

# Real-Time Cyber Threat Detection Using Deep Learning: A Step Towards Autonomous Security

Ankush G Hegde <sup>1</sup>, Anirudh P Nayak <sup>2</sup>, Shrikara P S Nakshatri <sup>3</sup>, Mrs. Geethapriya G H <sup>4</sup>

<sup>1</sup>Student, Computer Science and Engineering, Jyothy Institute of Technology, Bengaluru, India

<sup>2</sup>Student, Computer Science and Engineering, Jyothy Institute of Technology, Bengaluru, India

<sup>3</sup>Student, Computer Science and Engineering, Jyothy Institute of Technology, Bengaluru, India

<sup>4</sup>Assistant Professor, Dept. of Computer Science and Engineering, Jyothy Institute of Technology, Bengaluru, India

\*\*\*

**Abstract** - In today's rapidly evolving digital ecosystem, traditional rule-based cybersecurity systems are often ineffective against zero-day exploits and advanced persistent threats. This research presents an AI/ML-driven approach to intelligent intrusion detection and automated incident response. The proposed system captures real-time network traffic data, analyzes it using ensemble learning model trained on diverse attack patterns, and classifies potential threats with high accuracy. Upon detection, it generates context-aware mitigation recommendations and displays them via a user-friendly React-based dashboard. The solution helps businesses react to cyber threats more rapidly and precisely by utilizing data-driven automation and minimizing the need for manual monitoring. It improves the entire cybersecurity posture and adjusts to changing attack patterns through real-time detection and intelligent response. Results from experiments demonstrate its capacity to recognize various intrusion types and respond promptly, strengthening defenses against contemporary cyberthreats.

**Key Words:** Cybersecurity, Intrusion Detection System (IDS), Artificial Intelligence (AI), Machine Learning (ML), Real-time Threat Detection, Automated Incident Response, Network Traffic Analysis, Zero-day Exploits.

## 1. INTRODUCTION

In the digital age, cyberthreats have increased in number and sophistication. People and companies are always at danger of serious data breaches or interruptions of vital services due to malware, phishing, ransomware, and unauthorized access assaults. Traditional security measures, which rely on pre-established guidelines and established threat patterns, are no longer sufficient to thwart complex, fast-moving, and advanced attacks, particularly those that are novel or unidentified, such as multi-layer intrusions and zero-day vulnerabilities.

To overcome these limitations, there is a growing need for adaptive, intelligent, and real-time security mechanisms. Artificial Intelligence (AI) and Machine Learning (ML) have shown great promise in enhancing cybersecurity by enabling systems to learn from patterns, identify anomalies, and make data-driven decisions. This dynamic capability makes them particularly suitable for evolving threat landscapes.

Moreover, by reducing dependence on manual rule updates and security analysts, such systems can significantly lower response times and reduce operational overhead.

This research presents an automated cybersecurity incident response system that integrates a Machine Learning-based Intrusion Detection System (IDS) with real-time threat classification and response generation. By employing an ensemble learning model that has been taught using actual cases of normal traffic and various types of cyberattacks, the system monitors network traffic and calculates risks.

With an intuitive dashboard designed using React, the system identifies the type of threat and presents possible responses upon detection of anomalous activity. Its flexible design provides transparent visual representations, the ability to learn and get better over time, and simple integration with existing security settings.

## 2. DEFINITION AND CONCEPTUAL FRAMEWORK

Through observing network traffic and recognizing abnormal or harmful activity, an intrusion detection system (IDS) has a significant role in cybersecurity. The two most popular forms of traditional IDS solutions are anomaly-based, which detect anything that is not normal behavior, and signature-based, which look for patterns that match documented threats. While beneficial, these methods often miss newer or unknown attacks, especially zero-day attacks, and need to be updated often to remain effective.

This study employs ensemble learning model to track and classify network traffic in real time using Artificial Intelligence and Machine Learning to bypass the weaknesses of traditional systems. CNNs are extremely useful since they don't need human feature selection and can discover complex patterns in data automatically. With an easy-to-use dashboard built with React, the system offers real-time response suggestions when it detects suspicious activity. This approach minimizes the requirement for ongoing human supervision, streamlines threat response, and enhances detection accuracy by integrating automation and intelligence analysis.

### 3. HISTORICAL DEVELOPMENT

Cybersecurity has evolved alongside advances in computing and networking. At first, cybersecurity relied on rudimentary instruments such as passwords and antivirus software to safeguard networks. But during the late 1980s, when internet traffic grew rapidly, the demand for advanced security brought about the invention of Intrusion Detection Systems (IDS), which initially focused on detecting threats with known attack signatures. More recent IDS models that looked for unusual behaviour to detect unknown threats were developed during the 2000s as attackers became more sophisticated. But many false alarms were generated by these anomaly-based systems, which often detected benign activity as malicious.

The shortcomings of traditional intrusion detection systems became more evident as network traffic grew in volume and complexity. This compelled the cybersecurity community to explore more intelligent solutions, leading to the creation of machine learning (ML) and artificial intelligence (AI) for more dynamic and advanced threat detection. Since the early 2010s, machine learning (ML), specifically Deep Learning techniques such as ensemble learning model, has been critical to efficiently identifying threats and monitoring traffic patterns. This trend indicates a major move towards autonomous, self-adjusting security systems that can respond to new threats without the need for frequent human intervention updates.

### 4. LITERATURE REVIEW

- "Global cyber-threat intelligence system with artificial intelligence and convolutional neural network" [4] analyzes cyber-attack patterns and social media data through deep learning. Processing 30,203 attack records and 3,789 multilingual tweets, the system performs real-time anomaly detection and threat prediction. Interactive dashboards deliver cross-platform threat intelligence for strategic cybersecurity decision-making.

- "A Comparative Study of AI-based Intrusion Detection Techniques in Critical Infrastructures" [5] by Safa Otoum, Burak Kantarci, and Hussein Mouftah compares machine learning, deep learning, and reinforcement learning approaches for IDS in critical infrastructures using the KDD'99 dataset. The study evaluates five IDS models, with QL-IDS achieving nearly 100% accuracy and detection rates. Results highlight the effectiveness of reinforcement learning in enhancing real-time intrusion detection.

- "AI Use in Enhancing Cybersecurity for Safeguarding Digital Information" [6] by Ruibin Wang explores how the integration of Artificial Intelligence with homomorphic encryption can significantly improve cybersecurity. It highlights AI's role in real-time threat detection, predictive analysis, and anomaly identification, while preserving data confidentiality during processing. The study concludes that

this synergy enhances data protection against evolving cyber threats.

- "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation" [7] by Kavitha Dhanushkodi and S. Thejas reviews AI-driven cybersecurity methods like CNNs, RNNs, and GANs for real-time threat detection. It emphasizes explainability, scalability, and adaptability of AI across domains like IoT and Industry 5.0, highlighting its effectiveness against evolving threats.

- "AI-Driven Threat Detection and Response: A Paradigm Shift in Cybersecurity" [8] by Asad Yaseen explores how AI transforms cybersecurity by shifting from reactive to proactive defense mechanisms. It discusses the integration of machine learning models like CNNs, RNNs, and ensemble methods for real-time threat detection and response. The study highlights AI's potential to improve adaptability, accuracy, and resilience against evolving cyber threats.

- "AI-Powered Ransomware Detection Framework" [9] by Subash Poudyal and Dipankar Dasgupta proposes a hybrid AI-based approach combining static and dynamic malware analysis for ransomware detection. It utilizes tools like DLL, Ghidra, and Cuckoo sandbox to extract features at DLL, function call, and assembly levels, which are processed with NLP and machine learning algorithms. The proposed AIRaD tool achieved a high accuracy of 99.54%, demonstrating its effectiveness in identifying ransomware with minimal false positives.

- "An Artificial Intelligence-Based Intrusion Detection System using Optimization and Deep Learning" [10] proposes a Vulture-based Deep Belief System (VbDBNS) for intrusion detection, leveraging Min-Max normalization and feature extraction from the NSL-KDD dataset. The model achieves 99.85% accuracy and 99.94% recall by optimizing vulture fitness for continuous intrusion monitoring. Comparative results show superior performance in precision, F1-score, and execution time over existing methods like SMO-DNN and IDS-DNN.

### 5. CHALLENGES IN INTEGRATION AND IMPLEMENTATION

- **Dataset quality or availability:** Obtaining reliable, real-world data for training is perhaps the most challenging problem in creating intrusion detection systems. It is hard for models to perform well in real-world environments because most of the datasets that are presently available are either too outdated or artificially designed. Conversely, obtaining real-time traffic data is highly problematic with regards to user privacy and ethical use of data, making the process even more complicated.

- **Model accuracy or false positives:** It's difficult to achieve the perfect balance between accuracy and reliability

when it comes to AI-driven intrusion detection. Too many false alarms can flood security personnel with noise and lead to alert fatigue, which ultimately translates to missing detection of important threats. To avoid this, models need to be carefully tuned and trained on diverse sets of high-quality datasets that truly reflect network conditions in the real world.

- Real-time processing issues:** It could be difficult to process data packets rapidly and reduce model prediction latency with real-time threat detection if there is extensive network traffic. Resource-constrained processing units can slow or even lose packets. In order to ensure smooth performance within real-world implementations, it is critical to make the model more efficient without sacrificing accuracy.

- API/Dashboard integration:** There are special challenges in synchronizing data and ensuring real-time updates while integrating the AI-driven detection system with a responsive dashboard and APIs. Minimizing latency without compromising secure communication between the frontend user interface and the backend models is essential. Smooth and seamless integration also relies on ensuring that the different technologies complement each other.

- Hardware limitations:** In order for AI models to run in real time, particularly deep learning models such as CNNs, a significant amount of processing power is often needed. This tends to make the system lag and unresponsive on systems with very limited processing power or memory, like older systems or edge devices. Due to this, it can be challenging to run these models in low-resource scenarios.

- Security of the response system itself:** While the system is supposed to detect outside threats, its own elements, including the models, dashboards, and APIs, can also be open to attack. Hackers might find and exploit loopholes to alter detection results or even crash the system should proper security protocols not be followed. Because of this, it's important to enforce access limits, use secure coding practices, and encrypt all traffic.

## 6. METHODOLOGY

The proposed system adopts a structured, multi-stage machine learning pipeline aimed at detecting and classifying network intrusions in real time. The process begins with the collection of raw network traffic logs containing fields such as timestamp, source and destination IPs, protocol, ports, packet size, TTL, and TCP flags. The raw data often includes malformed or missing entries, which are filtered out during preprocessing to ensure data quality. After this, categorical values such as IP addresses and protocol identifiers are encoded using LabelEncoder. The encoders are saved and reused during prediction to maintain consistency between the training and inference phases.

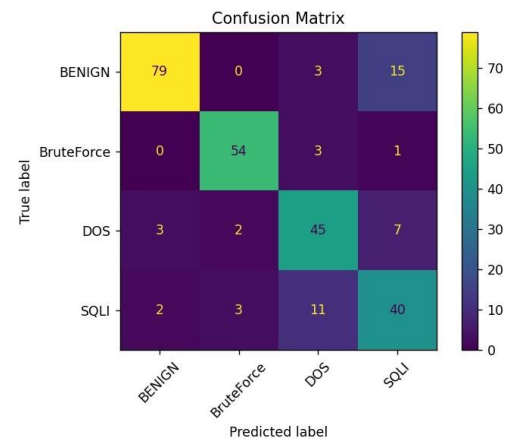


Fig -1: Confusion Matrix

Once the data is cleaned and encoded, the features are selected and formatted for model input. The system focuses on predicting whether a particular traffic flow is benign or malicious, and if malicious, it classifies it into specific categories like BruteForce, Denial-of-Service (DoS), or SQL Injection (SQLI). Extreme gradient boosting classifier is chosen due to its robustness against overfitting, its ability to handle mixed-type data, and its interpretability. The trained model is deployed using FastAPI, which acts as the backend inference engine. The prediction results are visualized using a web-based dashboard and stored in a MySQL database, enabling continuous monitoring and analysis of incoming network traffic.

## 7. MODEL TRAINING

The dataset used for model training includes labeled traffic flows, each described by 12 structured features and one output label. Features such as packet size, source and destination ports, protocol, TTL, and encoded IP addresses are used as input to the model. Before training, the dataset is shuffled and split into training and test sets using an 80:20 stratified split to maintain class distribution. Due to the class imbalance commonly found in cybersecurity datasets, class weights are calculated and incorporated into the model to ensure minority attack classes receive appropriate attention during learning.

```

Classification Report:
              precision    recall  f1-score   support

   BENIGN      0.90      0.77      0.83        97
  BruteForce  0.97      0.97      0.97        58
     DOS      0.76      0.82      0.79        57
     SQLI      0.62      0.71      0.66        56

 accuracy      0.81      0.82      0.81       268
 macro avg      0.81      0.82      0.81       268
weighted avg      0.83      0.81      0.82       268

Model and encoders saved successfully.

[Done] exited with code=0 in 4.835 seconds
  
```

**Fig -2: Classification Report**

The Extreme Gradient Boosting Classifier model is configured with 100 trees, a maximum depth of 100, and constraints on minimum sample splits and leaf sizes to reduce the risk of overfitting. Label encoders for the input and target columns are saved using joblib to ensure compatibility during the prediction phase. After training, the model is evaluated for accuracy and saved along with all necessary preprocessing components. This ensures the model can be deployed consistently and reused for real-time threat classification without retraining. The entire training pipeline is modular, making it suitable for updates with new datasets or model variations in the future.

### 8. EXPERIMENTAL SETUP

The implementation and experiments were conducted on a local machine using Python 3, Scikit-learn, and supporting libraries such as Pandas, Matplotlib, and Joblib. The labeled training data was sourced from custom-annotated logs and formatted as a CSV file with features that reflect actual packet-level network attributes. Real-time test data follows the same structure, excluding the label column, and is collected through simulated network traffic scenarios to ensure evaluation under realistic conditions.

For deployment, FastAPI was used to build the RESTful backend service responsible for real-time inference using the trained model. The system is integrated with a MySQL database where prediction logs are stored and retrieved by a React-based frontend dashboard. This architecture supports real-time visualization and system monitoring. Evaluation metrics such as accuracy, precision, recall, F1-score, and confusion matrix plots were used to measure performance, with results displayed both in the console and graphically for clarity.

### 9. TRAINING AND EVALUATION

The Extreme gradient boosting classifier was evaluated using a separate test set of 268 samples to assess its performance on unseen data. The classification report indicated a weighted average precision of 82% and recall of

81%, confirming the model's ability to generalize effectively. High accuracy was observed for BENIGN and Brute Force classes, while DOS and SQLI showed slightly lower recall due to a smaller number of samples in the dataset. The confusion matrix visualization revealed a well-balanced classification performance across most classes.

[16 rows x 12 columns]

```

✓ Total predictions: 16
✓ Prediction breakdown:
Prediction
BENIGN      14
BruteForce   1
DOS          1
Name: count, dtype: int64
  
```

**Fig -3: Training Result**

To further test real-world applicability, the model was evaluated on a dataset of 16 real-time traffic entries. Out of these, 14 flows were correctly identified as BENIGN, while one Brute Force and one DoS attack were successfully flagged. Safe domain filtering logic was incorporated to prevent false alarms on trusted domains like YouTube and Twitter. Overall, the system demonstrated reliable detection, minimal false positives, and readiness for practical deployment in live network environments. Its modular and extensible design allows for future improvements, such as integrating more attack types or refining the feature set.

### 10. OPPORTUNITIES

- **Real-time automation of threat response:** On their own, AI-powered systems can identify, recognize, and react to threats in real time, lessening the effects of an attack and bringing things under control sooner. They also streamline the process significantly, especially when dealing with multiple threats.
- **Scalability to large enterprise networks:** Because AI-driven intrusion detection systems are often built modularly, it is easy to deploy them onto large or scattered networks. This flexibility is ideal for organizations that have complex configurations. The system can expand with the network, ensuring reliable threat surveillance at all scales.
- **Integration with SIEM and cloud platforms:** The solution is readily compatible with cloud platforms and existing Security Information and Event Management (SIEM) solutions. Improved analysis, smarter warning management, and centralized logging are enabled by this. It helps to better

understand what's happening in both on-premise and cloud systems by integrating seamlessly.

- **Real-time automation of threat response:** Artificial intelligence (AI)-driven systems are designed to detect, categorize, and respond to threats in real-time—without human intervention. This quick response gets things in check much faster and assists in minimizing the damage. It keeps the system running smoothly and efficiently, which is particularly beneficial when faced with a wave of attacks.

- **Scalability to large enterprise networks:** The AI-based intrusion detection system's modularity makes deployment easier across large or distributed networks. This is perfectly suited for complexly configured businesses. The system can expand at the same rate as the network, ensuring precise threat detection irrespective of infrastructure size.

- **Integration with SIEM and cloud platforms:** Centralizing logging, analysis, and linking similar warnings is easier using the system due to its direct integration with cloud platforms and modern SIEM products. Such integration supports greater situational awareness as well as total visibility, especially in complicated systems that consolidate on-premises and cloud tech.

- **Continuous learning through feedback loops:** Machine learning models can, over time, become better at detecting risks by being updated with new data and new insights from security professionals. Through this, the system becomes more adaptive and sensitive to changing patterns of assault. Continuous learning reduces the necessity of constant manual tweaking or upgrading.

- **Reducing dependency on human analysts:** By removing the necessity for constant monitoring, automating the threat detection and response process takes a huge amount of pressure off security staff. Rather than getting bogged down by routine tasks, this allows analysts to spend their time on more complex and valuable subjects. Overall productivity increases as a consequence, and SOC teams are much less likely to suffer from burnout.

- **Opensource dataset and tool ecosystem:** Opensource, high-quality datasets and tools supporting AI-based security research and development are increasingly available. This speeds up the innovation process while reducing development costs. In addition, community-based resources are crucial to improve model benchmarking and ensure that results can be reproduced consistently.

## 11. CONCLUSIONS

To recognize and categorize network threats in real time, this paper introduces an AI-powered intrusion detection system that employs Extreme gradient boosting classifier. The system facilitates automated threat detection with minimal human intervention by integrating MySQL for

dashboard visualization with FastAPI for backend processing. Experiments have shown good categorization accuracy and efficacy across a variety of types of assaults. This approach holds great promise for implementation in real-world network environments. The system may be expanded to support more variety in security demands using extra information and optimization.

## REFERENCES

- [1] A global cyber-threat intelligence system with artificial intelligence and convolutional neural network Fahim Sufi Monash University, Melbourne, VIC 3004, Australia
- [2] Actionable Cyber Threat Intelligence using Knowledge Graphs and Large Language Models, Romy Fieblinger, Md Tanvirul Alam, Nidhi Rastogi
- [3] A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making Martijn Dekker LampisAlevizos
- [4] A global cyber-threat intelligence system with artificial intelligence and convolutional neural network, Fahim Sufi, Monash University, Melbourne, VIC 3004, Australia
- [5] A Comparative Study of AI-based Intrusion Detection Techniques in Critical Infrastructures, SAFA OTOUM, College of Technological Innovation, Zayed University, UAE BURAK KANTARCI AND HUSSEIN MOUFTAH, University of Ottawa
- [6] AI Use in Enhancing Cybersecurity for Safeguarding Digital Information, Ruibin Wang, Dongying Vocational Institute, Dongying, China
- [7] AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation, KAVITHA DHANUSHKODI AND S. THEJAS, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India
- [8] AI-DRIVEN THREAT DETECTION AND RESPONSE: A PARADIGM SHIFT IN CYBERSECURITY, Asad Yaseen
- [9] AI-Powered Ransomware Detection Framework, Subash Poudyal, Dipankar Dasgupta, Department of Computer Science, The University of Memphis, Memphis, TN, USA
- [10] An Artificial Intelligence-Based Intrusion Detection System using Optimization and Deep Learning, J. Electrical Systems 20-6s (2024): 1200-1217 1200, Satish Kumar Garapati, AN. Sigappi
- [11] D. Arivudainambi, B. Sridharan, M. Manikandan, T. Durga, S. Rani, and K. Prabakaran, "AI Use in Enhancing Cybersecurity for Safeguarding Digital Information," 2023 IEEE International Conference on Contemporary Computing and Communications (InC4), 2023, pp. 1–6.

- [12] S. S. Chakravorty, M. M. Hassan, A. Alqahtani, E. Ahmed, and D.-N. Le, "AI-Powered Ransomware Detection Framework for IoT Networks," 2020 International Conference on Computing, Networking and Communications (ICNC), pp. 674–679.
- [13] S. Sampath, G. R. Kanagachidambaresan, M. Ajay, and S. C. Pandian, "A Comparative Study of AI-based Intrusion Detection Techniques in Critical Infrastructures," *Materials Today: Proceedings*, vol. 61, Part 1, 2022, pp. 47–53.
- [14] Md. K. I. Rahmani, T. Bose, Md. K. N. Rahmani, and Z. Imtiaz, "AI-Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," *Sensors*, vol. 22, no. 21, 2022, pp. 1–20.
- [15] S. Sangeetha, M. Nithya, and K. Deepa, "An Artificial Intelligence-Based Intrusion Detection System using Optimization and Deep Learning," *International Journal of Research in Engineering, Science and Management*, vol. 5, no. 4, Apr. 2022. ISSN: 2581-5782.
- [16] M. Sabitha, R. Sandhiya, and T. Ramesh, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," *Materials Today: Proceedings*, Elsevier, 2022. doi: 10.1016/j.matpr.2022.07.123.
- [17] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)," 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 2015, pp. 1–6.
- [18] A. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," *Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1–6. doi: 10.1109/CISDA.2009.5356528.
- [19] T. Nguyen and G. Armitage, "A Survey of Techniques for Internet Traffic Classification using Machine Learning," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, 2008, pp. 56–76.
- [20] H. Hindy et al., "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, 2020, pp. 2696–2732.
- [21] William Stallings – *Network Security Essentials: Applications and Standards (6th Edition)*, Publisher: Pearson.
- [22] Chwan-Hwa (John) Wu and J. David Irwin – *Introduction to Computer Networks and Cybersecurity*, Publisher: CRC Press.
- [23] Russell Miller – *Machine Learning for Cybersecurity Cookbook*
- [24] Zhiqiang Lin, Xiangyu Zhang – *Artificial Intelligence and Security: Foundations, Methods, and Applications*, Publisher: Packt Publishing.
- [25] Soma Halder and Sinan Ozdemir – *Hands-On Machine Learning for Cybersecurity*, Publisher: Springer.
- [26] Ali Dehghantanha (Editor) – *Cyber Threat Intelligence*
- [27] Pethuru Raj, Anupama Raman – *Intelligent Cybersecurity for Modern Networks*, Publisher: Packt Publishing.
- [28] Aurélien Géron – *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow (3rd Edition)*, Publisher: Springer.
- [29] *A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making* Martijn Dekker LampisAlevizos Publisher: CRC Press