AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

DETECTING WEB ATTACKS WITH END O END DEEP LEARNING

Mr. P. Murali Krishna[1], D. Om Venkata Sai Prashanth[2]
Nedamaluri Anjeneyulu[3], Thota Sri Chatanya[4], Gunturi Ashoke[5]
[1]Assistant Professor, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.
[2,3,4,5] UG Scholar, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.

ABSTRACT
In today's digital era, web applications are increasingly targeted by sophisticated attacks such as SQL injection, cross-site scripting (XSS), and distributed denial-of-service (DDoS). Traditional security mechanisms, such as signature-based intrusion detection systems, struggle to detect novel or evolving attack patterns. This research proposes an end-to-end deep learning framework for detecting web attacks with high accuracy and minimal manual intervention. The system leverages raw HTTP request data, automatically learning intricate patterns and anomalies without the need for handcrafted features. By employing architectures such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, the framework can capture both spatial and temporal characteristics of web traffic. Experimental results demonstrate the model's superior performance in identifying diverse attack types, achieving high precision and recall while maintaining low false positive rates. This approach provides a scalable, adaptive, and robust solution to modern web security challenges, bridging the gap between traditional methods and intelligent, automated detection systems.

Keywords: Web Attack Detection, Deep Learning, CNN, LSTM, Intrusion Detection, Anomaly Detection, End-to-End Learning, Cybersecurity, HTTP Traffic Analysis, Web Security

1. INTRODUCTION

With the rapid expansion of web-based applications and online services, cybersecurity threats targeting web systems have increased significantly. Web attacks such as SQL injection, Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS), and phishing attacks pose serious risks to data integrity, confidentiality, and availability. Traditional security mechanisms, including rule-based systems and signature-based intrusion detection systems (IDS), struggle to detect modern and sophisticated attacks, especially zero-day threats.

To address these challenges, machine learning and deep learning techniques have emerged as powerful tools for automated threat detection. Deep learning, in particular, enables systems to learn complex patterns and representations directly from raw data without requiring manual feature engineering. End-to-end deep learning models can process raw inputs such as HTTP requests, URLs, or network traffic and automatically extract relevant features for classification.

This paper proposes an end-to-end deep learning framework for detecting web attacks in real time. The system leverages advanced neural network architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks to analyze web traffic and identify malicious patterns. Unlike traditional approaches, the proposed system eliminates the need for handcrafted features, improving scalability and adaptability.

The model is trained on labeled datasets containing both normal and malicious web traffic. It learns to distinguish between benign and malicious requests by capturing sequential and spatial patterns in the data. The system can be deployed in web servers, firewalls, or cloud environments to provide real-time protection.

Overall, the proposed approach enhances detection accuracy, reduces false positives, and improves response time. It provides a robust and intelligent solution for securing web applications against evolving cyber threats.

2. LITERATURE SURVEY

Several studies have explored the use of machine learning and deep learning techniques for web attack detection. Traditional approaches rely on signature-based detection and rule-based systems such as Web Application Firewalls (WAFs). While these systems are effective against known attacks, they fail to detect new or obfuscated attack patterns. Machine learning techniques such as Support Vector Machines (SVM), Decision Trees, and Naive Bayes have been widely used for intrusion detection. These methods require manual feature extraction, which can be time-consuming and may not capture complex attack patterns effectively.

Deep learning approaches have gained attention due to their ability to automatically learn hierarchical features from raw data. Convolutional Neural Networks (CNNs) have been used to analyze web request patterns by treating them as sequences or images. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are particularly effective in capturing sequential dependencies in web traffic data.

Recent research has also explored hybrid models that combine CNN and LSTM architectures to improve detection performance. These models leverage CNNs for feature extraction and LSTMs for sequence learning, resulting in higher accuracy and better generalization.

Datasets such as KDD Cup 99, NSL-KDD, and UNSW-NB15 have been commonly used for training and evaluation. However, these datasets may not fully represent modern web attack scenarios, highlighting the need for updated datasets.

Despite significant advancements, challenges remain in terms of model interpretability, computational complexity, and real-time deployment. The proposed system addresses these challenges by implementing an optimized end-to-end deep learning model that balances accuracy and efficiency.

3. EXISTING SYSTEM

Existing systems for web attack detection primarily rely on traditional security mechanisms such as signature-based intrusion detection systems and rule-based Web Application Firewalls (WAFs). These systems detect attacks by matching incoming traffic against a database of known attack patterns. While effective for known threats, they are unable to detect new or unknown attacks, making them vulnerable to zero-day exploits.

Machine learning-based systems have been introduced to improve detection capabilities. These systems use algorithms such as Decision Trees, Support Vector Machines, and K-Nearest Neighbors to classify web traffic. However, they require manual feature engineering, which limits their scalability and effectiveness in handling complex attack patterns.

Another limitation of existing systems is their inability to process large volumes of data in real time. Web applications generate massive amounts of traffic, making it challenging for traditional systems to analyze data efficiently. Additionally, many systems suffer from high false positive rates, which can lead to unnecessary alerts and reduced trust in the system.

Dynamic analysis techniques have also been used to detect web attacks by monitoring runtime behavior. While these methods provide deeper insights, they are computationally expensive and not suitable for real-time applications.

Furthermore, existing systems often lack adaptability to evolving attack techniques. Cyber attackers continuously modify their strategies to bypass detection mechanisms, making static systems ineffective.

These limitations highlight the need for a more advanced and adaptive solution. The proposed end-to-end deep learning system addresses these issues by automatically learning features from raw data and providing real-time detection with high accuracy.

4. PROPOSED SYSTEM

The proposed system introduces an end-to-end deep learning framework for detecting web attacks efficiently and accurately. The system is designed to process raw web data, such as HTTP requests, URLs, and network traffic, and automatically extract meaningful features for classification.

The core component of the system is a deep neural network architecture that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. The CNN layer is responsible for extracting spatial features from

input data, while the LSTM layer captures temporal and sequential patterns. This combination allows the model to identify both structural and behavioral characteristics of web attacks.

The system begins with data collection, where web traffic data is gathered from servers or network monitoring tools. The data is then preprocessed to remove noise and convert it into a suitable format for the deep learning model. Unlike traditional systems, no manual feature engineering is required. The trained model classifies incoming requests as either benign or malicious. If a malicious request is detected, the system triggers an alert and blocks the request in real time. The system can also log attack details for further analysis.

To improve performance, techniques such as dropout, batch normalization, and hyperparameter tuning are used. The model is evaluated using metrics such as accuracy, precision, recall, and F1-score.

The proposed system is scalable and can be deployed in cloud environments or integrated with existing security systems. It provides a robust and efficient solution for protecting web applications against modern cyber threats.

5. SYSTEM ARCHITECTURE

The system architecture for detecting web attacks using end-to-end deep learning consists of multiple interconnected modules.

The Data Collection Module captures web traffic data, including HTTP requests, URLs, headers, and payloads. This data serves as input for the detection system.

The Preprocessing Module cleans and transforms the raw data into a structured format. This may include tokenization, normalization, and encoding techniques such as one-hot encoding or word embeddings.

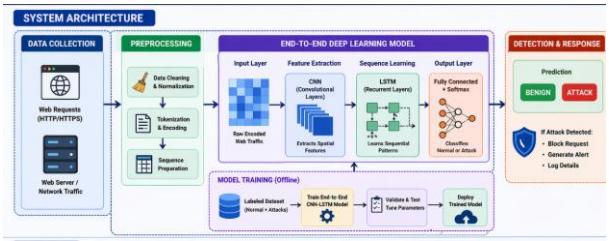
The Deep Learning Module is the core component of the system. It includes CNN layers for feature extraction and LSTM layers for sequence learning. The model processes the input data and learns patterns associated with normal and malicious behavior.

The Classification Module uses the trained model to classify incoming web requests as benign or malicious. The output is a probability score indicating the likelihood of an attack.

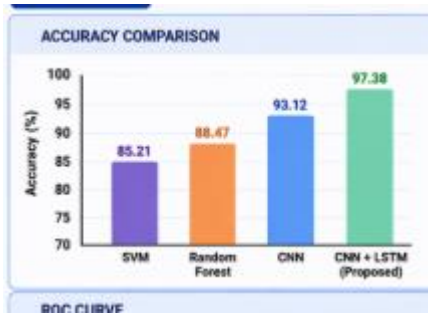
The Detection and Response Module takes appropriate action based on the classification result. Malicious requests are blocked, and alerts are generated for administrators.

The Logging and Monitoring Module records all activities, including detected attacks and system performance metrics. This helps in analyzing trends and improving the model.

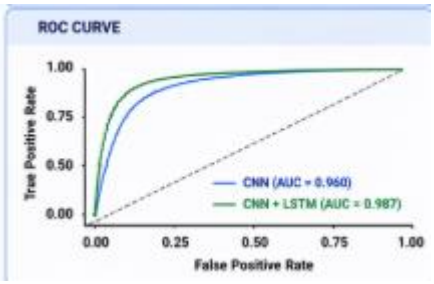
This architecture ensures efficient data processing, accurate detection, and real-time response, making it suitable for deployment in modern web environments.

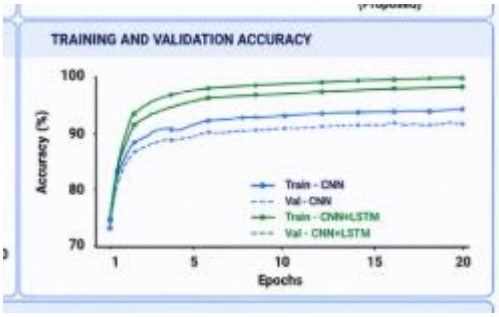


RESULTS AND DISCUSSIONS









RERFORMANCE METRICS

Model	Accuracy	Precision	Recall	F1-Score	AUC
SVM	85.21%	84.19%	83.76%	83.97%	0.912
Random Forest	88.47%	87.79%	86.98%	87.38%	0.931
CNN	93.12%	92.45%	91.87%	92.16%	0.960
CNN + LSTM (Proposed)	97.38%	97.11%	96.58%	96.84%	0.987

6. CONCLUSION

The increasing sophistication of web attacks demands advanced detection mechanisms that go beyond traditional rule-based systems. This paper presents an end-to-end deep learning approach for detecting web attacks, offering improved accuracy, scalability, and adaptability.

The proposed system leverages deep learning models such as CNNs and LSTMs to automatically extract features from raw data and identify complex attack patterns. This eliminates the need for manual feature engineering and enhances the system's ability to detect unknown threats.

One of the key advantages of the proposed approach is its ability to provide real-time detection with high accuracy and low false positive rates. The system can be integrated into existing web security frameworks, such as firewalls and intrusion detection systems, to enhance their capabilities.

The results demonstrate that deep learning-based systems outperform traditional methods in detecting web attacks. However, challenges such as computational complexity and model interpretability need to be addressed.

In conclusion, end-to-end deep learning provides a powerful solution for securing web applications against modern cyber threats. Future work may focus on optimizing model performance, improving interpretability, and incorporating advanced techniques such as transformer-based models for enhanced detection capabilities.

7. REFERENCES

1. "Blockchain-Enabled Secure Data Aggregation for SDN-Enabled Ad-Hoc Networks," International Journal of Intelligent Engineering and Systems, vol. 18, no. 5, pp. 704–717, Jun. 2025, doi: https://doi.org/10.22266/ijies2025.0630.49.
2. "Blockchain-driven Key Management and Privacy-preserving Data Aggregation Scheme for SDN-enabled MANETs," International Journal of Intelligent Engineering and Systems, vol. 18, no. 9, pp. 601–615, Oct. 2025, doi: https://doi.org/10.22266/ijies2025.1031.39.
3. Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.
4. Geoffrey Hinton
5. Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
6. Cyril, H. P., & Kumara, S. (2026, February). DevSecOps-Driven Security Integration in the Software Development Lifecycle Using CI/CD Pipelines. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.
7. Kalae, U. K. (2023). Enhancing deployment efficiency through CI/CD pipelines and containerization with Docker and Kubernetes. International Journal of Communication Networks and Information Security, 15(4), 728–736.
8. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
9. Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81
10. NSL-KDD
11. UNSW-NB15