JEENI: Journal of Electrical Engineering and Informatics
Homepage: https://journal.unm.ac.id/index.php/jeeni
Email: jtei@unm.ac.id

e-ISSN: 3025-213X
Jeeni, Vol. 3, No. 2, February 2026
Page 42-47

Literature Review: The Application of Deep Learning in Web Attack Detection

Sapuan[1*],
[1]Information Technology Study Program, Ar-Raniry State Islamic University, Aceh, Indonesia

ARTICLE INFO

Article history:
Submitted: April 12, 2026
Final Revised: April 28
Accepted: May 01, 2026
Published: May 02, 2026

Keywords:
Deep Learning; Web Attack Detection; Web Security; Machine Learning; Cybersecurity.

ABSTRACT

This study is motivated by the increasing need for web security systems, the rapid development of web-based applications, and the rise in cyber threats, such as cross-site scripting (XSS), SQL injection (SQLi), and HTTP manipulation. This study reviews the application of deep learning methods in web attack detection with a focus on frequently used algorithms, model performance, and challenges faced. This study uses a systematic literature review approach by analyzing various relevant scientific publications. Data were collected from reliable literature sources and analyzed qualitatively to identify patterns, methods, and research gaps. The results indicate that convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) algorithms are the most widely used methods and exhibit good performance in detecting web attacks. However, several obstacles remain, such as limited representative datasets, data imbalance, and high computational requirements. This study contributes in the form of a comprehensive synthesis of the application of deep learning in web security and identifies research gaps and development opportunities to improve model effectiveness and efficiency, particularly in the implementation of real-time attack detection.

Doi: https://doi.org/10.59562/jeeni.v3i2.12206

Introduction

The rapid advancement of web technologies and the increasing use of internet-based services have made web applications a critical component across various sectors, including electronic commerce (e-commerce), digital banking, education, and e-government services. The high level of dependency on web applications makes system security crucial for ensuring the continuity and reliability of digital services. However, the growing complexity of systems and interactions among network components has also expanded the potential vulnerabilities to various types of cyberattacks. Common attacks targeting web applications include cross-site scripting (XSS), SQL injection (SQLi), and hypertext transfer protocol (HTTP) request manipulation, which may lead to data breaches and service disruptions [1], [2].

In practice, various traditional security mechanisms have been implemented to protect web applications from cyber threats, such as rule-based systems and signature-based detection approaches. These methods operate by identifying known attack patterns based on predefined rules. Although effective in detecting previously identified threats, these approaches have limitations in recognizing new and evolving attack patterns. Consequently, traditional security systems tend to be less adaptive in addressing the dynamic nature of modern cyberattacks [3], [4].

Recent studies have explored the use of artificial intelligence-based approaches, particularly machine learning (ML) and deep learning (DL), to overcome the limitations of existing methods for attack detection. These approaches enable systems to learn patterns from network traffic data and attack behaviors, thereby enabling the automatic identification of suspicious activities. Owing to their data-driven learning capabilities, ML and DL methods are considered more adaptive than traditional approaches, as they can detect previously unseen attack patterns [5], [6], [7].

Despite the promising potential of machine learning and deep learning in enhancing web attack detection systems, several challenges remain in their implementation. These challenges include the lack of representative datasets that reflect recent attack patterns, class imbalance issues, and the high computational resources required, especially for complex deep learning architectures. These limitations indicate that further research is needed to improve the effectiveness and efficiency of AI-based web attack detection systems [8, 9].

To ensure the sustainability of research development in this field, a comprehensive research mapping is necessary to avoid redundancy and resource inefficiency. Moreover, collaborative efforts are needed to identify research priorities that align with the evolving landscape of cyber threats. Therefore, a literature review that not only provides a narrative overview but also evaluates studies using a systematic methodological framework is essential. This study aims to map the development and identify the challenges in the application of deep learning for web-attack detection. The method used is a systematic literature review of scientific publications sourced from major academic databases, such as Google Scholar, IEEE Xplore, and Scopus [10, 11].

Materials and Methods

This study employs a systematic literature review (SLR) method to analyze the application of deep learning in detecting web attacks. The approach is qualitative in nature and emphasizes the stages of identification, selection, and systematic evaluation of relevant literature in a structured manner [10], [12]. The review process follows the guidelines of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses to ensure transparency and validity of the research

findings [5]. The selected studies are assessed descriptively using performance metrics such as accuracy, precision, recall, and F1-score, along with an analysis of the reported challenges [8], [6]. Through this approach, the study aims to provide a comprehensive overview of algorithm trends, model performance, and key issues in the application of deep learning for web attack detection.

A. Selection Criteria and Research Framework

To ensure a systematic and relevant selection of the literature, this study adopts the PICOC (population, intervention, comparison, outcome, and context) framework in defining the selection criteria [10]. The PICOC framework applied in this study is presented in Table 1.

Table 1. Methodological Framework for Research Questions

Element	Description
Population (P)	Studies discussing web attack detection in web applications using Deep Learning methods
Intervention (I)	Implementation of Machine Learning and Deep Learning algorithms such as CNN, LSTM, Random Forest, and SVM
Comparison (C)	Comparison between algorithms or with traditional methods such as rule-based detection
Outcome (O)	Performance evaluation metrics such as accuracy, precision, recall, and F1-score
Context (C)	Studies published in scientific journals or conference proceedings in the field of cybersecurity

To clarify the focus of this study, three research questions (RQ1, RQ2, and RQ3) were formulated as the basis for the analysis. First, this study identifies the most commonly used deep learning algorithms in web attack detection (RQ1). Second, it evaluates the performance of deep learning algorithms based on the metrics reported in previous studies (RQ2). Third, by analyzing the limitations of existing studies, this research identifies the challenges in implementing deep learning for web attack detection systems, as well as future research opportunities (RQ3).

Furthermore, to ensure the quality and relevance of the study, only articles that meet the inclusion criteria are considered. These include empirical studies published in scientific journals or conference proceedings, written in Indonesian or English, and available in full text. Conversely, articles are excluded if they are not relevant to the topic, lack full-text access, are not empirical in nature, or fall outside the defined study period.

Table 2. Literature Selection Criteria

Criteria	Inclusion (In Scope)	Exclusion (Out of Scope)
Type of Study	Empirical studies related to web attack detection	Review or theoretical articles
Language	Indonesian or English	Other languages
Topic	Deep Learning for web attack detection	Not related to web security
Access	Full-text available	Full-text not available
Output	Includes performance metrics	Does not include evaluation

B. Literature Search Strategy

A literature search strategy was adopted to identify studies relevant to deep learning-based web attack detection. The search was performed across several major academic databases, including Google Scholar, IEEE Xplore, Scopus, and SpringerLink [10], [5]. The keywords used in the search process included "web attack detection," "web security," "deep learning," and "intrusion detection system." These keywords were combined using Boolean operators such as AND and OR to obtain more specific and relevant search results. This strategy was designed to capture the literature that addresses the research objectives, particularly those related to algorithms, model performance, and challenges in web attack detection [8], [7].

C. Selection Process

The literature selection process in this study follows the PRISMA methodology, which consists of four main stages: identification, screening, eligibility, and inclusion [5]. In the identification stage, articles were collected from predefined databases. The screening stage involved removing duplicate articles and filtering them based on their title and abstract. During the eligibility stage, the remaining articles were assessed according to predefined inclusion and exclusion criteria. The final stage refers to the selection of articles that met all the criteria and were deemed suitable for further analysis. This systematic process ensured that the selected literature maintained a high level of quality and relevance in accordance with the research objectives [10].

D. Data Extraction and Synthesis

After the selection was made, data extraction and synthesis were conducted to collect and analyze information from each selected study. The extracted data included: (1) study identification (author and year), (2) the deep learning algorithms used, (3) types of web attacks analyzed, (4) datasets employed, (5) evaluation methods and performance metrics, such as accuracy, precision, recall, and F1-score, and (6) key findings and research limitations [8], [6].

The collected data were analyzed using qualitative and descriptive approaches. Qualitative analysis was applied to identify trends in commonly used algorithms and frequently studied attack types, thereby addressing RQ1. Descriptive analysis was used to compare model performance based on reported evaluation metrics, thereby addressing RQ2. Additionally, data synthesis was conducted to identify challenges and limitations in previous studies, thereby addressing

RQ3 [8],[9]. Through this process, the study provides a comprehensive overview of the development, performance, and challenges in the application of deep learning to web attack detection.

Results

This section presents a systematic review of the literature related to the application of deep learning in web attack detection, with the main findings summarized in the results table (Table 3). Through the data synthesis conducted, this section aims to address the research questions (RQ) formulated in the previous section.

RQ1: Deep Learning Algorithms in Web Attack Detection

Based on the literature review, the use of deep learning (DL) algorithms for detecting web attacks has shown an increasing trend in recent years [8], [7]. The most commonly applied algorithms include convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks [5], [6]. CNN models are widely utilized because of their ability to automatically extract features from input data, particularly text-based data, such as HTTP logs and attack payloads. In contrast, RNNs and LSTMs are more suitable for handling sequential data, such as network traffic, because of their capability to capture temporal dependencies [5], [29]. In addition to single-model approaches, several studies have developed hybrid models by combining DL with traditional machine learning (ML) algorithms, such as random forest and support vector machine (SVM). These approaches have demonstrated improved performance in several studies, particularly in enhancing detection accuracy and reducing classification errors [27].

RQ2: Performance of Deep Learning Algorithms

The performance of deep learning algorithms in web attack detection is generally evaluated using metrics such as accuracy, precision, recall, and the F1-score. Based on the literature analysis, most deep learning models demonstrate high performance, with accuracy values typically exceeding 90% [5], [6], [7]. CNN models tend to perform well in detecting payload-based attack patterns, while LSTM shows better performance in analyzing sequential data. Additionally, hybrid models that combine multiple algorithms have demonstrated improvements in precision and recall, thereby reducing false positives and false negatives [27]. However, performance variations across studies remain significant. These differences are influenced by several factors, including the type of dataset used, preprocessing techniques, and evaluation methods applied [8], [9]. Therefore, model performance is not solely determined by the algorithm but also by data quality and data processing approaches.

RQ3: Challenges in Applying Deep Learning for Web Attack Detection

Despite the promising potential of deep learning, several challenges remain in its implementation for web attack detection systems [8], [7]. One of the primary challenges is the lack of representative datasets that reflect the latest attack patterns. Many studies still rely on outdated datasets that do not fully represent current cyber threat conditions [9]. In addition, class imbalance is a major issue in which the number of normal data instances significantly exceeds that of attack data. This imbalance can negatively affect the model's ability to accurately detect attacks [15].

Another challenge is the high computational cost required, particularly for complex deep learning architectures, which makes real-time implementation difficult [6], [18]. Furthermore, model interpretability is also a concern, as deep learning models are often considered black boxes, making it difficult to explain the prediction results transparently [8]. Considering these challenges, further research is needed to improve the effectiveness and efficiency of deep learning models, particularly in terms of developing more representative datasets, optimizing model performance, and enhancing transparency in the decision-making process [8], [7].

Table 3. Summary of Deep Learning-Based Web Attack Detection Literature

Nu.	Study	Database	Attack Type	Model / Architecture	Metrics	Dataset	Key Findings
1	Alghofaili et al. [1]	Scopus	General Web Attacks	CNN, LSTM, DNN	Accuracy, F1-Score	CICIDS2017	No universally best model
2	J. Park & Y. Park [9]	IEEE	SQL Injection, XSS	LSTM, DNN	Accuracy, Precision	CSIC 2010 HTTP Dataset	LSTM excels on sequential data
3	S. Husain [25]	Springer	Web Attack	CNN, LSTM, Transformer	Accuracy, Recall	UNSW-NB15	Model combination improves accuracy
4	M. Alashjaee [11]	Nature	Intrusion Detection	CNN-LSTM + Attention	Accuracy, F1-Score	CICIDS2018	Hybrid model is highly effective
5	Shivani et al. [27]	Google Scholar	Web Attack	End-to-End DL	Accuracy	CSIC HTTP Dataset	Adaptive to new attacks
6	N. Rahmeisi et al. [16]	Google Scholar	Web Attack	CNN, LSTM, SVM	Accuracy, F1-Score	NSL-KDD	CNN & LSTM are most popular

Nu.	Study	Database	Attack Type	Model / Architecture	Metrics	Dataset	Key Findings
7	X. Zhou et al. [29]	Scopus	Web Attack	DL + Uncertainty	Accuracy	CICIDS2017	Improves model confidence
8	W. Shi & J. Dong [28]	IEEE	Adversarial Attack	Deep Neural Network	Accuracy	UNSW-NB15	Vulnerable to adversarial attacks
9	A. Salam et al. [3]	MDPI	Web Attack	Deep Learning	Accuracy, Recall	UNSW-NB15	Effective in modern systems
10	S. Chaganti et al. [24]	Springer	Intrusion Detection	LSTM	Precision, Recall	NSL-KDD	More adaptive than rule-based methods
11	P. Kumar et al. [19]	ScienceDirect	Web Attack	ANN, CNN, RNN	Accuracy	KDD Cup 99	DL improves detection performance
12	O. K. Sahingoz et al. [17]	ScienceDirect	Web Attack	CNN Hybrid	Accuracy, F1-Score	HTTP Dataset	Suitable for real-time detection
13	R. Lamrani Alaoui & E. H. Nfaoui [21]	MDPI	Web Attack	Deep Learning (Review)	F1-Score	Various Datasets	DL outperforms traditional methods
14	IDS Study [8]	IEEE	Intrusion Detection	Deep Neural Network	Accuracy	NSL-KDD	Issue: class imbalance
15	G. Kim et al. [7]	IEEE	Web Attack	CNN-Based Detection	Accuracy, Precision	HTTP Traffic Dataset	CNN effective for payload-based detection

Discussion

The results of the literature review indicate that the application of Deep Learning in web attack detection has experienced significant development in recent years. These findings are consistent with various recent studies (2020–2025), which report that algorithms such as Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and Long Short-Term Memory (LSTM) dominate data-driven approaches for detecting attack patterns. In addition, several recent studies highlight the effectiveness of hybrid approaches that combine Deep Learning with conventional Machine Learning methods to improve accuracy and enhance model robustness against diverse attack variations.

In terms of performance, most studies report high accuracy levels, generally exceeding 90%, with evaluations conducted using metrics such as accuracy, precision, recall, and the F1-score. These results reinforce previous findings that deep learning has a strong capability to automatically extract complex features. However, these outcomes are also aligned with recent studies indicating that model performance is highly dependent on dataset quality, preprocessing techniques, and the evaluation strategies employed. In addition, recent studies have emphasized several unresolved challenges, including the lack of representative datasets reflecting the latest attack patterns, class imbalance issues, high computational requirements, and limited model interpretability. These findings highlight existing research gaps that require further investigation, particularly in developing more efficient, transparent, and real-time-capable models.

Conclusions

This study concludes that deep learning is an effective and adaptive approach for detecting web attacks and is capable of overcoming the limitations of traditional rule-based security methods. This research successfully addresses existing gaps by providing a comprehensive synthesis of commonly used algorithms, model performance, and key challenges in their implementation. The novelty of this study lies in the integrated analysis of recent studies to identify patterns in algorithm usage, factors influencing model performance, and potential directions for future development. The contribution of this research is not only theoretical, in enriching the existing body of literature, but also practical, by offering insights that can serve as a foundation for developing more effective, efficient, and real-time web attack detection systems.

Acknowledgement

The authors express their sincere gratitude to all parties who contributed to the literature collection, data analysis, and completion of this research. Appreciation is also extended to the institutions that provided access to various scientific references, which greatly supported the successful completion of this study.

References

[1] A. Seeam, C. Tachtatzis, and S. Member, 'A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion', vol. 4, pp. 1–28, 2017.
[2] A. Informations, 'Machine Learning and Deep Learning Approaches for SQL Injection Detection : A Review', vol. 4, pp. 1–17, 2025.
[3] S. Silakari, 'An Ensemble Approach for Cyber Attack Detection System : A Generic Framework'.
[4] G. Betarte and R. Mart, 'Web Application Attacks Detection Using Machine Learning Techniques', pp. 1–8.
[5] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and P. Group, 'Preferred reporting items for systematic reviews and meta-analyses : the PRISMA statement', vol. 2535, no. July, pp. 1–8, 2009, doi: 10.1136/bmj.b2535.
[6] K. Singh, '1D-CNN based Model for Classification and Analysis of Network Attacks', vol. 12, no. 11, pp. 604–613, 2021.
[7] F. M. Aswad, A. Mohammed, S. Ahmed, N. Ali, and M. Alhammadi, 'Deep learning in distributed denial - of - service attacks detection method for Internet of Things networks', 2023.
[8] B. R. Dawadi, B. Adhikari, and D. K. Srivastava, 'Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks †', pp. 1–16, 2023.
[9] J. Pendidikan, N. Mulyana, R. Nursiaga, T. S. Ali, and I. Santoso, 'Model Konseptual Arsitektur Pertahanan Diri Adaptif Berbasis RASP dan MAPE-K untuk Aplikasi Web Jurnal Pendidikan Sains dan Komputer', vol. 5, no. 02, pp. 307–318, 2025.
[10] M. S. Albulayhi and D. M. Ibrahim, 'IS e C ure', 2021, doi: 10.22042/ISECURE.2021.0.0.0.
[11] A. Alharthi, M. Alaryani, and S. Kaddoura, 'A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems', vol. 26, no. February, 2025.
[12] R. L. Alaoui, 'Deep Learning for Vulnerability and Attack Detection on Web Applications : A Systematic Literature Review', 2022.
[13] D. T. T. Hien and P. Van Hau, 'Enhancing Web Application Security: A Deep Learning and NLP-based Approach for Accurate Attack Detection', *J. Sci. Technol. Inf. Secur.*, no. 3, pp. 77–87, 2023, doi: 10.54654/isj.v3i20.1008.
[14] N. Montes, G. Betarte, R. Martínez, and A. Pardo, 'Web Application Attacks Detection Using Deep Learning', *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12702 LNCS, pp. 227–236, 2021, doi: 10.1007/978-3-030-93420-0_22.
[15] R. Yuranda and E. S. Negara, 'Application of Deep Learning Algorithm for Web Shell Detection in Web Application Security System', vol. 13, pp. 330–336, 2024.
[16] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, 'An optimized LSTM-based deep learning model for anomaly network intrusion detection', *Sci. Rep.*, vol. 15, no. 1, pp. 1–21, 2025, doi: 10.1038/s41598-025-85248-z.
[17] T. V. Vishnu Kumar, A. John, M. Vighnesh, and M. Jagannath, 'Social distance monitoring system using deep learning and entry control system for commercial application', *Mater. Today Proc.*, vol. 62, pp. 4605–4611, 2022, doi: 10.1016/j.matpr.2022.03.077.
[18] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. Aboras, and N. Gowtham, 'An optimized LSTM-based deep learning model for anomaly network intrusion detection', pp. 1–21, 2025.
[19] S. Kitchenham, B., & Charters, 'Guidelines for performing systematic literature reviews in software engineering', *Tech. report, Ver. 2.3 EBSE Tech. Report. EBSE*, no. January 2007, pp. 1–57, 2007.
[20] V. G. Thamaraiselvi, 'International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)', *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 14, no. 4, 2025, doi: 10.15680/ijirset.2025.1412112.
[21] M. S. Sahira, R. Indriati, and A. Ristyawan, 'Analisis Risiko Website Sistem Keamanan Informasi Menggunakan Metode Fmea dan Framework ISO/IEC 27002:2022', *JSITIK J. Sist. Inf. dan Teknol. Inf. Komput.*, vol. 3, no. 2, pp. 128–138, 2025, doi: 10.53624/jsitik.v3i2.722.
[22] Y. Zhou, H. Zhu, Y. Chai, Y. Liu, Y. Jiang, and Y. Qian, 'Toward trustworthy web attack detection: An uncertainty-aware ensemble deep kernel learning model', *Inf. Manag.*, vol. 63, no. 4, pp. 1–22, 2026, doi: 10.1016/j.im.2026.104325.
[23] L. N. Alghofaili and D. M. Ibrahim, 'Web-Based Attacks Detection Using Deep Learning Techniques: A Comprehensive Review', *Indones. J. Electr. Eng. Comput. Sci.*, vol. 39, no. 1, p. 466, 2025, doi: 10.11591/ijeecs.v39.i1.pp466-484.
[24] A. Halimi, F. N. Fajri, and F. Rizal, 'Pengembangan Sistem Identifikasi Ancaman Keamanan pada Sistem Penerimaan Mahasiswa Baru dengan Framework Laravel', *COREAI J. Kecerdasan Buatan, Komputasi dan Teknol. Inf.*, vol. 6, no. 1, pp. 29–36, 2025, doi: 10.33650/coreai.v6i1.11537.
[25] A. Salam, F. Ullah, F. Amin, and A. Mohammad, 'Deep Learning Techniques for Web-Based Attack Detection in', *Mdpi*, pp. 1–18, 2023.
[26] M. M. Hasan, R. Islam, Q. Mamun, M. Z. Islam, and J. Gao, 'Adversarial Attacks on Deep Learning-Based Network Intrusion Detection Systems: A Taxonomy and Review', *Available SSRN 4863302*, 2024, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4863302
[27] N. Rahmeisi, E. Gani, and A. Arfriandi, 'Literature Review : A Machine Learning Approach to Web Attack Detection', vol. 4, no. 3, pp. 772–791, 2025.

[28] M. S. Albulayhi and D. M. Ibrahim, 'Open Web Application Security Project Components with Known Vulnerabilities: A Comprehensive Study', *ISC Int. J. Inf. Secur.*, vol. 13, no. 3, pp. 59–67, 2021, doi: 10.22042/ISECURE.2021.0.0.0.

[29] J. A. N. Lansky, S. Ali, M. Mohammadi, M. K. Majeed, and A. M. Rahmani, 'Deep Learning-Based Intrusion Detection Systems : A Systematic Review', *IEEE Access*, vol. 9, pp. 101574–101599, 2021, doi: 10.1109/ACCESS.2021.3097247.

[30] R. Jangra and A. Kajal, 'A Review of Deep Learning based Intrusion Detection Systems', *Proc. - 4th IEEE 2023 Int. Conf. Comput. Commun. Intell. Syst. ICCCIS 2023*, vol. 56, pp. 1004–1009, 2023, doi: 10.1109/ICCCIS60361.2023.10425595.

***Sapuan (Corresponding Author)**
Department of Information Technology,
Universitas Islam Negeri Ar-Raniry,
Banda Aceh, Aceh, Indonesia
Jl. Wedana No. 177, Banda Aceh, Aceh, Indonesia
Email: 190705065@student.ar-raniry.ac.id