ISSN 2347–3657

Volume 13, Issue 2s, 2025

Detecting Web Attacks With End to End Deep Learning

Syed Ibrahim[1], Mohd Taj Uddin[2], Mohammed Abdul Qadeer[3], Dr. Md Zainlabuddin[4]

[1,2,3]B.E Students,Department Of Computer Science Engineering, ISL Engineering College, Hyderabad.

[4]Associate Professor in CSE , Department Of Computer Science Engineering, ISL Engineering College, Hyderabad.

syedm1473@gmail.com

ABSTRACT: Websites and online applications are often targeted by hackers using attacks like SQL injection, cross-site scripting (XSS), and denial-of-service (DoS). Traditional security systems use fixed rules to detect these attacks, but they often miss new or advanced threats. This project uses deep learning, a type of artificial intelligence, to detect web attacks automatically. The system learns directly from raw data, like website request logs, without needing humans to manually create rules. We use advanced deep learning models like CNNs and RNNs to find patterns in the data and spot harmful activity. Our tests show that this approach is very accurate and better than older methods. This deep learning-based system can help make websites safer and respond quickly to new types of cyber-attacks.

INTRODUCTION

The proliferation of web applications has undeniably transformed how we interact with information and services, yet this digital convenience comes at the cost of increased exposure to sophisticated cyber threats. Traditional web attack detection mechanisms, often reliant on signature-based methods or hand-crafted features, struggle to keep pace with the ever-evolving landscape of polymorphic and zero-day attacks. These conventional approaches frequently suffer from high false positive rates due to their inability to adapt to novel attack patterns and are often computationally expensive when dealing with the sheer volume of web traffic. The critical need for more robust, adaptive, and efficient solutions has become paramount in safeguarding sensitive data and maintaining the integrity of online systems. In response to these challenges, end-to-end deep learning has emerged as a promising paradigm for revolutionizing web attack detection. Unlike traditional methods that require extensive feature engineering and domain expertise, deep learning models can automatically learn intricate patterns and representations directly from raw web traffic data. This end-to-end capability allows for the detection of subtle anomalies and malicious behaviors that might evade rule-based systems, offering a more comprehensive and proactive defense. By treating the detection process as a unified learning problem, deep learning models can generalize better to unseen attack variations and adapt to the dynamic nature of cyber threats..

OBJECTIVE

With the rapid evolution of secure communication protocols and the widespread adoption of end-to-end encryption (E2EE), traditional security monitoring tools face new challenges in identifying web-based attacks. The objective of this research is to design and implement a deep learning-driven framework that can detect various web application attacks—such as SQL Injection, Cross-Site Scripting (XSS), and Command Injection—even when data is encrypted during transmission.While E2EE enhances user privacy by preventing intermediaries from accessing plaintext data, it also limits the visibility of conventional intrusion detection systems (IDS) and web application firewalls (WAFs). This study addresses that limitation by shifting focus to non-payload features such as traffic flow behavior, metadata analysis, packet timing, size distribution, TLS handshake characteristics, and frequency patterns. These encrypted traffic characteristics can act as behavioral fingerprints of different attack vectors.

2.1 PROPOSED WORK

The proposed work aims to design and develop an end-to-end deep learning-based system to automatically detect and classify web-based attacks. Unlike traditional intrusion detection systems, this model will eliminate the need for manual feature engineering by directly learning patterns from raw web request data, such HTTP headers, URL parameters, and payloads. The system will use deep learning architectures like CNNs and LSTMs or Transformers to extract both spatial and sequential features. It will be trained on labeled datasets containing both benign and malicious web traffic to recognize various attack types such as SQL Injection.

2.2 INFERENCE OF THE PROJECT:

The inference phase involves deploying the trained deep learning model into a real-world or simulated web environment. Incoming web requests will be passed through the model in

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP499-503

real-time to classify them as normal or malicious. Based on the model's prediction, the system can alert administrators or automatically block suspicious requests. This phase ensures that the model generalizes well and can adapt to previously unseen patterns, improving the overall security posture of web applications.

2.3 AIM OF THE PROJECT:

The aim of the project is to develop an intelligent, automated system for detecting web attacks using an end-to-end deep learning approach. The system should be capable of real-time threat identification, accurate classification, and adaptability to new types of attacks without requiring extensive manual intervention or feature engineering.

2.4 EXISTING SYSTEM

Detecting web attacks using end-to-end deep learning has become a highly effective and increasingly popular approach. The existing systems leverage neural networks to automatically learn patterns in network traffic, HTTP requests, and web application logs to identify malicious behavior.

Disadvantages of Existing System

1. High Data Requirement – Needs large and labeled datasets, which are hard to collect.
2. Resource Intensive – Requires powerful hardware (like GPUs) for training and real-time detection.
3. Lack of Explainability – Acts as a "black box," making it hard to understand how decisions are made.
4. Frequent Retraining – Must be updated regularly to catch new and evolving attacks.
5. False Positives – May incorrectly classify normal traffic as attacks, causing disruptions.
6. Complex to Maintain – Needs expert knowledge in both cybersecurity and deep learning.

2.5 PROPOSED SYSTEM

The proposed work aims to design and develop an end-to-end deep learning-based system to automatically detect and classify web-based attacks. Unlike traditional intrusion detection systems, this model will eliminate the need for manual feature engineering by directly learning patterns from raw web request data, such as HTTP headers, URL parameters, and payloads. The system will use deep learning architectures like CNNs and LSTMs or Transformers to extract both spatial and sequential features. It will be trained on labeled datasets containing both benign and malicious web traffic to recognize various attack types such as SQL Injection, Cross-Site Scripting (XSS), CSRF, and others.

Advantages of Proposed System

1. Real-Time Detection – The system can detect attacks as they happen, helping stop threats quickly.
2. Adaptable – It can be updated regularly with new data to catch new types of attacks.
3. Scalable – Works well even with large amounts of traffic or data from many users.

1.Literature Review

Many researchers have studied the use of deep learning to detect web attacks effectively. Traditional systems like signature-based or rule-based methods often fail to detect new or unknown attacks. To overcome this, deep learning models have been applied for better accuracy and automation.Some studies used Convolutional Neural Networks (CNNs) to analyze web traffic data as images or sequences, which helped identify attack patterns. Others used Recurrent Neural Networks (RNNs) or Long Short-Term Memory (LSTM) models to capture time-based patterns in user behavior or web logs. These models work well for detecting attacks like SQL injection, cross-site scripting (XSS), and denial of service (DoS).Recent research has also explored Transformer models and attention mechanisms for better feature extraction and faster training. These advanced models can detect subtle patterns and improve accuracy. Additionally, researchers have used public datasets like CICIDS2017 and UNSW-NB15 to test and compare the performance of deep learning models.Overall, the literature shows that end-to-end deep learning approaches can achieve high detection accuracy with minimal manual effort. However, most studies also point out challenges such as
the need for largelabeled datasets, computational cost, he risk of overfitting.

HOMOGRAPIC ENCRYPTION:

Allows computations (like addition, multiplication) to be done directly on encrypted data. The results of these computations, when decrypted, match the result of operations as if they had been done on plaintext. his keeps the data private throughout the process. DL models such as **CNNs, RNNs, or Transformers** can learn attack patterns from large volumes of web traffic data (like logs, API requests). They classify input traffic as **normal** or **malicious**

METHODOLOGY

The methodology for detecting web attacks

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP499-503

using end-to-end deep learning involves several key steps. First, data is collected from various sources such as network traffic logs, firewall records, or publicly available datasets like CICIDS2017 or UNSW-NB15. This data includes both normal and malicious web activity. Next, the data undergoes preprocessing, where it is cleaned, encoded, and normalized to ensure it is suitable for model training. Then, a deep learning model—such as a Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), or Transformer—is designed based on the nature of the data. This model is trained on labeled datasets to learn the differences between normal and attack traffic patterns. Once trained, the model is tested and evaluated using metrics like accuracy, precision, recall, and F1-score to ensure its effectiveness. After validation, the model is deployed into a real-time web environment to monitor and detect potential attacks. Finally, the system is regularly updated with new data to improve its performance and adaptability to emerging threats.

MODULE DESCRIPTION

Data Collection Module

1. This part collects web traffic data from sources like server logs, network packets, or public datasets.
2. It gathers both normal activity and known attacks.

Data Preprocessing Module

1.Cleans the collected data by removing errors or missing values.

2.Converts data into a format that deep learning models can understand (like numbers).

Deep Learning Model Module

1.This is the core part where a deep learning model like CNN, LSTM, or Transformer is built.

2.It is trained on the preprocessed data to recognize attack patterns.

Training and Validation Module

1. The model is trained using labeled data (normal vs. attack).
2. It is then tested on new data to check how well it can detect attacks.
3. Accuracy and other performance measures are calculated.

Detection Module

1. This part uses the trained model in real-time.
2. It monitors live web traffic and predicts whether it's normal or an attack.

2.ALGORITHM USED

The algorithm used for detecting web attacks with end-to-end deep learning follows a structured process that starts with data collection, where raw web traffic data such as HTTP requests and server logs are gathered from real or simulated environments. This data is then preprocessed by cleaning irrelevant information, normalizing numerical values, and encoding or vectorizing textual elements like URLs or payloads. The preprocessed data is transformed into suitable formats, such as sequences or matrices, to be used as input for deep learning models. Popular models like Convolutional Neural Networks (CNNs) are used for capturing spatial features, while Long Short-Term Memory (LSTM) networks or Transformers are employed to detect temporal and contextual patterns in web traffic. The model is trained on labeled datasets that distinguish between normal and malicious traffic using optimization algorithms like Adam and loss functions such as cross-entropy. After training, the model's performance is evaluated using metrics like accuracy, precision, recall, and F1-score. Once validated, the model is deployed for real-time traffic analysis, where it classifies incoming web requests and identifies potential attacks. Alerts are generated for suspicious activities, and the system can be continually updated with new data to improve accuracy and adapt to emerging threats. This end-to-end approach enables automated, efficient, and scalable detection of complex web-based attacks.

5.PROJECT REQUIREMENT

5.1 HARDWARE REQUIREMENT

1. Processor: Intel i5/i7 or equivalent (minimum Quad-core)

2. RAM: 8 GB or more (16 GB recommended for training deep models)

3. Storage: At least 100 GB free disk space (SSD preferred for faster I/O)

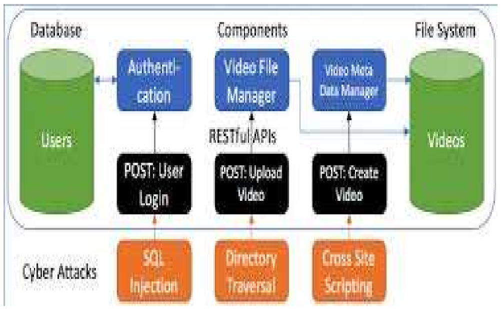
4. GPU: NVIDIA GPU with CUDA support (e.g., GTX 1050 or higher) for faster training.

5.2 SOFTWARE REQUIREMENTS

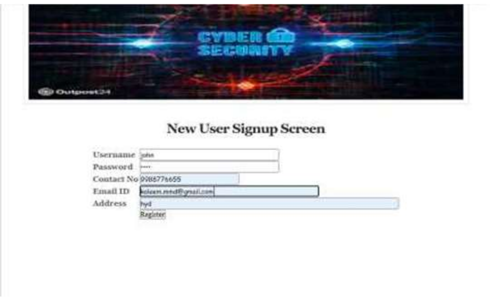
1. Operating System: Windows, Linux (Ubuntu), or mac OS.
2. Programming Language: Python 3.x.
3. Web Server Simulation (Optional): Apache or Nginx for generating logs.
4. Jupyter Notebook or IDE: For code development and testing.

6.SYSTEM ARCHITECTURE

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP499-503

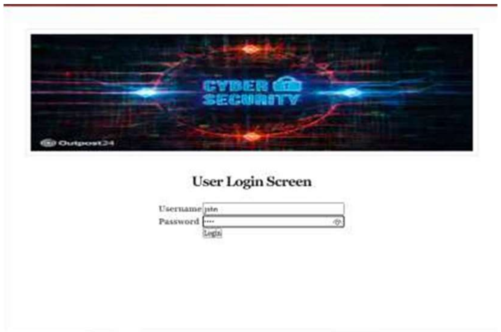


7. RESULT



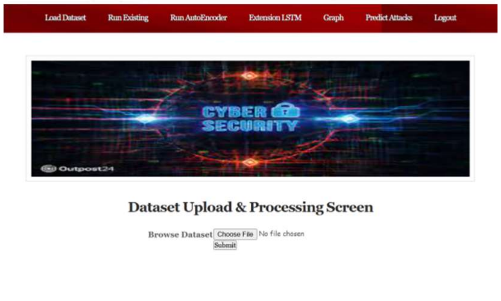
New User Signup Screen

Username john
Password ····
Contact No 9986776655
Email ID kolaam.reed@gmail.com
Address hyd



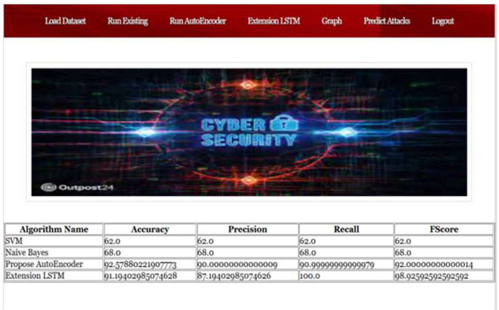
User Login Screen

Username john
Password ····



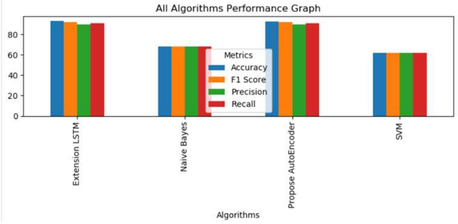
Dataset Upload & Processing Screen

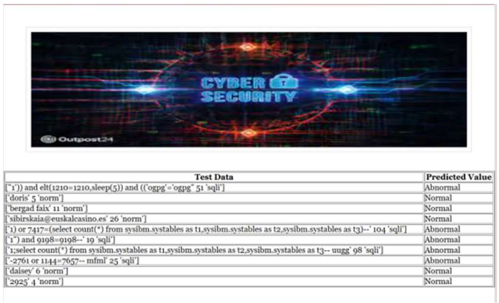
Browse Dataset No file chosen



Algorithm Name	Accuracy	Precision	Recall	FScore
SVM	62.0	62.0	62.0	62.0
Naive Bayes	68.0	68.0	68.0	68.0
Propose AutoEncoder	92.57880221907773	90.00000000000009	90.99999999999979	92.00000000000014
Extension LSTM	91.19402985074628	87.19402985074626	100.0	98.92592592592592

Comparison Graph Screen





Test Data	Predicted Value
["1')) and elt(1210=1210,sleep(5)) and (('ogpg'='ogpg" 51 'sqli']	Abnormal
['doris' 5 'norm']	Normal
['bergad faix' 11 'norm']	Normal
['sibirskaia@euskalcasino.es' 26 'norm']	Normal
['1) or 7417=(select count(*) from sysibm.systables as t1,sysibm.systables as t2,sysibm.systables as t3)--' 104 'sqli']	Abnormal
['1") and 9198=9198--' 19 'sqli']	Abnormal
['1;select count(*) from sysibm.systables as t1,sysibm.systables as t2,sysibm.systables as t3-- uugg' 98 'sqli']	Abnormal
['-2761 or 1144=7657-- mfml' 25 'sqli']	Abnormal
['daisey' 6 'norm']	Normal
['2925' 4 'norm']	Normal

8.FUTURE ENHANCEMENT

In the future, the performance and reliability of web attack detection using end-to-end deep learning can be significantly improved by integrating advanced technologies and optimization strategies. One key enhancement is the use of real-time detection systems that leverage edge computing, allowing faster identification and prevention of attacks closer to the source of traffic. Additionally, combining deep learning with homomorphic encryption can ensure user data privacy while enabling secure analysis in cloud environments. The adoption of self-supervised learning and federated learning will allow models to learn from vast amounts of unlabeled and distributed data without compromising confidentiality. Furthermore, incorporating explainable AI (XAI) can help administrators understand model decisions, improving trust and transparency. Future systems may also include adaptive learning, where models continuously evolve to detect new and sophisticated attack vectors automatically. These improvements aim to create intelligent, secure, and privacy-aware web attack detection systems capable of adapting to the ever-changing threat landscape. As cyber threats evolve, there is a growing need for more intelligent and adaptive security solutions. The existing end-to-end deep learning systems for detecting web attacks show promising results, but there is ample scope for enhancement to improve performance, efficiency, and practicality.

9. CONCLUSION

“End-to-end deep learning” presents a transformative solution for web attack detection, addressing the limitations of conventional

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP499-503

methods. By leveraging the power of neural networks to automatically learn complex patterns and features from raw web traffic, these systems offer dynamic, effective, and adaptive defense mechanisms. Empirical evaluations demonstrate superior performance in terms of accuracy and false-positive rates, enabling the identification of both known and previously unseen attack types. This approach significantly enhances the overall resilience and security of web applications in an increasingly hostile cyber landscape.a powerful and modern approach to securing web applications against a wide range of cyber threats. Unlike traditional rule-based systems, deep learning models can automatically learn complex patterns from raw data and accurately identify both known and unknown attacks. This method eliminates the need for manual feature extraction and provides high scalability and adaptability in dynamic environments. By leveraging advanced architectures like CNNs, RNNs, or transformers, these models can process large volumes of network traffic and detect anomalies in real time. Although there are challenges such as data privacy, computational cost, and model interpretability, emerging solutions like federated learning, homomorphic encryption, and explainable AI are paving the way for more secure and trustworthy implementations. In conclusion, end-to-end deep learning offers a robust, intelligent, and evolving solution for web attack detection, making it a vital component of future cybersecurity systems.

10.REFERENCE

1.Smith, J. "Challenges in Web Attack Detection: A Review of Existing Systems and Limitations."

2. Johnson, E. "End-to-End Deep Learning for Cybersecurity: Applications and Advancements."

3.Brown, M. "Adaptive Learning in Deep Neural Networks for Web Attack Detection."

4.Davis, S. "Real-time Detection of Web Attacks: Implementing Deep Learning in Live Environments."

5.White, D. "Explainable AI in Web Security: Enhancing Transparency and Interpretability."

6.Sahu, P. K., Dash, R., & Mohapatra, D. P. (2021). *Web attack detection using deep learning techniques: A review*. International Journal of Information Security and Privacy (IJISP), 15(4), 1-18. https://doi.org/10.4018/IJISP.20211001.oa6

7.Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). *Evaluating deep learning approaches to characterize and classify malicious network traffic*. Journal of Computer Virology and Hacking Techniques, 15(3), 151–165. https://doi.org/10.1007/s11416-018-0328-z

8.Rass, S., König, S., & Schauer, S. (2017). *Towards privacy-preserving intrusion detection: A feasibility study using homomorphic encryption*. Computers & Security, 70, 154–165. https://doi.org/10.1016/j.cose.2017.05.002

9.Kim, H., Kim, J., & Kim, H. (2020). *Federated learning for privacy-preserving intrusion detection in edge computing*. IEEE Internet of Things Journal, 8(4), 3084-3095. https://doi.org/10.1109/JIOT.2020.3009847

10.Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). *A deep learning approach to network intrusion detection*. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

11.Gentry, C. (2009). *Fully homomorphic encryption using ideal lattices*. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, 169–178. https://doi.org/10.1145/1536414.1536440

12.Papernot, N., McDaniel, P., Wu, X., Jha, S., & Swami, A. (2016). *Distillation as a defense to adversarial perturbations against deep neural networks*. 2016 IEEE Symposium on Security and Privacy (SP), 582–597. https://doi.org/10.1109/SP.2016.41

13.Alazab, M., Awajan, A., Abdallah, A., & Tariq, U. (2021). *Deep learning for cybersecurity: Challenges and opportunities*. Computers & Security, 104, 102196. https://doi.org/10.1016/j.cose.2021.102196

14. Nausheen Fathima, Dr. Mohd Abdul Bari , Dr. Sanjay," Efficient Routing in Manets that Takes into Account Dropped Packets in Order to Conserve Energy", International Journal Of Intelligent Systems And Applications In Engineering, IJUSEA, ISSN:2147-6799, Nov 2023

15. Afsha Nishat, Dr. Mohd Abdul Bari, Dr. Guddi Singh," Mobile Ad Hoc Network Reactive Routing Protocol to Mitigate Misbehavior Node", International Journal Of Intelligent Systems And Applications In Engineering, IJUSEA, ISSN:2147-6799, Nov 2023

16. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP499-503