ISSN [Online]: 2583-2654

Cloud Security with Deep Learning- Based Intrusion Detection

[1] Geetha C Megharaj, [2] Premalatha D ,[3]Bijesh Sagar A, [4]Hema Priya K M,
[5]Bhavana S Prabhu, [6]Ramya S R

Department of CSE, Dr. T. Thimmaiah Institute of Technology
KGF, India

Abstract: Cloud technologies have significantly influenced infrastructure design, allowing scalable and economical on-demand services across diverse environments. However, this growth has introduced numerous cybersecurity threats, particularly due to its decentralized and accessible nature. Conventional IDS frequently struggle to detect evolving threats, especially unknown or zero-day attacks, within modern cloud setups. This paper introduces a deep learning-based IDS utilizing Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) models to enhance threat detection accuracy and reduce false alarm rates. The system is evaluated using benchmark datasets to assess its effectiveness in detecting anomalies and mitigating threats. In addition, the paper discusses the deployment challenges, computational demands, and potential future improvements that can further enhance the robustness and adaptability of IDS in complex cloud ecosystems.

Keywords: Cloud Security, Intrusion Detection System, Deep Learning, CNN, RNN, Threat Detection

I. INTRODUCTION

Organizations increasingly rely on cloud solutions to enhance data flexibility and reduce infrastructure overhead. While this innovation has propelled digital transformation across industries, it has also introduced complex security challenges such as DDoS attacks, data breaches, and unauthorized access. Conventional defense mechanisms, including firewalls and signature-based IDS, are often inadequate for the evolving threat landscape.

Deep learning methods have emerged as a powerful approach to secure cloud platforms. These methods surpass traditional IDS by continuously learning from large datasets to identify irregular traffic patterns and adapt to new attack vectors in real time. CNNs and LSTMs can uncover complex and novel intrusion patterns by analyzing both structural and temporal features of network data. This paper presents a Modern deep learning methods offer advanced capabilities for detecting irregular traffic behavior and emerging threat vectors. It outlines the deployment of multiple models and discusses their performance in identifying threats across various cloud scenarios.

Additionally, the system architecture, preprocessing techniques, and training methodologies are explained, along with an evaluation of challenges and future enhancement opportunities.

II. METHODOLOGY

This section outlines the step-by-step process adopted to develop the deep learning-based IDS. The system is trained using open-source datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15.

A. *Data Collection and Preprocessing*

Traffic data is collected from virtualized cloud resources including VMs, containers, and IoT gateways. We applied a preprocessing pipeline involving outlier removal, key feature identification, data normalization, and dataset partitioning:

- Noise Filtering: Removing corrupted and irrelevant data entries.
- Feature Extraction: Identifying critical indicators of intrusions.
- Data Normalization: Ensuring uniform scale across features.
- Dataset Segmentation: Creating training, validation, and test subsets.

B. Feature Selection and Dimensionality Reduction Significant attributes are selected using statistical correlation and PCA to minimize redundancy. This reduces overfitting, enhances detection speed, and improves model generalization.

C. Model Selection and Training

The framework incorporates CNNs for spatial inference, LSTMs for sequence-based learning, and autoencoders for detecting irregular behaviors in unlabeled data.

- CNNs for learning spatial relationships in traffic features.
- LSTMs for detecting temporal dependencies and long-term patterns.
- Autoencoders for unsupervised anomaly detection.

The Model development and training were carried out using TensorFlow and PyTorch, with configurations tailored for each algorithm.

D. Detection and Classification

Trained models monitor live cloud traffic to classify potential threats. Anomalies are categorized based on severity levels, and the model adjusts using reinforcement learning for continuous adaptation.

E. Threat Response: Detected threats trigger automatic countermeasures:

- IP blocking
- Instance isolation
- Alert generation
- Security rule updates

This module interfaces with SIEM tools to enhance incident handling.

F. Evaluation Metrics: The models are evaluated using metrics such as:

- Accuracy
- Precision
- Recall and F1-Score
- False Positive Rate
- Latency and Throughput under live test conditions

G. Deployment and Adaptation: The IDS is deployed in containers across cloud platforms. Federated learning and periodic retraining improve adaptability while protecting data privacy.

H. Feature Learning: All deep learning models contribute to learning high-level abstract representations of traffic behavior. CNNs specialize in spatial extraction, LSTMs in sequence modeling, and autoencoders in anomaly reconstruction.

III. SYSTEM ARCHITECTURE

The IDS architecture includes:

- Data Integration Layer: Aggregates data from cloud services.
- Preprocessing Layer: Normalizes and cleans input.
- Detection Engine: Applies deep learning models.
- Monitoring and Alerting: Notifies users of threats.
- Response Layer: Automates mitigation tasks.

The architecture supports real-time data flow and ensures scalability using container orchestration tools like Docker and Kubernetes. Integration with existing cloud services and SIEM solutions ensures seamless threat intelligence flow.

ISSN [Online]: 2583-2654

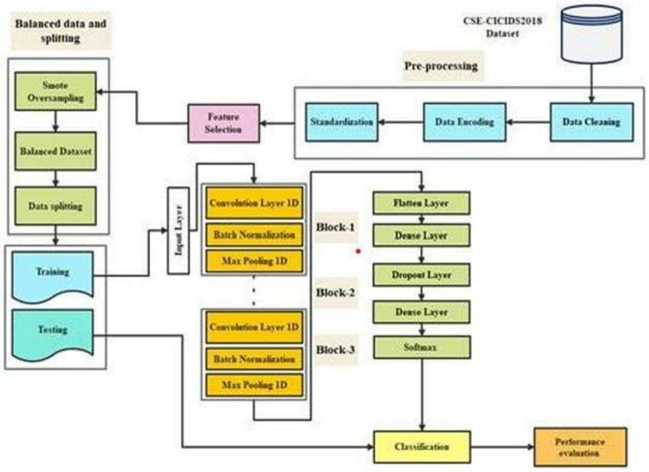


Fig-1 System Architecture

IV. DATA FLOW DIAGRAM

The data flow illustrates the lifecycle of network traffic from ingestion to detection:

1. Data is collected from cloud nodes.
2. Preprocessing filters noise and structures input.
3. The detection engine analyzes data using deep learning.
4. Alerts are generated and responses are executed.

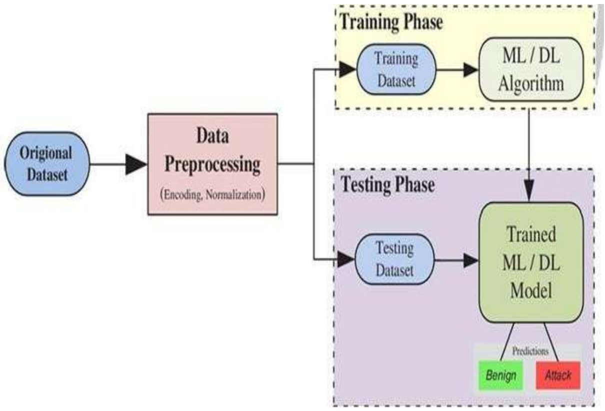


Fig -2 Data Flow Diagram

V. SEQUENCE DIAGRAM

The sequence diagram illustrates the dynamic flow of interactions between major components involved in the deep learning-based intrusion detection system within a cloud environment. It outlines the chronological exchange of data and control signals between the system modules to detect, classify, and respond to potential security threats.

The process begins when the Cloud Security Administrator initiates the monitoring operation. The Cloud Infrastructure generates real-time data, which is captured by the Data

Collector module. This data includes logs, traffic patterns, and system events.

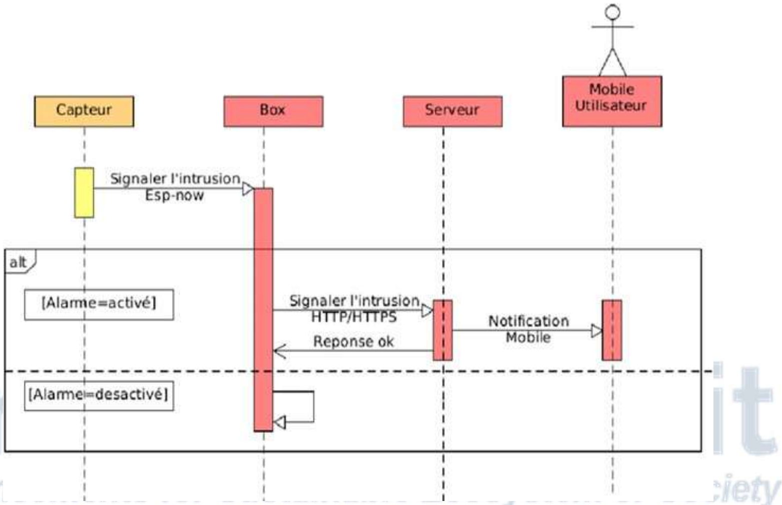


Fig -4 Sequence Diagram

Once collected, the information is sent to the Preprocessing Unit, which is responsible for cleaning the raw data, normalizing inputs, and extracting relevant features. These preprocessed inputs are then forwarded to the Deep Learning Engine, which consists of trained models like CNNs, RNNs, or LSTMs. The engine analyzes the data to identify patterns associated with known or anomalous threats.

If suspicious activity is detected, the Alert Manager component is triggered. It classifies the threat based on severity and initiates the Automated Response System, which can carry out predefined actions such as blocking malicious IP addresses, isolating affected resources, or generating real-time notifications.

ISSN [Online]: 2583-2654

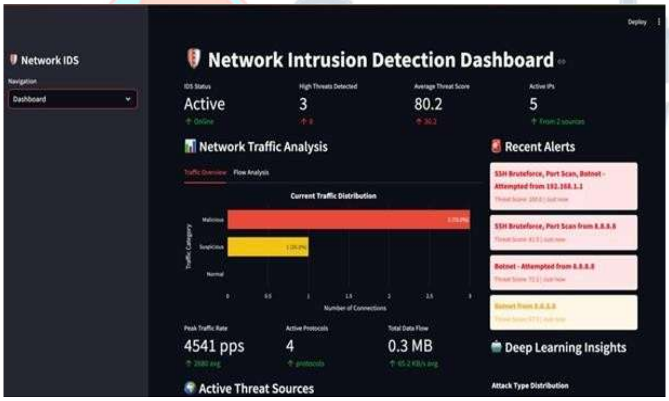
Finally, the Security Dashboard displays the incident summary, visual analytics, and live alerts to the administrator, completing the sequence.

This flow ensures a real-time, intelligent intrusion detection process that enhances cloud security through automation and deep learning.

VI. SYSTEM OUTPUT

The system generates logs and visual outputs that demonstrate the effectiveness of the trained deep learning models. Key output components include:

- Confusion matrices displaying classi0fication accuracy.
- Real-time detection logs showing flagged anomalies.
- Graphs illustrating model performance
- Dashboard visualizations for monitoring active cloud threats.



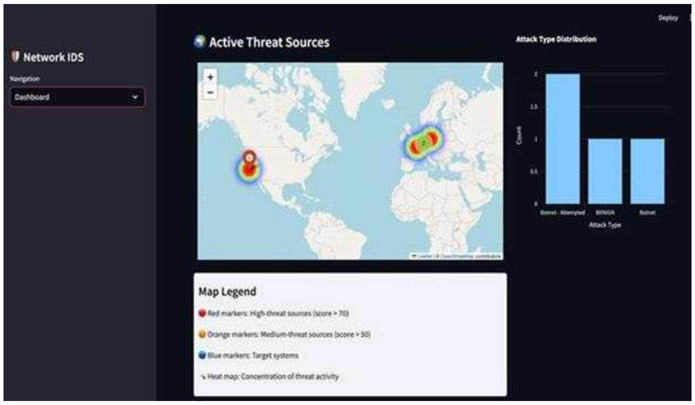
Network Intrusion Detection Dashboard

IDS Status: Active ↑ Online
High Threats Detected: 3
Average Threat Score: 80.2
Active IPs: 5 ↑ From 2 sources

Recent Alerts
SSH Bruteforce, Port Scan, Botnet - Attempted from 192.168.1.1
SSH Bruteforce, Port Scan from 8.8.8.8
Botnet - Attempted from 8.8.8.8
Botnet from 1.1.1.1

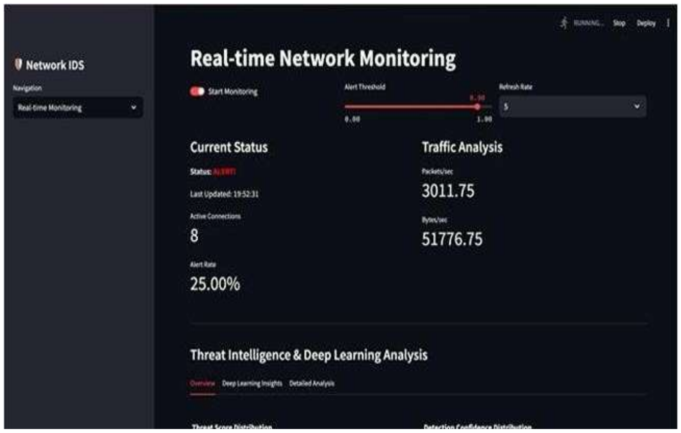
Peak Traffic Rate: 4541 pps
Active Protocols: 4 ↑ protocols
Total Data Flow: 0.3 MB

Fig -4 Dashboard



Map Legend
🔴 Red markers: High-threat sources (score > 70)
🟠 Orange markers: Medium-threat sources (score > 50)
🔵 Blue markers: Target systems
Heat map: Concentration of threat activity

Fig-5 Active Threat Source



Real-time Network Monitoring

Start Monitoring
Alert Threshold: 0.00 – 1.00
Refresh Rate: 5

Current Status
Status: ALERT!
Last Updated: 19:52:31
Active Connections: 8
Alert Rate: 25.00%

Traffic Analysis
Packets/sec: 3011.75
Bytes/sec: 51776.75

Threat Intelligence & Deep Learning Analysis

Fig-6 Real-Time Network Monitoring

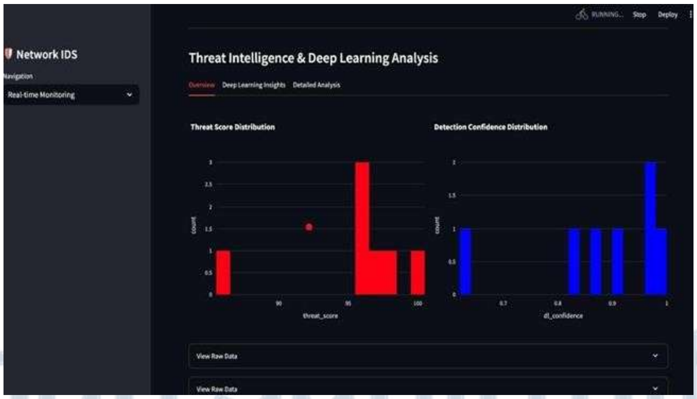


Fig-7 Threat Intelligence & Deep Learning Analysis

VII.CONCLUSION

We presented a deep learning-integrated IDS designed to operate within modern cloud infrastructures. Through a layered architecture, the system improves detection accuracy and operational resilience. The inclusion of both supervised and unsupervised learning provides robustness against known and novel threats. Automated response functions reduce manual intervention and response times.

VIII.FUTURE WORK

Future improvements may include integrating edge-based detection, explainable AI (XAI), and blockchain for audit trails. Also, federated learning will enable secure, collaborative threat detection across cloud environments while preserving data privacy.

REFERENCES

[1] M. Jouini and L. B. A. Rabai, "A security model for safe cloud computing environments," in Cloud Security: Principles and Practices, IGI Global, pp. 249–263, 2019.

[2] P. Saini, S. Behal, and S. Bhatia, "Identifying DDoS attacks using machine learning," in IEEE Conf. on Computing for Sustainable Global Development, New Delhi, India, pp. 16– 21, Mar. 2020.

[3] L. Wang et al., "Overview of cloud computing concepts," New Generation Computing, vol. 28, no. 2, pp. 137–146,2010.

[4] M. Bakro et al., "Encryption performance in cloud environments," in Advances in Intelligent Computing, Springer, pp. 357–367, Dec. 2020

[5] H. El Alloussi et al., "Security in Cloud Computing: A Survey," in Proc. INTIS, Morocco, Nov. 2012.

[6] J. Gu et al., "Intrusion detection using ensemble SVMs with augmented features," Computers & Security, vol. 86, pp. 53–62, 2019.

[7] D. I. Edeh, "Intrusion Detection via Deep Learning," M.S. thesis, Dept. of Computing, Univ. of Turku, Finland, 2021.

[8] H. Attou et al., "Machine learning-based IDS for cloud environments," Big Data Mining and Analytics, vol. 6, no. 4, pp. 311–320, 2023.

[9] A. Aldallal, "Hybrid deep learning for intrusion detection," Symmetry, vol. 14, no. 11, p. 1916, 2022.

[10] D. Srilatha and G. K. Shyam, "Intrusion detection using kernel fuzzy logic and deep networks," Cluster Computing, vol. 24, no. 4, pp. 2657–2672, 2021.

[11] S. N. Mighan and M. Kahani, "Scalable IDS with deep learning," Int. J. Inf. Security, vol. 20, no. 3, pp. 387–403, 2021.

[12] H. Liu and B. Lang, "Review of ML/DL techniques in intrusion detection," Applied Sciences, vol. 9, no. 20, p. 4396, 2019.

[13] R. I. Farhan et al., "Binary PSO-optimized deep learning for cloud IDS," J. Al-Qadisiyah Comput. Sci. Math., vol. 12, no. 1, pp. 16–27, 2020.

[14] O. Bamasag et al., "RT-AMD: Real-time DDoS detection for cloud services," PeerJ Comput. Sci., vol. 7, e814, 2022.