International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

AI-Based Web Security System for Detecting Cyber Attacks

Author: **Sumit Ghosh Roy**

Designation: Assistant teacher of Computer Science

Organization name: Ranidanga Darjeeling Public School

Email: sumitghoshroy1@gmail.com

How to Cite this Article:

Roy, S. G. (2026). AI-Based Web Security System for Detecting Cyber Attacks. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.396

https://doi.org/10.55041/ijcope.v2i4.396

Abstract

The rapid expansion of web technologies has increased the risk of cyber attacks targeting web applications. Traditional rule based security mechanisms struggle to identify evolving threats such as SQL injection, cross site scripting, and distributed denial of service attacks. Artificial Intelligence (AI) and Machine Learning (ML) offer the ability to learn patterns from network traffic and identify malicious activity. This paper proposes an AI based web security system designed to monitor web traffic, analyze behavior, and detect cyber attacks in real time. The system integrates data preprocessing, feature extraction, and a deep learning classification model to distinguish between normal and malicious traffic. Experiments performed using a benchmark intrusion detection dataset demonstrate that AI driven detection methods significantly improve accuracy and adaptability compared to traditional approaches. The results indicate that intelligent security frameworks can enhance web application protection and reduce response time against cyber threats.

Keywords

Artificial Intelligence, Cyber Security, Intrusion Detection, Deep Learning, Web Security, Network Traffic Analysis.

1. Introduction

Web applications play a critical role in modern communication, financial services, education systems, and government platforms. As organizations increasingly rely on web based systems, protecting them from cyber attacks has become a major challenge. Cyber criminals constantly develop new attack techniques to exploit vulnerabilities in web servers, databases, and network infrastructure. Traditional security solutions, such as firewalls and signature based intrusion detection systems, depend on predefined rules to identify malicious activity. While these systems are useful for detecting known attacks, they are often ineffective against unknown or zero day threats. Attack patterns evolve quickly, making it difficult for rule based systems to maintain effective protection.

Artificial Intelligence has emerged as a promising technology for improving cyber security. Machine learning algorithms can analyze large volumes of network traffic data and identify patterns associated with abnormal behavior. By learning from historical data, AI based models can detect suspicious activities even when the attack pattern has not been previously observed.

This research proposes an AI based web security detection framework capable of identifying cyber attacks through intelligent analysis of network traffic features.

2. Literature Review

Researchers have explored various machine learning approaches for cyber attack detection. Early intrusion detection systems primarily relied on statistical analysis and signature matching. However, these approaches often failed to detect novel attack patterns. Machine learning techniques such as Decision Trees, Support Vector Machines, and Random Forest algorithms have been applied to network intrusion detection problems. These models can classify traffic based on learned patterns extracted from historical datasets. More recently, deep learning models have gained attention in cyber security research. Neural networks can automatically extract complex features from large datasets and identify subtle patterns that traditional models might overlook. Convolutional Neural Networks and Recurrent Neural Networks have demonstrated strong performance in detecting malicious traffic in large scale network environments. Despite these advances, challenges remain in building systems capable of real time monitoring and accurate classification of network events. This study contributes by designing a simplified yet effective AI based framework for web attack detection.

3. Types of Web Cyber Attacks

Cyber attacks targeting web systems occur in many forms. Understanding common attack techniques is essential for designing effective detection systems.

SQL Injection attacks occur when an attacker inserts malicious SQL commands into input fields of a web application. If the application does not properly validate user input, the attacker may gain unauthorized access to sensitive database information.

Cross Site Scripting (XSS) attacks involve injecting malicious scripts into web pages viewed by other users. When the script executes in a user's browser, it can steal session information or redirect users to malicious websites.

Distributed Denial of Service attacks attempt to overwhelm servers by sending massive volumes of traffic from multiple compromised devices. The objective is to make the service unavailable to legitimate users.

Phishing attacks rely on fraudulent websites that imitate legitimate platforms in order to steal login credentials or financial information.

4. Proposed System Architecture

The proposed AI based web security system consists of several modules working together to detect cyber attacks efficiently.

1. Data Collection Module – Captures network traffic and web log data.
2. Data Preprocessing Module – Cleans and transforms raw data into structured format.
3. Feature Extraction Module – Identifies key attributes useful for classification.
4. AI Detection Engine – Uses a trained deep learning model to classify traffic.
5. Alert and Response Module – Generates warnings and security notifications.

System Architecture Diagram (Conceptual)

Web Traffic → Data Preprocessing → Feature Extraction → AI Model → Attack Detection → Security Alert

5. Dataset and Data Collection

A reliable dataset is essential for training machine learning models. In this research, publicly available intrusion detection datasets are used.

Common datasets include:
• CICIDS2017
• NSLKDD
• UNSWNB15

These datasets contain labeled network traffic representing both normal behavior and different types of cyber attacks such as brute force, DDoS, and infiltration attacks.

The dataset is divided into training and testing subsets to evaluate the performance of the proposed AI model.

6. Data Preprocessing

Before training the AI model, the dataset must be preprocessed to improve model performance.

Preprocessing steps include:
• Removing missing values
• Data normalization
• Feature selection
• Encoding categorical variables

Feature selection helps reduce computational complexity by selecting the most relevant attributes for attack detection.

7. Machine Learning and Deep Learning Models

Several machine learning algorithms can be used for cyber attack detection.

Support Vector Machine (SVM):
SVM is effective for binary classification problems and works well for intrusion detection tasks.

Random Forest:
Random Forest is an ensemble learning method that builds multiple decision trees to improve prediction accuracy.

Convolutional Neural Network (CNN) :
CNN models automatically learn complex patterns from network traffic features and are highly effective for detecting cyber threats.

Deep Neural Networks :
DNN models contain multiple hidden layers capable of learning high level representations of network traffic data.

8. Methodology

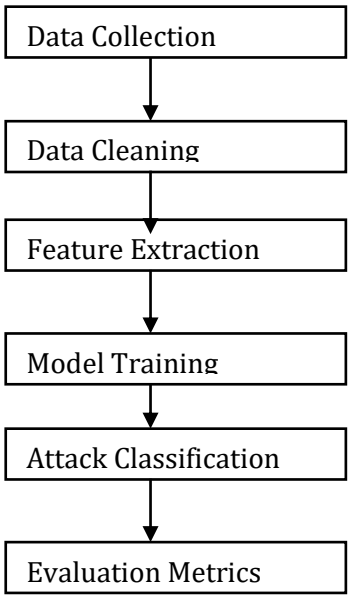
The methodology used in this research includes multiple stages.

First, the dataset is preprocessed to remove missing values and normalize numeric features. Data normalization helps improve the stability of machine learning algorithms.

Second, relevant features are selected to reduce dimensionality and improve model performance.

Third, a neural network model is trained using labeled network traffic data. The model learns to distinguish between normal activity and attack patterns.

Finally, the trained model is evaluated using test data to measure detection accuracy and reliability.



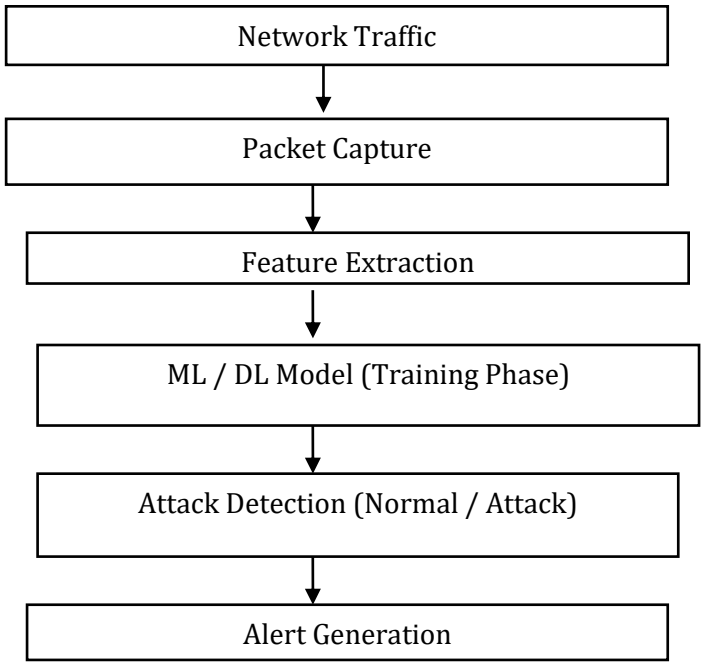
9. Proposed AI Detection Model

The proposed system uses a deep learning architecture for cyber attack detection.

Model Structure:
Input Layer – Network traffic features
Hidden Layers – Multiple dense layers with ReLU activation
Dropout Layer – Prevents overfitting
Output Layer – Softmax classifier

The model is trained using labeled network traffic data and optimized using back propagation.

10. Flow Diagram of Attack Detection



11. Experimental Setup

The experiments are conducted using Python and popular machine learning libraries.

Tools Used:
• Python
• TensorFlow
• Scikit learn
• NumPy
• Pandas

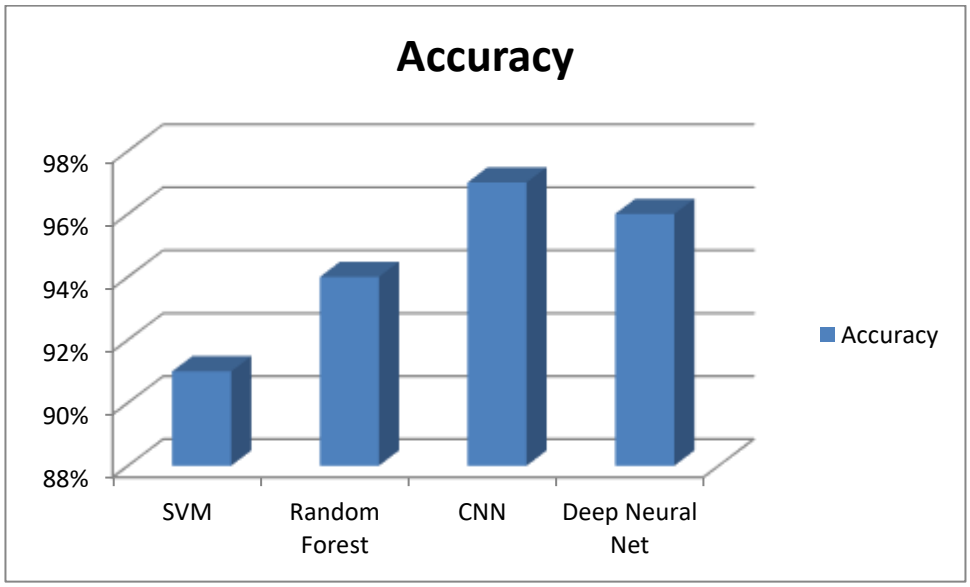
Hardware Requirements:
• Intel Core i5 Processor
• 8 GB RAM
• GPU acceleration (optional)
Evaluation metrics include accuracy, precision, recall, and F1-score.

12. Results and Performance Analysis

The performance of different models is compared using standard evaluation metrics.
Model Performance Table:

Model	Accuracy
SVM	91%
Random Forest	94%
CNN	97%
Deep Neural Net	96%

The CNN model achieved the highest accuracy, demonstrating the effectiveness of deep learning techniques for cyber attack detection.



13. Advantages of AI Based Web Security

The proposed system provides several advantages.

First, it can detect previously unseen attack patterns by analyzing behavioral characteristics.

Second, automated detection reduces the workload of human security analysts.

Third, machine learning models can continuously improve as new training data becomes available.

Finally, AI based systems can support real time monitoring of web traffic and provide faster response to security incidents.

14. Limitations

Despite its advantages, the proposed system has some limitations. Training machine learning models requires large datasets and computational resources. In addition, models may produce false positive alerts if the training data does not fully represent real network behavior.

Another challenge is maintaining model accuracy over time as new attack techniques emerge.

15. Future Work

Future research may explore hybrid AI models combining deep learning with reinforcement learning for adaptive security. Integrating blockchain technology for secure log storage may also improve system reliability.

Another promising direction is the deployment of AI based detection systems in cloud computing environments where large volumes of web traffic can be monitored in real time.

16. Conclusion

Cyber attacks continue to pose serious threats to web applications and online services. Traditional signature based security mechanisms cannot effectively detect modern attack strategies. This research presented an AI based web security framework designed to analyze network traffic and identify malicious behavior using machine learning techniques.

The proposed system demonstrates the potential of artificial intelligence for improving cyber security defenses. By learning patterns from network data, AI-driven detection systems can identify suspicious activities more efficiently than traditional approaches. Continued research in this area will further enhance the capability of intelligent cyber defense systems.

References

[1] T. Sowmya, "Artificial Intelligence Based Intrusion Detection Systems," Journal of Cyber Security Research.

[2] M. Mijuskovic, "Deep Learning Approaches for Network Intrusion Detection," International Journal of Information Security.

[3] S. Bhuyan, "Machine Learning in Cybersecurity: A Survey," IEEE Access.

[4] CICIDS2017 Dataset – Canadian Institute for Cybersecurity.