *Damn Vulnerable Web Application* (DVWA) menunjukkan bahwa serangan ini sangat mudah dilakukan pada tingkat keamanan rendah karena lemahnya validasi input. Sebaliknya, pada tingkat keamanan yang lebih tinggi, penggunaan *prepared statements* dan mekanisme validasi ketat mampu menurunkan risiko secara signifikan [7].

Di sisi lain, command injection terjadi ketika aplikasi mengeksekusi input pengguna sebagai perintah sistem tanpa melakukan sanitasi ataupun pembatasan yang memadai. Kerentanan ini dapat dimanfaatkan penyerang untuk menjalankan perintah sistem secara bebas, memanipulasi file, atau bahkan melakukan eskalasi hak akses. Dengan demikian, baik *SQL Injection* maupun command injection sama-sama menekankan pentingnya kontrol input dan mekanisme keamanan yang kuat pada aplikasi [8].

Mitigasi terhadap serangan injection umumnya dilakukan melalui penerapan praktik pengembangan aplikasi yang aman, seperti penggunaan parameterized queries atau prepared statements, sanitasi serta validasi pada seluruh input dan output, pemanfaatan *Web Application Firewall* (WAF), serta penerapan enkripsi dan kontrol akses. Beberapa penelitian yang mengkaji penggunaan WAF seperti ModSecurity menunjukkan bahwa sistem ini mampu mendeteksi dan memblokir berbagai payload injeksi yang berbasis signature atau pola serangan yang telah teridentifikasi [9]. Namun, pendekatan tradisional tersebut mulai menunjukkan keterbatasan ketika berhadapan dengan serangan yang lebih kompleks, seperti payload yang di-obfuscate, dimodifikasi, atau pola injeksi baru yang tidak terdapat dalam basis data signature. Kondisi ini mendorong banyak peneliti untuk mengembangkan model deteksi berbasis data, termasuk teknik *machine learning* (ML) dan *deep learning* (DL), yang dinilai lebih adaptif dalam mengenali pola serangan modern [10].

3. METODOLOGI PENELITIAN

3.1. *Pertanyaan dalam Penelitian*

Daftar pertanyaan penelitian atau RQ telah disusun untuk menentukan arah dan tujuan utama dalam literatur review ini. Rancangan entitas dalam kajian ini dirancang dengan menggunakan sistem *Population, Intervention, Comparasion, Outcomes,* dan *Context* (PICOC). Susunan pertanyaan dalam penelitian berbasis PICOC dapat dilihat pada Tabel 1.

Tabel 1. Kerangka PICOC

No	PICOC	Deskripsi
1	*Population* (Populasi)	Penelitian ini mengarah pada pemanfaatan aplikasi berbasis web yang rentan terhadap serangan siber seperti *Phising*, DDos, *SQL Injection*, atau serangan *malware*. Studi harus relevan dengan domain keamanan aplikasi web.
2	*Intervention* (Intervensi)	Penerapan teknik *Machine learning* (ML) atau *Deep learning* (DL) sebagai metode untuk mendeteksi, mengklasifikasi, mencegah ancaman keamanan pada aplikasi web. Termasuk penggunaan algoritma seperti SVM, *Random Forest*, *Decision Tree*, KNN, XGBoost, CNN, atau RNN.
3	*Comparison* (Perbandingan)	Perbandingan dilakukan terhadap pendekatan tradisional (*rule-based*, manual, *signature-based*) atau antar algoritma ML yang berbeda, untuk mengevaluasi perbaikan kinerja dan efisiensi sistem keamanan.
4	*Outcome* (Hasil yang diharapkan)	Hasil berupa peningkatan performa keamanan aplikasi web, meliputi akurasi deteksi yang lebih tinggi, *False Positive* lebih rendah, respon yang lebih cepat, serta kemampuan adaptasi terhadap ancaman baru.
5	*Context* (Konteks Penelitian)	Studi yang diterbitkan dalam rentang waktu 2021-2025, baik berbahasa indonesia maupun inggris, yang berfokus pada ML untuk keamanan siber berbasis web. Sumber artikel diambil dari Google Scholar dan Scopus.

Kajian yang diakukan dalam penelitian ini berdasarkan dua pertanyaan penelitian utama yang berhubungan dengan penggunaan *machine learning* untuk memperbaiki keamanan aplikasi web. Pertanyaan-pertanyaan ini berperan sebagai petunjuk dalam melakukan identifikasi, seleksi, dan analisis terhadap literatur yang relevan, yang dirumuskan sebagai berikut:

RQ1: Bagaimana machine learning diterapkan untuk meningkatkan keamanan aplikasi web?

RQ2: Bagaimana performa dan efektivitas berbagai pendekatan machine learning dalam mendeteksi dan mencegah ancaman pada aplikasi web?

p-ISSN : 2803-1507 e-ISSN : 2803-1531

3.2. *Kriteria Inklusi dan Ekslusi*

Proses pemilihan artikel dilakukan dengan menggunakan kriteria inklusi dan eksklusi. Kriteria inklusi memberikan penekanan pada studi mengenai penggunaan *machine learning* dalam keamanan aplikasi web, sementara kriteria eksklusi menyingkirkan studi yang tidak relevan atau tidak sesuai fokus kajian. Kriteria ini dirancang untuk memastikan bahwa hanya artikel yang memiliki relevansi dan kualitas tinggi yang dipilih untuk dianalisis lebih lanjut. Tabel 2 menunjukkan berbagai kategori kriteria inklusi dan eksklusi yang diterapkan dalam penelitian ini.

Tabel 2. Kriteria Inklusi dan Eksklusi

Kategori	Kriteria Inklusi	Kriteria Eksklusi
Topik Penelitian	Artikel yang membahas tentang penerapan *machine learning* untuk mendeteksi, mencegah, atau mengingatkan keamanan aplikasi web.	Artikel yang tidak membahas mengenai keamanan aplikasi web, atau hanya fokus pada keamanan jaringan tanpa keterkaitan dengan aplikasi web.
Metode yang Digunakan	Studi yang menggunakan algoritma *machine learning* (misalnya : SVM, *Random Forest*, *Desicion Tree*, CNN, dll).	Studi yang tidak menggunakan *machine learning* atau hanya berfokus pada metode manual / tradisional.
Jenis Artikel	Artikel jurnal atau prosiding konferensi yang diterbitkan dan dapat diakses melalui Scopus dan Google Scholar.	Artikel non-ilmiah, whitepaper, laporan perusahaan, atau tulisan popular.
Bahasa Publikasi	Artikel yang ditulis dalam bahasa indonesia dan bahasa inggris.	Artikel dalam bahasa lain yang tidak memiliki terjemahan resmi.
Tahun Publikasi	Artikel yang diterbitkan antara tahun 2021 hingga 2025, untuk mencakup perkembangan terbaru dalam keamanan aplikasi web berbasis ML.	Artikel yang diterbitkan sebelum tahun 2020
Ketersediaan Dokumen	Artikel yang diakses dengan penuh (full-text available) untuk dianalisis lebih lanjut.	Artikel yang tidak dapat diakses secara penuh.

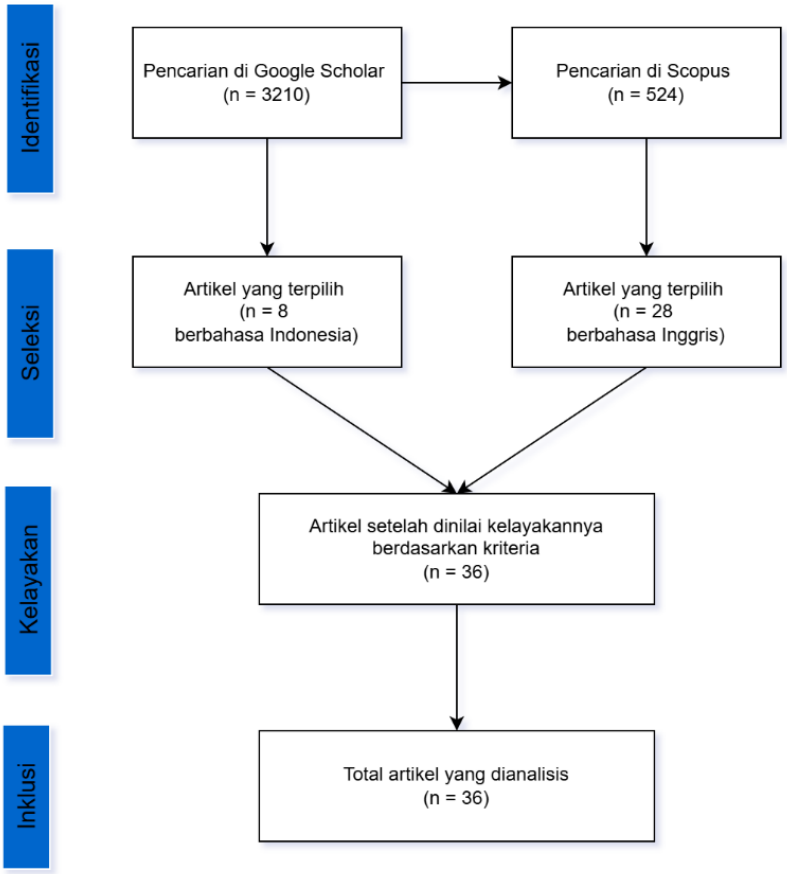
3.3. *Strategi Pencarian Literatur*

Proses pencarian literatur dalam penelitian ini dilakukan secara sistematis untuk memperoleh sumber yang relevan dengan topik penerapan *machine learning* dalam peningkatan keamanan aplikasi web. Pencarian dilakukan melalui dua basis data utama yaitu, Google Sholar dan Scopus, dengan menerapkan pendekatan PICOC untuk memastikan kesesuaian artikel dengan fokus kajian penelitian. Pada pencarian melalui Google Scholar, digunakan kata kunci : ”*Machine learning* Keamanan Aplikasi Web Deteksi Serangan”. Sementara itu, pencarian di Scopus menggunakan kueri yang mencakup kombinasi istilah: ("*machine learning*" *OR* "*deep learning*" *OR* "*artificial intelligence*") *AND* ("*web application*" *OR* "*web security*" *OR* "*application layer security*") *AND* ("*cybersecurity*" *OR* "*intrusion detection*" *OR* "*threat detection*" *OR* "*anomaly detection*"), dengan pembatasan tahun publikasi antara 2020–2025, bidang kajian ilmu komputer dan teknik, serta hanya mencakup artikel berbahasa Inggris yang terindeks dan dapat diakses secara terbuka.

3.4. *Proses Seleksi Literatur*

Proses seleksi literatur dilakukan secara bertahap dengan mengacu pada alur *PRISMA* (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) yang disederhanakan. Tahap pertama melibatkan pencarian literatur yang relevan melalui database akademik seperti Google Scholar, PubMed, dan Scopus. Selanjutnya, literatur yang ditemukan disaring berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan, seperti tahun publikasi dan kesesuaian topik. Hanya studi yang memenuhi kriteria tersebut yang kemudian dievaluasi lebih lanjut untuk analisis yang mendalam, sebagaimana ditunjukkan pada Gambar 1.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 1. Diagram PRISMA

Tahap identifikasi menghasilkan total 3.734 artikel, yang terdiri dari 3.210 artikel dari Google Scholar dan 524 artikel dari Scopus. Selanjutnya, pada tahap seleksi, artikel disaring berdasarkan judul dan abstrak untuk menilai kesesuaian topik dengan penelitian. Pada tahap ini diperoleh 8 artikel berbahasa Indonesia dari Google Scholar dan 28 artikel berbahasa Inggris dari Scopus yang dianggap relevan. Artikel yang lolos tahap seleksi kemudian memasuki tahap kelayakan, yaitu penilaian terhadap teks lengkap (*full-text*) berdasarkan kriteria inklusi, meliputi fokus pada keamanan aplikasi web, penggunaan metode machine learning, serta kejelasan metodologi dan kontribusi penelitian. Berdasarkan evaluasi kelayakan tersebut, seluruh artikel yang diseleksi dinyatakan layak untuk dianalisis lebih lanjut. Pada tahap inklusi, sebanyak 36 artikel (8 artikel nasional dan 28 artikel internasional) digunakan sebagai sumber utama dalam analisis dan sintesis pada penelitian Systematic Literature Review ini.

3.5. *Sintesis Temuan*

Data yang telah diekstraksi selanjutnya dianalisis untuk menjawab kedua rumusan pertanyaan penelitian (RQ). Analisis terhadap RQ1 difokuskan pada kajian penerapan *machine learning* dalam mengatasi berbagai ancaman terhadap keamanan aplikasi web, seperti *phishing*, DDoS, *malware*, dan *intrusion attack*, dengan meninjau pendekatan teknis serta arsitektur sistem yang digunakan. Sedangkan analisis RQ2 diarahkan pada evaluasi kinerja dan efektivitas berbagai algoritma *machine learning* berdasarkan metrik pengukuran seperti akurasi, presisi, *recall*, F1-*score*, dan efisiensi komputasi dari model seperti SVM, *Random Forest*, *Decision Tree*, XGBoost, CNN, dan TabNet. Hasil keseluruhan analisis ini memberikan pemahaman komprehensif mengenai perkembangan terkini dalam riset keamanan aplikasi web berbasis *machine learning*, sekaligus mengidentifikasi efektivitas pendekatan yang ada serta peluang pengembangan di masa mendatang.

4. HASIL DAN PEMBAHASAN

Dalam penelitian terkait keamanan aplikasi web berbasis machine learning, berbagai metode dan algoritma telah diuji untuk mendeteksi ancaman seperti *DDoS*, *SQL Injection*, dan *Phishing*. Beberapa artikel

p-ISSN : 2803-1507 e-ISSN : 2803-1531

membandingkan efektivitas berbagai teknik, seperti *Long Short-Term Memory* (*LSTM*), *Convolutional Neural Network* (*CNN*), hingga model *ensemble*, dengan menggunakan berbagai jenis dataset, mulai dari trafik jaringan hingga payload *HTTP*. Selain itu, performa numerik yang diperoleh, termasuk akurasi dan *F1-score*, menunjukkan variasi hasil yang signifikan tergantung pada algoritma yang diterapkan. Tabel 3 menyajikan ringkasan hasil dari penelitian-penelitian tersebut, memberikan gambaran mengenai penerapan dan performa setiap algoritma yang digunakan.

Tabel 3. Ringkasan Hasil Systematic Literature Review Keamanan Aplikasi Web Berbasis Machine Learning

Daftar Artikel	Dataset	Algoritma yang Dibandingkan	Performa Numerik
NetSentry: A *deep learning* approach to detecting incipient large-scale network attacks	Network Traffic	LSTM, CNN & ML tradisional	Akurasi > 90 %
Multi-Stage Learning Framework Using Convolutional Neural Network and Decision Tree-Based Classification for Detection of DDoS Pandemic Attacks in SDN-Based SCADA Systems	Kubernetes Logs	ML Scheduler	Waktu eksekusi menurun
DRaNN_PSO: A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things	UNSW-NB15, ToN-IoT	DRaNN, DRaNN+PSO	Akurasi > 98%
Detection and defending the XSS attack using novel hybrid stacking ensemble learning-based DNN approach	HTTP Payload	DNN, Ensemble	Akurasi > 96%
A BERT-Enhanced Exploration of Web and Mobile Request Safety Through Advanced NLP Models and Hybrid Architectures	HTTP & SQL Request	CNN, RNN, BERT+CNN	Akurasi > 97%
Effective Filter for Common Injection Attacks in Online Web Applications	Web Input	Filter-based vs ML	Akurasi 98,4%
Cybersecurity in *Deep learning* Techniques: Detecting Network Attacks	HTTP DATASET CSIC 2010	Decision Tree (DT), Random Forest (RF), Long Short-Term Memory (LSTM), CNN	Akurasi mencapai 99,5%
Using attack graphs to defend healthcare systems from cyberattacks: a longitudinal empirical study	CVSS, ICS Dataset	KNN, RF, SVM	KNN terbaik
An empirical assessment of ensemble methods and traditional *machine learning* techniques for web-based attack detection in industry 5.0	HTTP Logs	RF, Gradient Boosting	Akurasi > 95%
Injections Attacks Efficient and Secure Techniques Based on Bidirectional Long Short Time Memory Model	SQL Payload	Bi-LSTM, SVM	Akurasi > 97%
Research on *Deep learning* and Feature Aggregation Techniques for Web Security	Web Traffic	SSA-ResNet-SAN	Akurasi > 98%
Deep learning anomaly detection based on hierarchical status-connection features in networked control systems	Industrial Web App	SUSAN	FP rendah
Improved Phishing Attack Detection with *Machine learning*: A Comprehensive Evaluation of Classifiers and Features	URL Dataset	RF, XGBoost, DT	Akurasi 97–99%
Web Attack Intrusion Detection System Using *Machine learning* Techniques	Network Traffic	SVM, RF, KNN	Akurasi > 95%
Validation of a *Machine learning*-Based IDS Design Framework Using ORNL Datasets for Power System with SCADA	ORNL SCADA	RF, GAN-based	F1-score 94,09%
AE-Net: Novel Autoencoder-Based Deep Features for *SQL Injection* Attack Detection	SQL Queries	AE-Net vs Manual	Akurasi 0,99
Toward the flow-centric detection of browser fingerprinting	JavaScript Code	Static Analysis	F-measure 97,81%
Threat Hunting Architecture Using a *Machine learning* Approach for Critical Infrastructures Protection	Network Logs	ML Threat Hunting	Deteksi *Real-time*
Vulnerabilities of Web Applications: Good Practices and New Trends	OWASP Testbed	Layered Security	Serangan menurun signifikan
Victim Verification with the Use of Deep Metric Learning in DVI System Supported by Mobile Application	Image Dataset	Deep Metric Learning	Akurasi ±60%

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Deteksi Phishing Websit e menggunakan *Machine learning* Metode Klasifikasi Phishing Website Detection using *Machine learning* Classification	URL Dataset	Decision Tree	Akurasi > 80%
Deteksi Website Phishing Menggunakan Teknik *Machine learning*	URL Dataset	XGBoost	Akurasi > 95%
Implementasi Metode Adasyn Dalam Deteksi Url Berbahaya Menggunakan *Machine learning*: Demi Meningkatkan Keamanan Siber Di Era Digital	URL Dataset	RF + ADASYN	Akurasi 99%
Klasifikasi Deteksi Link *Phising* DANA Kaget Menggunakan Metode Support Vector Machine Berbasis Website	URL Dataset	SVM	Akurasi > 90%
Klasifikasi URL Phishing untuk SIEM: Perbandingan Model *Machine learning* XGBoost dan *Deep learning* TabNet dalam Deteksi Ancaman Siber	URL Dataset	XGBoost	Akurasi > 95%
DDoS Penerapan Random Forest dan Adaboost untuk Klasifikasi Serangan DDoS	CICDDoS2019	RF, AdaBoost	F1-score 99%
Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging	Network Traffic	RF + FS	FP turun signifikan
Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan *Machine learning*: (Metode SVM dan ANN) Comparative Study of Network Intrusion Detection Using *Machine learning*: (SVM and ANN Method)	Network Traffic	SVM, ANN	Akurasi hamper 100%
SQL Injection Detection Using *Machine learning* and Explainability	Web Dataset	Stacking vs Single	Stacking unggul
A *machine learning* based cyber security threat prediction algorithm for tourism hotels	Hospitality Data	XG-CatSec	Akurasi 97,65%
Hybrid Detection Framework Using Natural Language Processing (NLP) and Reinforcement Learning (RL) for Cross-Site Scripting (XSS) Attacks	HTTP Payload	NLP + RL	Akurasi > 96%
Detecting unknown intrusions from large heterogeneous data through ensemble learning	NSL-KDD, CICIDS	Ensemble ML	Unknown attack melonjak

4.1. *Penerapan Machine Learning untuk Meningkatkan Keamanan Aplikasi Web*

Berdasarkan analisis mendalam terhadap literatur terpilih, ditemukan bahwa Machine learning (ML) dan Deep learning (DL) tidak lagi sekadar menjadi pelengkap, melainkan komponen inti dalam arsitektur keamanan modern. Penerapannya diklasifikasikan ke dalam empat domain ancaman utama sebagai berikut:

4.1.1. *Deteksi Phishing Malware, dan Privasi Pengguna*

Serangan phishing telah berevolusi dari email spam sederhana menjadi situs web tiruan yang sangat mirip dengan aslinya. Pendekatan konvensional berbasis *Blacklist* dinilai tidak lagi efektif karena siklus hidup situs phishing yang sangat singkat.

Analisis Multi-Modal dan NLP: Alsaedi dkk. [5] memperkenalkan pendekatan inovatif "Multi-Modal" yang tidak hanya menganalisis teks URL, tetapi juga mengonversi URL menjadi representasi gambar (*image-based*) dan diproses menggunakan Convolutional Neural Network (CNN). Hal ini sejalan dengan Salim dan Lahcen [11] yang memanfaatkan model bahasa canggih (BERT dan RoBERTa) untuk menganalisis keamanan *request* pada aplikasi web dan seluler, menunjukkan bahwa pemahaman kontekstual mendalam sangat krusial untuk membedakan *request* berbahaya dari pengguna sah.

Penelitian oleh Vebriani dan Yustanti [12] mengimplementasikan Support Vector Machine (SVM) untuk mendeteksi penipuan spesifik "DANA Kaget". Mereka tidak hanya melihat URL, tetapi juga memproses struktur teks dalam tautan tersebut. Serupa dengan itu, Bambang dan Handaya [13] serta Lunak dkk [14]. mengembangkan sistem yang mengekstraksi fitur leksikal URL (seperti panjang domain, keberadaan karakter khusus, dan usia domain) untuk melatih model supervised learning agar mampu membedakan situs sah dan berbahaya secara otomatis.

Studi Kasus Penipuan Spesifik: Dewanto dkk. [6] memperluas cakupan ini dengan menganalisis modus penipuan penambah followers Instagram. Studi ini menyoroti bahwa serangan rekayasa sosial sering kali memanfaatkan psikologis pengguna, sehingga model ML dilatih untuk mendeteksi pola janji palsu pada konten halaman web.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Penanganan Ketidakseimbangan Data: Salah satu tantangan terbesar dalam deteksi phishing adalah jumlah situs aman yang jauh lebih banyak daripada situs berbahaya. Setyawan dkk. [15] mengatasi masalah ini dengan menerapkan metode ADASYN (Adaptive Synthetic Sampling Approach). Teknik ini secara sintetis menghasilkan data sampel serangan baru untuk menyeimbangkan dataset, sehingga model tidak menjadi bias dan mampu mendeteksi ancaman yang jarang muncul dengan lebih akurat.

Privasi dan Browser Fingerprinting: Di sisi privasi, Zhao [16] menyoroti ancaman pelacakan pengguna melalui *browser fingerprinting*. Ia mengembangkan pendekatan berbasis aliran data (*flow-centric*) untuk mendeteksi skrip yang mencoba mengambil sidik jari perangkat pengguna secara diam-diam, sebuah aspek keamanan yang sering terabaikan namun krusial dalam keamanan web.

4.1.2. *Mitigasi Serangan Injeksi (SQL Injection dan XSS)*

Serangan injeksi menargetkan celah pada validasi input aplikasi. Penerapan ML di sini bertujuan untuk memahami konteks dan sintaksis kode, bukan sekadar mencocokkan *string*.

Pertahanan Aktif dan Pengujian Standar: Wang dkk. [8] mengusulkan sistem pertahanan aktif bernama "*Spinner*", yang secara dinamis melakukan perturbasi (pengacakan) pada subsistem perintah. Teknik ini membuat penyerang kesulitan memprediksi struktur sistem target, sehingga serangan injeksi menjadi tidak efektif. Selain itu, [17] menekankan bahwa penerapan algoritma cerdas harus tetap didampingi oleh praktik keamanan standar OWASP untuk meminimalkan permukaan serangan.

***Deep Feature Extraction pada SQLi*:** Thalji dkk. [18] memperkenalkan arsitektur AE-Net yang berbasis Autoencoder. Berbeda dengan metode tradisional, AE-Net bekerja secara unsupervised untuk mempelajari representasi fitur mendalam dari query SQL yang normal. Ketika ada query yang menyimpang dari pola normal tersebut (anomali), sistem akan langsung menandainya sebagai serangan, bahkan jika pola serangan tersebut belum pernah dikenali sebelumnya.

***Natural Language Processing* (NLP) untuk XSS:** Abuda [19] mengusulkan pendekatan hibrida yang inovatif dengan menggabungkan NLP dan *Reinforcement Learning* (RL). Dalam skema ini, skrip berbahaya diperlakukan layaknya bahasa alami yang harus diterjemahkan dan dipahami konteksnya. Agen RL kemudian "belajar" dari interaksi dengan payload serangan untuk memperbarui kebijakan pertahanannya secara dinamis. Krishnan dkk. [20] mendukung temuan ini dengan menggunakan ensemble learning untuk mendeteksi skrip XSS yang sering kali disamarkan (obfuscated) menggunakan encoding URL yang rumit.

Validasi Eksperimental: Wiandani dkk. [7] dan Wahdana & Hanif [9] menggunakan Damn Vulnerable Web Application (DVWA) sebagai testbed. Hasil eksperimen mereka menunjukkan bahwa model ML mampu mendeteksi pola injeksi pada level parameter HTTP request dengan tingkat keberhasilan yang jauh lebih tinggi dibandingkan Web Application Firewall (WAF) berbasis aturan statis.

4.1.3. *Deteksi Serangan DDoS dan Manajemen Trafik*

Serangan Distributed Denial of Service (DDoS) memiliki karakteristik volume trafik yang masif dan tiba-tiba. ML diterapkan untuk mengklasifikasikan paket data dalam kecepatan tinggi.

Multi-Stage Framework: Polat dkk. [21] merancang kerangka kerja pembelajaran bertingkat (multi-stage learning) yang menggabungkan *Convolutional Neural Network* (CNN) untuk ekstraksi fitur otomatis dan Decision Tree untuk klasifikasi cepat. Penerapan ini dikhususkan untuk sistem SCADA berbasis *Software-Defined Networking* (SDN), di mana latensi rendah sangat krusial.

Klasifikasi Trafik *Real-time*: Fauzi dkk. [22] membandingkan algoritma *Random Forest* dan *Adaboost* untuk memisahkan trafik *flash crowd* (lonjakan pengunjung asli) dengan serangan DDoS. Hasilnya menunjukkan bahwa algoritma ensemble mampu menangani noise pada data trafik jaringan dan mencegah terjadinya false alarm yang dapat memblokir pengguna sah.

4.1.4. *Modernisasi Intrusion Detection System (IDS)*

IDS tradisional sering gagal mendeteksi serangan *zero-day*. Oleh karena itu, penelitian terbaru berfokus pada pendekatan berbasis anomali (*anomaly-based detection*).

Pendeteksian Serangan Insipien: Liu dan Patras[23] mengembangkan "NetSentry", sebuah model berbasis *Deep learning* yang dirancang untuk mendeteksi serangan jaringan berskala besar sejak tahap awal (insipien). Hal ini memungkinkan administrator jaringan untuk melakukan mitigasi sebelum serangan mencapai

p-ISSN : 2803-1507 e-ISSN : 2803-1531

puncaknya. Jemili dkk. [24] memperluas cakupan ini dengan menerapkan ensemble learning pada data heterogen skala besar, membuktikan bahwa penggabungan berbagai sumber data trafik meningkatkan akurasi deteksi intrusi yang tidak dikenal. Lozano dkk. [25] melengkapi strategi ini dengan arsitektur *Threat Hunting* berbasis ML untuk infrastruktur kritis, yang secara proaktif mencari indikator serangan tersembunyi yang mungkin lolos dari deteksi otomatis standar.

Optimasi pada IoT: Pada lingkungan *Industrial Internet of Things* (IIoT) yang memiliki keterbatasan daya komputasi, Ahmad dkk. [26] menerapkan *Deep Random Neural Network* yang bobotnya dioptimalkan menggunakan algoritma Particle Swarm Optimization (PSO). Metode ini terbukti efisien secara komputasi namun tetap handal dalam mendeteksi intrusi pada protokol komunikasi industri. dilengkapi dengan sistem notifikasi *Real-time* berbasis *cloud* yang dikembangkan oleh Riza [27]. Baklizi dkk. [28] juga memvalidasi bahwa IDS berbasis ML mampu beradaptasi dengan berbagai jenis serangan web modern.

4.2. *Performa dan Efektivitas Pendekatan Machine learning*

Bagian ini mengevaluasi kinerja model berdasarkan metrik akurasi, presisi, recall, dan efisiensi komputasi, guna menentukan algoritma yang paling efektif untuk keamanan web.

4.2.1. *Dominasi Random Forest dan XGBoost pada Data Tabular*

Berdasarkan sintesis data dari berbagai studi, algoritma berbasis pohon keputusan (tree-based) menunjukkan dominasi yang kuat dalam hal akurasi dan stabilitas.

Keunggulan Random Forest (RF): Alhamyani dan Alshammari [29] mencatat pencapaian luar biasa di mana Random Forest mencapai akurasi 99.78% dalam mendeteksi serangan XSS. Tingginya akurasi ini disebabkan oleh mekanisme bagging pada RF yang mengurangi varians dan risiko overfitting. Temuan ini diperkuat oleh Kapan dan Gunal [30] serta Chakir dkk. [31], yang menempatkan RF sebagai pengklasifikasi teratas untuk deteksi phishing dan serangan web umum karena kemampuannya menangani fitur data yang kompleks dan berdimensi tinggi.

Efisiensi XGBoost: Tjahjono dkk. [32] melakukan perbandingan head-to-head antara XGBoost dan *Deep learning* (TabNet) untuk sistem SIEM. Hasilnya mengejutkan, di mana XGBoost tidak hanya memberikan akurasi yang kompetitif, tetapi juga unggul signifikan dalam kecepatan training dan inference. Hal ini dikonfirmasi oleh penelitian Hussain dkk. [33] dan Lukito & Handaya [13] yang melaporkan akurasi hingga 96% dengan XGBoost setelah dilakukan hyperparameter tuning. Kecepatan eksekusi XGBoost menjadikannya kandidat ideal untuk sistem keamanan *Real-time*. Fan [34] turut mengembangkan algoritma "XG-CatSec" yang memadukan XGBoost dan CatBoost untuk memprediksi ancaman siber, menghasilkan prediksi yang lebih *robust* dibandingkan model tunggal.

4.2.2. *Superioritas Deep learning pada Data Kompleks dan Sekuensial*

Meskipun membutuhkan sumber daya lebih besar, *Deep learning* (DL) menjadi tak tergantikan untuk jenis data yang tidak terstruktur atau memiliki dependensi waktu yang panjang.

Fitur Agregasi: Wang[35] mengusulkan metode deteksi kebocoran *side-channel* menggunakan SSA-ResNet, yang mengoptimalkan seleksi fitur menggunakan algoritma pencarian Sparrow Search. Pendekatan ini membuktikan bahwa DL mampu menangkap kebocoran informasi halus yang tidak terlihat oleh metode statistik biasa.

***Long Short-Term Memory* (LSTM):** Farea dkk. [36] dan Ghazal & Mjlae [37] menunjukkan bahwa arsitektur LSTM dan Bi-LSTM sangat superior dalam menangani serangan berbasis injeksi kode. Kemampuan LSTM untuk "mengingat" urutan input sebelumnya memungkinkannya mendeteksi payload serangan yang terpecah atau disisipkan di antara kode yang sah, sesuatu yang sulit dilakukan oleh model tradisional seperti SVM.

***Autoencoder* dan CNN:** Baklizi dkk. [28] dan Zaman dkk. [38] membuktikan bahwa penggunaan CNN dan *Autoencoder* sangat efektif untuk ekstraksi fitur otomatis dari trafik jaringan mentah (raw traffic). Dalam studi perbandingan oleh Tan dkk. [39], Artificial Neural Network (ANN) terbukti mengungguli SVM secara signifikan ketika diuji pada dataset dengan volume besar, meskipun SVM masih kompetitif pada dataset berukuran kecil.

4.2.3. *Peran Krusial Model Hybrid dan Explainability*

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tren terbaru menunjukkan pergeseran menuju penggabungan beberapa metode untuk menutupi kelemahan masing-masing model tunggal.

***Stacking Ensemble*:** Krishnan dkk. [20] mendemonstrasikan bahwa teknik Hybrid Stacking Ensemble—yang menggabungkan prediksi dari beberapa model lemah—secara konsisten menghasilkan skor F1 yang lebih tinggi dibandingkan model individu. Ini menegaskan bahwa kolaborasi algoritma adalah strategi pertahanan paling robust.

Tantangan Interpretasi: Mahmood [40] menyoroti isu kritis mengenai "black-box" pada model DL. Ia menekankan pentingnya integrasi metode *Explainable AI* (XAI) seperti LIME atau SHAP dalam sistem deteksi *SQL Injection*. Tanpa explainability, administrator keamanan akan kesulitan memvalidasi apakah sebuah alert merupakan serangan nyata atau positif palsu, yang pada akhirnya dapat menurunkan kepercayaan terhadap sistem otomatisasi keamanan tersebut. Di sisi lain, [41] mengingatkan bahwa filter validasi input tradisional yang efektif tetap menjadi lapisan pertahanan esensial yang harus bekerja berdampingan dengan model prediksi canggih.

5. DISKUSI

Hasil *systematic literature review* memperlihatkan bahwa pendekatan *machine learning* dan *deep learning* diterapkan secara luas untuk menangani variasi ancaman pada lapisan aplikasi web, termasuk *phishing*, *SQL Injection*, *XSS*, *DDoS*, dan *intrusion detection*. Pada studi-studi yang berfokus pada deteksi *phishing*, model berbasis fitur URL dan teks menunjukkan performa tinggi ketika dikombinasikan dengan algoritma seperti Random Forest dan XGBoost, sebagaimana dilaporkan oleh [30]. Pendekatan berbasis *natural language processing* seperti BERT juga digunakan untuk memahami konteks permintaan HTTP dan payload berbahaya, yang memperluas cakupan analisis dibandingkan metode leksikal murni [11]. Variasi pendekatan ini menunjukkan bahwa karakteristik data masukan sangat memengaruhi pemilihan model deteksi ancaman.

Pada ancaman injeksi, terutama *SQL Injection* dan *XSS*, model *deep learning* cenderung digunakan untuk menangkap pola sintaksis dan struktur payload yang kompleks. Autoencoder pada AE-Net digunakan untuk mempelajari representasi query normal sehingga anomali dapat diidentifikasi meskipun pola serangan belum pernah muncul sebelumnya [18]. Pendekatan hibrida yang menggabungkan *natural language processing* dan *reinforcement learning* juga digunakan untuk memahami konteks skrip berbahaya pada serangan *XSS* [19]. Hasil-hasil ini memperlihatkan perbedaan dengan pendekatan *rule-based* atau *signature-based* yang bergantung pada pola statis dan lebih rentan terhadap teknik *obfuscation* [41].

Untuk serangan *DDoS* dan intrusi jaringan, algoritma berbasis *ensemble* dan *deep learning* banyak digunakan karena mampu memproses trafik berukuran besar dan bersifat sekuensial. Model seperti CNN dan LSTM diterapkan untuk mengekstraksi fitur otomatis dari trafik jaringan dan mendeteksi pola serangan sejak tahap awal [21], [23]. Random Forest dan AdaBoost juga digunakan untuk membedakan lonjakan trafik sah dan serangan *DDoS*, dengan penekanan pada pengurangan *false positive* [22]. Temuan ini memperkuat hasil penelitian sebelumnya yang menyatakan bahwa pendekatan berbasis pohon keputusan stabil pada data tabular, sementara model sekuensial lebih sesuai untuk data berbasis waktu [31], [37].

Dari sisi evaluasi performa, algoritma Random Forest dan XGBoost secara konsisten dilaporkan memiliki akurasi tinggi pada berbagai dataset URL dan trafik web, dengan nilai akurasi yang sering berada di atas 95% [29], [32], [33]. Model *deep learning* seperti CNN, LSTM, dan Autoencoder menunjukkan keunggulan pada data kompleks, meskipun membutuhkan sumber daya komputasi yang lebih besar [35], [36]. Model *hybrid* dan *stacking ensemble* digunakan untuk mengombinasikan kelebihan beberapa algoritma dan menghasilkan skor F1 yang lebih stabil pada berbagai skenario serangan [20]. Keterbatasan yang muncul dalam studi-studi tersebut berkaitan dengan ketergantungan pada dataset publik, variasi metrik evaluasi, serta perbedaan lingkungan pengujian yang dapat memengaruhi perbandingan performa antarpenelitian.

6. KESIMPULAN DAN SARAN

6.1. *Kesimpulan*

Tinjauan sistematis terhadap seluruh artikel yang dianalisis menunjukkan bahwa pemanfaatan *machine learning* memiliki peran yang sangat penting dalam meningkatkan keamanan aplikasi web. Berbagai model ML mampu mengidentifikasi beragam bentuk ancaman mulai dari *Phising*, URL berbahaya, serangan DDoS, sehingga injeksi SQL, XSS, serta intrusi jaringan. Beragam algoritma mulai dari SVM, *Random Forest*,

p-ISSN : 2803-1507 e-ISSN : 2803-1531

XGBoost, CNN, LSTM, hingga model hybrid menunjukkan kinerja yang unggul, baik dalam meningkatkan akurasi deteksi maupun dalam menekan tingkat kesalahan prediksi. Efektivitas tersebut turut diperkuat oleh teknik pendukung seperti feature selection, ADASYN, dan pemrosesan bahasa alami. Secara keseluruhan, hasil kajian ini menegaskan bahwa pendekatan berbasis *machine learning* tidak hanya memberikan peningkatan performa deteksi, tetapi juga menyediakan kemampuan adaptif terhadap pola serangan baru, sehingga menjadi landasan penting bagi pengembangan sistem keamanan aplikasi web yang lebih cerdas, responsif, dan berkelanjutan.

6.2. *Saran*

6.2.1. *Saran Bagi Peneliti Selanjutnya*

1. Penelitian lanjutan disarankan untuk lebih banyak menggunakan dataset yang benar-benar merepresentasikan trafik aplikasi web modern, misalnya yang mencakup API-based *traffic*, *microservices*, serta pola serangan terkini seperti account takeover dan abuse pada autentikasi multi-faktor.
2. Banyak studi yang berfokus pada akurasi, *precision*, atau *recall*, namun masih minim membahas aspek *explainability* dan *robustness* terhadap *adversarial attack*. Oleh karena itu, penelitian ke depan sebaiknya mengintegrasikan pendekatan *Explainable AI* (XAI) dan pengujian ketahanan model terhadap manipulasi input.
3. Diperlukan lebih banyak eksperimen yang memadukan model ML dengan praktik OWASP (*logging*, sanitasi input, *rate limiting*, dsb.), sehingga diperoleh gambaran yang lebih realistis tentang bagaimana model bekerja di atas fondasi kontrol keamanan tradisional, bukan hanya di lingkungan simulasi.

6.2.2. *Saran Bagi Praktisi dan Pengembang Sistem*

1. Pengembang dan tim keamanan disarankan untuk tidak hanya mengejar akurasi deteksi yang tinggi, tetapi juga mempertimbangkan keseimbangan antara deteksi dan False Positive agar sistem dapat dioperasikan secara berkelanjutan tanpa membebani tim operasi keamanan.
2. Penerapan model ML di lingkungan produksi sebaiknya dilakukan secara bertahap melalui pendekatan offline evaluation → shadow mode → full deployment, agar dampak terhadap kinerja aplikasi web dan pengalaman pengguna dapat dipantau dan dioptimalkan.

DAFTAR PUSTAKA

[1] D. Mairaj Inamdar and S. Gupta, "A Survey on Web Application Security," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3307, pp. 223–228, 2020, doi: 10.32628/cseit206543.

[2] S. Soni, "Survey on Machine Learning Techniques Used for Information Security," in *Proceedings of the International Conference on Emerging Trends in Artificial Intelligence and Smart Systems (THEETAS 2022)*, Jabalpur, India, 2022, doi: 10.4108/eai.16-4-2022.2318143.

[3] A. G. Pongoh, R. A. Fahreza, B. Al Kindi, F. S. Pribadi, and R. A. Aprilianto, "Systematic Literature Review (SLR): Dampak Pemanfaatan Artificial Intelligence untuk Meningkatkan Cyber Security," *Cyber Security dan Forensik Digital*, vol. 7, no. 1, pp. 34–41, 2024, doi: 10.14421/csecurity.2024.7.1.4486.

[4] R. L. Alaoui and E. H. Nfaoui, "Deep Learning for Vulnerability and Attack Detection on Web Applications: A Systematic Literature Review," *Future Internet*, vol. 14, no. 4, p. 118, 2022, doi: 10.3390/fi14040118.

[5] M. Alsaedi, F. A. Ghaleb, F. Saeed, J. Ahmad, and M. Alasli, "Multi-Modal Features Representation-Based Convolutional Neural Network Model for Malicious Website Detection," *IEEE Access*, vol. 12, no. December 2023, pp. 7271–7284, 2024, doi: 10.1109/access.2023.3348071.

[6] M. A. B. Dewanto, M. Fathurrahman, D. R. Firdaus, and A. Setiawan, "Penipuan Penambah Followers Instagram: Analisis Serangan Phising dan Dampaknya pada Keamanan Data," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/pjise.v1i4.2672.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[7] R. S. Wiandani, M. Tahir, I. A. Dyransyha, and R. Ummah, "Identifikasi Serangan *SQL Injection* Berbantuan Aplikasi Pengujian Keamanan Web DVWA (Damn Vulnerable Web Application)," *Digital Transformation Technology*, vol. 5, no. 1, pp. 375–382, 2025, doi: 10.47709/digitech.v5i1.5922.

[8] M. Wang, C. Jung, A. Ahad, and Y. Kwon, "Spinner: Automated Dynamic Command Subsystem Perturbation," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 1839–1860, 2021, doi: 10.1145/3460120.3484577.

[9] W. Wahdana and K. H. Hanif, "Implementasi Keamanan Informasi Menggunakan Metode Web Application Firewall terhadap Serangan *SQL Injection*," *Jurnal Informatika Polinema*, vol. 11, no. 4, pp. 399–406, 2025, doi: 10.33795/jip.v11i4.7376.

[10] A. W. Kuncoro and F. Rahma, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," *Automata*, vol. 3, no. 1, pp. 1–5, 2021. [Online]. Available: https://journal.uii.ac.id/automata/article/view/21893

[11] S. Salim and O. Lahcen, "A BERT-Enhanced Exploration of Web and Mobile Request Safety Through Advanced NLP Models and Hybrid Architectures," *IEEE Access*, vol. 12, no. April, pp. 76180–76193, 2024, doi: 10.1109/access.2024.3406413.

[12] M. Vebriani and W. Yustanti, "Klasifikasi Deteksi Link *Phising* DANA Kaget Menggunakan Metode Support Vector Machine Berbasis Website," *Journal of Informatics and Computer Science (JINACS)*, vol. 6, no. 02, pp. 408–416, 2024, doi: 10.26740/jinacs.v6n02.p408-416.

[13] L. Lukito and W. B. T. Handaya, "Deteksi Website Phishing Menggunakan Teknik Machine Learning," *Jurnal Informatika Atma Jogja*, vol. 6, no. 1, pp. 69–80, 2025, doi: 10.24002/jiaj.v6i1.11538.

[14] A. F. Mahmud and S. Wirawan, "Deteksi Phishing Website Menggunakan Machine Learning Metode Klasifikasi," *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 4, pp. 1368–1380, 2024. [Online]. Available: https://sistemasi.ftik.unisi.ac.id/index.php/stmsi/article/view/3456

[15] G. D. Setyawan, A. Yuswanto, A. M. Ridwan, B. Wibowo, and M. Firmansyah, "Implementasi Metode Adasyn dalam Deteksi URL Berbahaya Menggunakan Machine Learning: Demi Meningkatkan Keamanan Siber di Era Digital," *TEKNOKOM: Jurnal Teknologi dan Rekayasa Sistem Komputer*, vol. 6, no. 2, pp. 123–126, 2023, doi: 10.31943/teknokom.v6i2.153.

[16] R. Zhao, "Toward the Flow-Centric Detection of Browser Fingerprinting," *Computers & Security*, vol. 137, p. 103642, 2024, doi: 10.1016/j.cose.2023.103642.

[17] M. Nawrocki and J. Kołodziej, "Vulnerabilities of Web Applications: Good Practices and New Trends," *Applied Cybersecurity and Internet Governance*, vol. 3, no. 2, pp. 122–143, 2024, doi: 10.60097/acig/199521.

[18] N. Thalji, A. Raza, M. S. Islam, N. A. Samee, and M. M. Jamjoom, "AE-Net: Novel Autoencoder-Based Deep Features for SQL Injection Attack Detection," *IEEE Access*, vol. 11, pp. 135507–135516, 2023, doi: 10.1109/access.2023.3337645.

[19] C. J. P. Abuda, "Hybrid Detection Framework Using Natural Language Processing (NLP) and Reinforcement Learning (RL) for Cross-Site Scripting (XSS) Attacks," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 6, pp. 736–747, 2025, doi: 10.14569/ijacsa.2025.0160673.

[20] M. Krishnan, Y. Lim, S. Perumal, and G. Palanisamy, "Detection and Defending the XSS Attack Using Novel Hybrid Stacking Ensemble Learning-Based DNN Approach," *Digital Communications and Networks*, vol. 10, no. 3, pp. 716–727, 2024, doi: 10.1016/j.dcan.2022.09.024.

[21] O. Polat, M. Türkoğlu, H. Polat, S. Oyucu, H. Üzen, F. Yardımcı, and A. Aksöz, "Multi-Stage Learning Framework Using Convolutional Neural Network and Decision Tree-Based Classification for Detection of DDoS Pandemic Attacks in SDN-Based SCADA Systems," *Sensors*, vol. 24, no. 3, p. 1040, 2024, doi: 10.3390/s24031040.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[22] A. Fauzi, E. Utami, and A. D. Hartanto, "DDoS Penerapan Random Forest dan Adaboost untuk Klasifikasi Serangan DDoS," *Journal on Education*, vol. 5, no. 3, pp. 7925–7937, 2023, doi: 10.31004/joe.v5i3.1920.

[23] H. Liu and P. Patras, "NetSentry: A Deep Learning Approach to Detecting Incipient Large-Scale Network Attacks," *Comput Commun*, vol. 191, pp. 119–132, 2022, doi: 10.1016/j.comcom.2022.04.020.

[24] F. Jemili, K. Jouini, and O. Korbaa, "Detecting Unknown Intrusions from Large Heterogeneous Data Through Ensemble Learning," *Intelligent Systems with Applications*, vol. 25, p. 200465, 2025, doi: 10.1016/j.iswa.2024.200465.

[25] M. Lozano, I. Pérez-Llopis, and M. Esteve Domingo, "Threat Hunting Architecture Using a *Machine learning* Approach for Critical Infrastructures Protection," *Big Data and Cognitive Computing*, vol. 7, no. 2, p. 65, 2023, doi: 10.3390/bdcc7020065.

[26] J. Ahmad, S. A. Shah, S. Latif, F. Ahmed, Z. Zou, and N. Pitropakis, "DRaNN_PSO: A Deep Random Neural Network with Particle Swarm Optimization for Intrusion Detection in the Industrial Internet of Things," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8112–8121, 2022, doi: 10.1016/j.jksuci.2022.07.023.

[27] F. Riza, "Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging," *Jurnal Sistim Informasi dan Teknologi*, vol. 5, pp. 7–9, 2022, doi: 10.37034/jsisfotek.v5i1.161.

[28] M. K. Baklizi *et al.*, "Web Attack Intrusion Detection System Using Machine Learning Techniques," *International Journal of Online and Biomedical Engineering*, vol. 20, no. 3, pp. 24–38, 2024, doi: 10.3991/ijoe.v20i03.45249.

[29] R. Alhamyani and M. Alshammari, "Machine Learning-Driven Detection of Cross-Site Scripting Attacks," *Information (Switzerland)*, vol. 15, no. 7, p. 420, 2024, doi: 10.3390/info15070420.

[30] S. Kapan and E. Sora Gunal, "Improved Phishing Attack Detection with Machine Learning: A Comprehensive Evaluation of Classifiers and Features," *Applied Sciences (Switzerland)*, vol. 13, no. 24, p. 13269, 2023, doi: 10.3390/app132413269.

[31] O. Chakir *et al.*, "An Empirical Assessment of Ensemble Methods and Traditional Machine Learning Techniques for Web-Based Attack Detection in Industry 5.0," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 3, pp. 103–119, 2023, doi: 10.1016/j.jksuci.2023.02.009.

[32] A. F. Tjahjono, H. Hasan, R. P. Putera, D. M. P. Indranto, and A. T. Hermawan, "Klasifikasi URL Phishing untuk SIEM: Perbandingan Model Machine Learning XGBoost dan Deep Learning TabNet dalam Deteksi Ancaman Siber," *Sains Data Jurnal Studi Matematika dan Teknologi*, vol. 3, no. 2, pp. 62–71, 2025, doi: 10.52620/sainsdata.v3i2.227.

[33] S. Hussain *et al.*, "Optimizing Malicious Website Prediction: An Advanced XGBoost-Based Machine Learning Model," *Nonlinear Engineering*, vol. 14, no. 1, p. 20240069, 2025, doi: 10.1515/nleng-2024-0069.

[34] D. Fan, "A Machine Learning Based Cyber Security Threat Prediction Algorithm for Tourism Hotels," *International Journal of Information and Communication Technology*, vol. 1, no. 1, pp. 89-103, 2025, doi: 10.1504/ijict.2025.10070773.

[35] J. Wang, "Research on Deep Learning and Feature Aggregation Techniques for Web Security," *Journal of Web Engineering*, vol. 24, no. 2, pp. 291–316, 2025, doi: 10.13052/jwe1540-9589.2426.

[36] A. A. R. Farea *et al.*, "Injections Attacks Efficient and Secure Techniques Based on Bidirectional Long Short Time Memory Model," *Computers, Materials and Continua*, vol. 76, no. 3, pp. 3605–3662, 2023, doi: 10.32604/cmc.2023.040121.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[37] S. F. Ghazal and S. A. Mjlae, "Cybersecurity in Deep Learning Techniques: Detecting Network Attacks," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 11, pp. 221–230, 2022, doi: 10.14569/ijacsa.2022.0131125.

[38] M. Zaman, D. Upadhyay, and C.-H. Lung, "Validation of a Machine Learning-Based IDS Design Framework Using ORNL Datasets for Power System with SCADA," *IEEE Access*, vol. 11, pp. 118414–118426, 2023, doi: 10.1109/access.2023.3326751.

[39] T. Tan, H. Sama, G. Wijaya, and O. E. Aboagye, "Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning: (Metode SVM dan ANN) Comparative Study of Network Intrusion Detection Using *Machine learning*: (SVM and ANN Method)," *Jurnal Teknologi dan Informasi (JATI)*, vol. 13, no. 2, pp. 152–164, 2023, doi: 10.34010/jati.v13i2.

[40] S. S. Mahmood, "*SQL Injection* Detection Using Machine Learning and Explainability," *Journal of Internet Services and Information Security*, vol. 15, no. 2, pp. 309–324, 2025, doi: 10.58346/jisis.2025.i2.022.

[41] S. Ibarra-Fiallos, J. B. Higuera, M. Intriago-Pazmino, J. R. B. Higuera, J. A. S. Montalvo, and J. Cubo, "Effective Filter for Common Injection Attacks in Online Web Applications," *IEEE Access*, vol. 9, pp. 10378–10391, 2021, doi: 10.1109/access.2021.3050566.