Journal of Innovative Technologies
https://journalinnotech.com/
Vol 1(1) 2025

AI-Based Intrusion Detection and Security Threat Analysis in Cloud Computing

Emily J. Anderson
Faculty of Computing & Data Sciences, Boston University, Boston, MA, USA
Corresponding Email: emilyanderson.cds@gmail.com

Abstract

Cloud computing provides flexible and scalable infrastructure for storing data, hosting applications, and delivering digital services. However, the increasing use of cloud platforms has also introduced security challenges, including unauthorized access, malicious network activity, data breaches, and distributed attacks. Traditional security mechanisms often depend on predefined rules and known attack patterns, which may not identify unfamiliar or rapidly changing threats. Artificial intelligence offers new opportunities to strengthen cloud security by analyzing network traffic, user activities, and system behavior to identify suspicious patterns. This paper presents an AI-based approach for intrusion detection and security threat analysis in cloud computing environments. The proposed approach collects relevant security information, processes network and system data, and applies machine learning techniques to classify normal and potentially malicious activities. The methodology considers detection accuracy, precision, recall, and false alarm rates to evaluate security performance. It also examines how intelligent threat analysis can support faster security responses and improve the protection of cloud resources. The proposed approach provides a framework for developing adaptive intrusion detection systems that can respond to changing security conditions. Its effectiveness depends on the quality of training data, model performance, and the ability to distinguish legitimate activities from malicious behavior.

***Keywords*:** Artificial Intelligence, Cloud Computing, Intrusion Detection, Cybersecurity, Machine Learning, Threat Analysis, Network Security

1. Introduction

Cloud computing has transformed the way organizations store information, manage applications, and access computing resources. Instead of maintaining all computing infrastructure locally, organizations can use cloud platforms to operate services through distributed networks and shared resources. Although this model provides flexibility and scalability, it also creates security risks because cloud environments depend on network communication, remote access, and interconnected services.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

Cloud security threats include unauthorized access, malicious login attempts, denial-of-service attacks, suspicious network traffic, and attempts to exploit software vulnerabilities. These threats can compromise confidential information, interrupt services, and affect the availability of cloud resources. As cloud environments become larger and more complex, monitoring every activity through manual inspection becomes increasingly difficult.

Traditional intrusion detection systems commonly use predefined signatures or fixed detection rules to identify suspicious activities. These systems can detect known threats effectively when accurate signatures are available. However, they may struggle with unfamiliar attack patterns, changing network behavior, and threats that do not match previously defined rules. This limitation creates a need for more adaptive security monitoring approaches.

Artificial intelligence can improve intrusion detection by learning patterns from network traffic, access records, and system activities. Machine learning models can distinguish normal behavior from suspicious activity and identify unusual patterns that may indicate security threats. This paper proposes an AI-based intrusion detection approach for cloud computing environments, focusing on intelligent data analysis, threat classification, and security response support.

2. Security Threats in Cloud Computing

Cloud computing environments face several categories of security threats because applications, databases, virtual machines, and network services operate within interconnected infrastructure. Unauthorized access is one of the major concerns, as attackers may attempt to obtain access through compromised credentials, weak authentication mechanisms, or misconfigured permissions. Once access is obtained, sensitive information and cloud resources may become vulnerable[1].

Network-based attacks are another important security concern. Distributed denial-of-service attacks can generate excessive traffic and affect service availability. Malicious scanning activities may identify exposed services and potential vulnerabilities, while unusual communication patterns can indicate unauthorized data transfers or compromised systems.

Cloud environments may also experience account misuse and privilege-related threats. An attacker using a compromised account may access resources that are normally restricted to authorized users. Similarly, excessive permissions can increase the impact of an account compromise. Monitoring user behavior and access patterns is therefore important for identifying suspicious activity.

Traditional security mechanisms remain useful for enforcing access policies, filtering network traffic, and detecting known attack signatures. However, their effectiveness may decrease

when threats change or when malicious activity resembles legitimate operations. AI-based security analysis can complement these mechanisms by examining multiple indicators together and identifying patterns that may not be covered by fixed detection rules.

3. Proposed AI-Based Intrusion Detection Framework

The proposed framework uses artificial intelligence to monitor and analyze security-related activities in cloud computing environments. Its first component collects information from network traffic, authentication records, system logs, and cloud monitoring services. These records provide information about communication patterns, access attempts, resource usage, and other activities that may indicate suspicious behavior .

The collected information is processed before being provided to the machine learning model. Data preparation includes removing incomplete records, handling inconsistent values, selecting relevant features, and converting available security information into a suitable format. This stage is important because inaccurate or incomplete data can negatively affect intrusion detection performance.

The AI detection component analyzes the prepared information and classifies activities as normal or potentially malicious [2]. Depending on the selected model, the system may use supervised learning with labeled attack records or anomaly detection to identify unusual behavior without requiring every threat to be previously labeled. The model can also assign risk scores to suspicious activities to support further investigation.

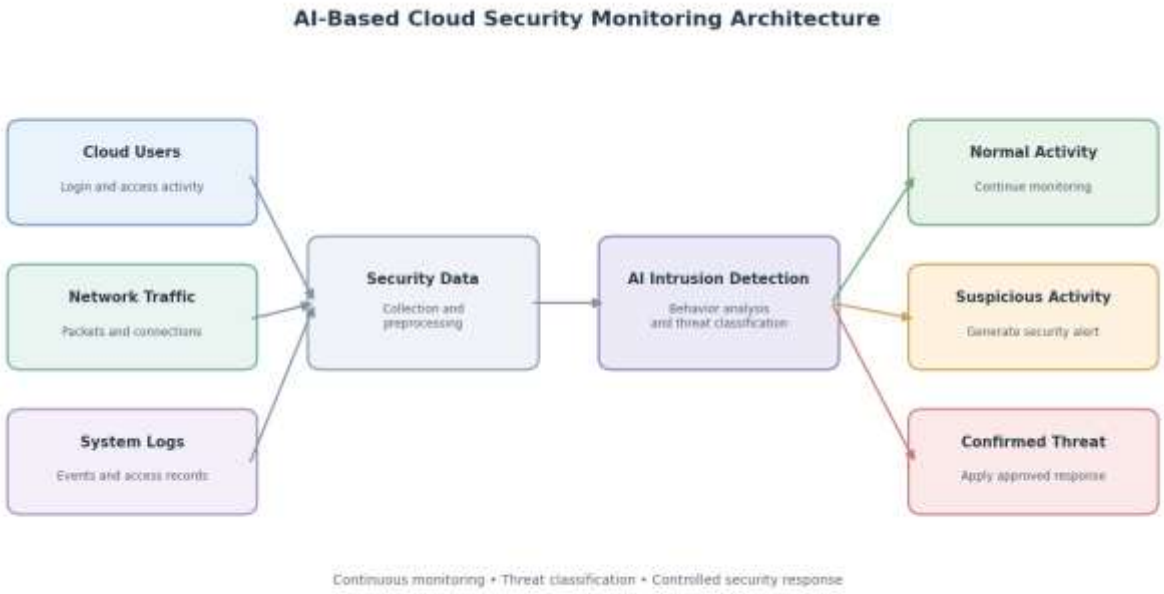


Figure 1: AI-based cloud security monitoring architecture for intrusion detection and threat analysis.

The final component supports security monitoring and response. When suspicious activity is detected, the system can generate an alert for security administrators or recommend an appropriate action. Possible responses include reviewing an account, restricting suspicious access, applying additional authentication, or investigating unusual network communication. Important security actions should follow established policies and authorization procedures to avoid blocking legitimate users unnecessarily [3].

4. Methodology

The proposed methodology uses a cloud security dataset containing network activity records, access information, and labeled examples of normal and malicious behavior. The dataset may include features such as connection duration, packet volume, protocol type, source and destination information, authentication attempts, and traffic frequency. Sensitive information should be removed or appropriately protected before model training.

The dataset is divided into training, validation, and testing subsets. The training data are used to develop the machine learning model, while validation data support model selection and parameter adjustment. The testing data are kept separate to evaluate the model's ability to identify previously unseen observations. When records are time-dependent, chronological separation can help reduce data leakage [4].

A machine learning classifier is trained to distinguish normal activities from potentially malicious activities. Suitable approaches may include decision trees, random forests, support vector machines, or neural networks. The choice of model depends on dataset size, feature characteristics, computational requirements, and the expected detection environment. In addition to detection accuracy and false positive rate, precision is used to evaluate the reliability of positive threat predictions. It determines how many activities classified by the intrusion detection model as malicious are actually associated with security threats [5]. A higher precision value indicates that the model generates fewer false security alerts and provides more reliable threat identification. Detection accuracy is calculated using the following equation:

.

$$Precision = \frac{TP}{TP + FP}$$

Where **TP** represents true positives, referring to malicious activities correctly identified by the model, and **FP** represents false positives, referring to legitimate activities incorrectly classified as malicious. Precision is particularly important in cloud security because excessive false alerts can increase the workload of security administrators and lead to unnecessary investigations. Therefore, a higher precision value indicates better reliability in identifying actual security threats.

5. Results and Discussion

The proposed evaluation examines how effectively an AI-based intrusion detection model distinguishes legitimate cloud activities from potentially malicious behavior. The model analyzes selected network and system features and uses learned patterns to classify incoming observations. Its performance depends on the diversity and quality of the dataset used during training and testing.

Detection accuracy provides an overall measure of classification performance, but it does not independently establish that a model is suitable for practical security monitoring [6]. In datasets containing significantly more normal observations than attack records, a model may achieve high accuracy while failing to detect important threats. Precision and recall are therefore necessary to examine the reliability of positive threat predictions and the proportion of actual attacks successfully identified.

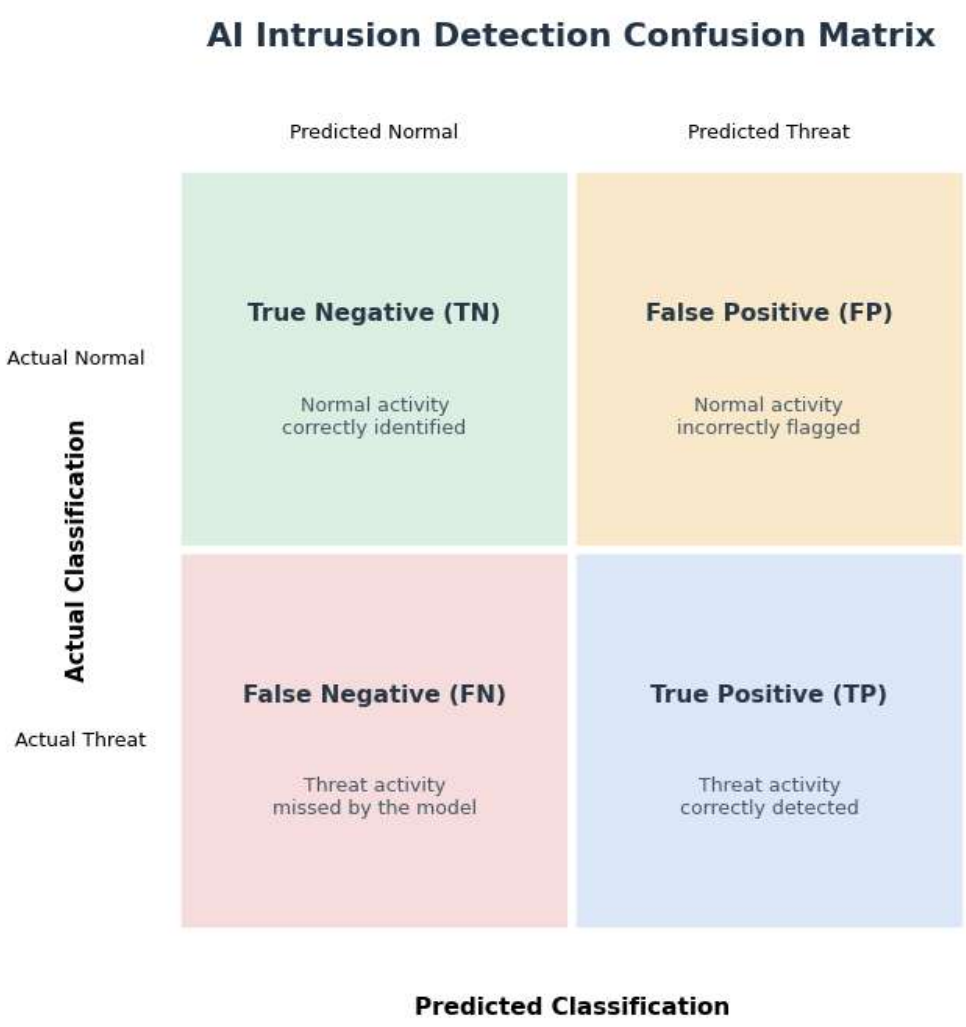


Figure 2: Confusion matrix for evaluating AI-based intrusion detection performance.

False positive rate is also important because frequent incorrect alerts can increase the workload of security administrators[7]. A practical intrusion detection system should identify suspicious activities without generating excessive warnings for legitimate users. Model thresholds can be adjusted according to the security requirements and operational conditions of the cloud environment. The proposed framework can support continuous monitoring by analyzing incoming security information and generating alerts when suspicious patterns are identified. However, its performance should be verified through controlled experiments using representative datasets. Without measured experimental results, no specific improvement in detection accuracy or threat prevention can be claimed.

6. Intelligent Security Monitoring and Threat Response

Intelligent security monitoring extends intrusion detection by continuously examining changes in cloud activity. Instead of analyzing isolated events only, an AI-based system can evaluate patterns across multiple observations[8]. For example, repeated failed login attempts followed by an unusual access location or unexpected resource activity may indicate a compromised account. Combining these indicators can provide more useful security information than evaluating each event independently.

When suspicious behavior is identified, the system can assign a risk level and notify the security team. Low-risk events may require additional monitoring, while higher-risk events may require immediate investigation. Depending on the organization's security policies, responses can include temporarily restricting access, requiring additional authentication, isolating a potentially compromised workload, or blocking confirmed malicious communication.

Automated threat response should be carefully controlled. An incorrect classification could restrict a legitimate account or interrupt an important cloud application. Therefore, high-impact actions should use appropriate verification, authorization, and recovery procedures. Security administrators should also be able to review alerts and understand the information that influenced a model's decision [9].

Continuous feedback can improve the detection process. Confirmed security incidents and incorrectly generated alerts can be reviewed and used to refine the model. Regular evaluation helps identify performance changes when cloud workloads, user behavior, and attack patterns evolve. This makes intelligent security monitoring an ongoing process rather than a one-time model deployment.

7. Challenges and Limitations

AI-based intrusion detection depends on the availability of accurate and representative security data. Training datasets may not contain all possible attack types, and some malicious activities may be incorrectly labeled as normal. Incomplete or outdated datasets can reduce the model's ability to recognize new threats and unfamiliar attack patterns.

Another challenge is the changing nature of cyberattacks. Attackers may modify their techniques to avoid detection, while legitimate cloud workloads may also change over time. This can cause a model trained on historical data to become less effective [10]. Continuous monitoring, model evaluation, and carefully managed updates are necessary to address these changes.

False positives and false negatives remain important limitations. False positives can generate unnecessary alerts and interrupt legitimate operations, while false negatives may allow malicious activities to remain undetected. Selecting an appropriate detection threshold requires balancing security requirements with operational needs.

Computational overhead is also a consideration. Monitoring large volumes of network traffic and system records can require significant processing and storage resources [11]. The detection system must therefore operate efficiently without creating additional performance problems. Privacy and data protection must also be considered when collecting user activity and network information. Appropriate access controls, data minimization, and secure storage practices are necessary for responsible deployment.

8. Conclusion

This paper presented an AI-based approach for intrusion detection and security threat analysis in cloud computing environments. The proposed framework combines security data collection, data preparation, machine learning-based threat classification, and intelligent response support to strengthen cloud security monitoring. The methodology evaluates intrusion detection performance through accuracy and false positive rate, while precision and recall provide additional information about threat identification. These measures help assess whether the system can distinguish malicious behavior from legitimate cloud activities without producing excessive incorrect alerts. AI-based intrusion detection can complement traditional security mechanisms by identifying suspicious patterns and supporting more adaptive security analysis. However, its effectiveness depends on representative datasets, suitable model selection, continuous evaluation, and carefully controlled response procedures. Future research can investigate deep learning-based intrusion detection, real-time cloud traffic analysis, explainable AI, and adaptive threat classification. These developments may support more reliable security monitoring and improve the protection of cloud computing infrastructure.

REFERENCES:

[1] I. Ikram and Z. Huma, "An Explainable AI Approach to Intrusion Detection Using Interpretable Machine Learning Models," *Euro Vantage journals of Artificial intelligence,* vol. 1, no. 2, pp. 57-66, 2024.

[2] J. Zhao, Q. Yan, J. Li, M. Shao, Z. He, and B. Li, "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data," *Computers & Security,* vol. 95, p. 101867, 2020.

[3] S. K. Mandru, "Machine Learning and AI in Endpoint Security: Analyzing the use of AI and machine learning algorithms for anomaly detection and threat prediction in endpoint security," *Journal of Scientific and Engineering Research,* vol. 8, no. 3, pp. 264-270, 2021.

[4] P. Evangelatos *et al.*, "Named entity recognition in cyber threat intelligence using transformer-based models," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021: IEEE, pp. 348-353.

[5] S. K. Mandru, "Explainable AI for Endpoint Security Threat Analysis," *European Journal of Advances in Engineering and Technology,* vol. 11, no. 1, pp. 56-63, 2024.

[6] J. K. Manda, "AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations," *Educational Research (IJMCER),* vol. 6, no. 2, pp. 333-340, 2024.

[7] A. Kumar, "The impact of AI on predictive performance tuning in cloud computing environments," 2018.

[8] P. Nama, S. Pattanayak, and H. S. Meka, "AI-driven innovations in cloud computing: Transforming scalability, resource management, and predictive analytics in distributed systems," *International research journal of modernization in engineering technology and science,* vol. 5, no. 12, p. 4165, 2023.

[9] N. Karra, R. K. Agrawal, and W. M. A. Tambe, "AI-Driven Cloud Computing: Predictive vs. Conventional Resource Management," *Euro Vantage journals of Artificial intelligence (EVJAI),* vol. 2, no. 1, pp. 76-94, 2025.

[10] M. Bayer, T. Frey, and C. Reuter, "Multi-level fine-tuning, data augmentation, and few-shot learning for specialized cyber threat intelligence," *Computers & Security,* vol. 134, p. 103430, 2023.

[11] N. Mazher and I. Ashraf, "A Survey on data security models in cloud computing," *International Journal of Engineering Research and Applications (IJERA),* vol. 3, no. 6, pp. 413-417, 2013.