AI-Based Security Device for Cloud Computing

Mande Priyanka Santosh[1]; Malve Swaraj Sanjay[2];
Chaugule Sonali Dyaneshwar[3]; Chaugule Swapnali Dyaneshwar[4]

[1,2,3,4]Assistant Professor

[12,3,4]Jaihind Institute of Management and Research, Kuran – Vadgaon Sahani, Maharashtra, India &
Jaihind College of Engineering, Kuran, Maharashtra, India

Publication Date: 2025/05/31

Abstract: Cloud computing is a promising and inexpensive solution for scaling and cost-effective computing of high quality. Aspects of cloud computing that are frequently encountered include serious security issues such as confidentiality/integrity threats as well as access control threats. In this paper, we propose an artificial intelligence-based security device which uses machine learning algorithms to detect and mitigate threat in cloud environments in real time. The proposed device is based on a deep learning-based intrusion detection system (IDS) trained on set of cloud traffic datasets including NSL-KDD and CICIDS2017 which uncover anomalies and vulnerabilities to detect and defend against threats. We utilize supervised learning models such as Random Forest and LSTM to obtain highly accurate threat classification and response metrics. Results of experiments show that the proposed device has 96. 3% detection accuracy and low false positives compared to traditional IDS systems. The proposed device can also learn to adapt and response to new threats by continuously learning using continuous learning mechanisms. Our work suggests that intelligent systems can be applied in cloud security frameworks in order to achieve a more resilient and self-sustaining defence architecture. This contribution comes with the benefits of proactive threat management and also improves trust in cloud service providers, especially enterprise in sensitive data management. Further works will explore implementation of federated learning for privacy-preserving model training across distributed cloud systems.

Keywords: *Cloud Computing, AI Security, Intrusion Detection System, Machine Learning, Data Protection, Deep Learning.*

How to cite: Mande Priyanka Santosh; Malve Swaraj Sanjay; Chaugule Sonali Dyaneshwar; Chaugule Swapnali Dyaneshwar; (2025) AI-Based Security Device for Cloud Computing. *International Journal of Innovative Science and Research Technology,* 10(5), 2661-2663. https://doi.org/10.38124/ijisrt/25may922

I. INTRODUCTION

Cloud computing revolutionized data storage and processing in the cloud and also produced new security issues and vulnerabilities to business and individuals in a new form of a security threat. New security threats:

- Unauthorized access to the data
- Physical access to the data
- Complex high-level cyber attacks

While AI-based security devices have not been usually successful in securing enterprises and individuals, there has been a trend for AI-based security devices. In this paper we propose a new artificial intelligence-based security device which is capable of responding and detecting a security event in real time for confidentiality and integrity of the cloud storage of data.

II. LITERATURE REVIEW

One revolutionary strategy to counter the increasing number of cyberthreats is the incorporation of artificial intelligence (AI) into cloud security. Through automated response systems, anomaly analysis, and real-time threat detection, researchers have thoroughly examined how machine learning and deep learning algorithms can improve the security posture of cloud infrastructures.

An AI-based data classification model was presented by Bhuvana et al. (2024) with the goal of enhancing cloud security. Through automated feature selection and classification, their research highlights the significance of intelligent systems in differentiating between benign and malicious activities. The study found that using supervised learning algorithms like Decision Trees and Support Vector Machines increased the accuracy of identifying complex cloud threats.

For effective data storage in cloud computing, Parkash and Mittal (2024) suggested an improved security framework that makes use of Particle Swarm Optimization (PSO). Through resource allocation optimization and security parameter tuning, their work focuses on enhancing data confidentiality and integrity. The responsiveness of AI models in cloud environments is improved by this optimization.

In order to improve cloud network security, Wang and Yang (2025) investigated AI algorithms. Their method demonstrated the potential for high adaptability in dynamic threat environments by combining rule-based systems with anomaly detection models. Better identification of unknown vulnerabilities and zero-day attacks in cloud infrastructures was made possible by the use of hybrid models.

A thorough investigation into the integration of cloud security architectures with AI and machine learning was carried out by Abdel-Wahid (2024). The study demonstrated how AI can be used to address conventional

An AI-enabled system for quick cyber incident response in cloud environments was created by Farzaan et al. in 2024. Convolutional neural networks (CNNs), a deep learning technique, were used by their system to monitor network traffic and send out real-time alerts. The outcomes showed improved accuracy and responsiveness, particularly when advanced persistent threats were present.

All of these studies show that artificial intelligence (AI) and machine learning have a lot to offer cloud security, especially when it comes to intrusion detection systems (IDS) and real-time monitoring tools. Nonetheless, there are still issues with data privacy, model interpretability, computational overhead, and the requirement for sizable labelled datasets. These revelations offer a strong basis for creating AI-based cloud security systems that are more intelligent, flexible, and privacy-preserving.

III. METHODOLOGY

A pre-processing engine, a threat detection process, and a data collection process comprise the device's architecture. Publicly available datasets (NSL-KDD, CICIDS2017) are used to gather, label, and store network traffic data. Normalization and feature extraction are examples of pre-processing data. The gadget uses a variety of models. While a long short-term memory (LSTM) neural network model finds patterns in temporal or time series data, a random forest classifier model performs the classification output. Tensor Flow is used in Python for model training, and grid search is used for hyperparameter searches. Accuracy, precision, recall, and F1-Score are used to evaluate the device system.

A. Software requirement

➤ *Operating System*

- Ubuntu Linux (preferred for compatibility with machine learning libraries and cloud environments)
- Windows 10/11 (for local development/testing)

➤ *Programming Languages & Frameworks*

- Python 3.8 or above (Main language for model development and integration)

➤ *Machine Learning & Deep Learning Libraries*

- TensorFlow (for LSTM model implementation)
- Scikit-learn (for Random Forest and other ML models)
- Pandas and NumPy (for data handling and preprocessing)
- Matplotlib / Seaborn (for data visualization)

➤ *Model Development Tools*

- Jupyter Notebook / Google Collab (for model training and testing)
- Spyder / VS Code (for development environment)

➤ *Dataset Sources & Management*

- NSL-KDD dataset
- CICIDS2017 dataset
- Tools for data annotation and labelling

➤ *Network Simulation / Virtualization*

- OpenStack (for simulating private cloud environment)
- Wireshark or similar (for capturing and analysing network traffic)

➤ *API and Integration*

- RESTful API development framework: Flask or Fast API
- JSON-based communication for data transfer

➤ *Cloud & Storage*

- AWS S3 / Google Cloud Storage / Azure Blob (for storing models and logs)
- Docker (for containerization of the AI-based security system)

➤ *Security & Privacy*

- SSL/TLS for secure API communications
- Basic authentication/token-based access control

➤ *Version Control & CI/CD*

- Git (for version control)
- GitHub/GitLab (for collaboration)

- Jenkins or GitHub Actions (for continuous integration/deployment)

IV. RESULTS

The recommended tool got an average finding skill of 96.3% better than the base models like SVM and KNN. Mistake rates were cut by 40% with LSTM added. It took about 1.2 seconds on average to respond to odd happenings, thus allowing close to real-time threat response. Proving how well it works happened under made attack situations in a private cloud setting using and also demonstrating its capabilities were done under made attack scenarios in a private cloud environment via Open Stack.

V. DISCUSSION

Cloud security is being transformed using AI tools, with adaptability and predictive ability. In addition to the compatibility of the device in efficiency of threat detection, the model suffers from computational overhead and data privacy while training the model. Looking at the proposed system, detect known and zero-day attacks healthy through its ability to learn. The main limitation lies in not being able to operate in an unsupervised environment as labelled datasets are required.

In the area of cloud security, AI tools are adopting new paradigms of adaptability and prediction. Along with issues pertaining to the device compatibility in performance of threat detection, the model has computational overhead and data privacy issues in training the model. Looking at the proposed systems, detecting both known and zero-day threats is robust through the ability to learn. The major limitation lies with not being able to work in an unsupervised way since labels are needed for the datasets.

VI. CONCLUSION

The research offered an AI-based security device for possible introducing security into a cloud computing environment by way of intelligent threat detection and response. This technology is designed to be better able to accurately identify and effectively respond to security threats with greater accuracy and adaptive capabilities than existing instruments. Future work with this device would involve implementing federated learning and edge computing, particularly for decentralized cloud services for better scalability and security.

REFERENCES

[1]. Bhuvana, J., Srivastav, V., Singh, P., Mishra, A., & Kaur, S. (2024). Enhancing Cloud Security: Artificial Intelligence-based Data Classification Model for Cloud Computing. *International Journal of Intelligent Systems and Applications in Engineering*, 12(4), 233–240.

[2]. Parkash, D., & Mittal, S. (2024). An Enhanced Security Framework for Storage using PSO in Cloud Computing. *IJISAE*, 11(1), 118–125.

[3]. Wang, Y., & Yang, X. (2025). Research on Enhancing Cloud Computing Network Security using Artificial Intelligence Algorithms. *arXiv preprint* arXiv: 2502.17801.

[4]. Abdel-Wahid, T. (2024). AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning. *International Journal of Information Technology and Electrical Engineering*, 13(3), 145–155.

[5]. Farzaan, M. A. M., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2024). AI-Enabled System for Efficient Cyber Incident Response in Cloud Environments. *ArXiv preprint* arXiv: 2404.05602.