Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

Generative AI for Real-Time Cloud Security: Advanced Anomaly Detection Using GPT Models

[1]S Jubeda Banu, [2]S Oshin Wenona, [3]M Shamshunnisa, [4]Y Afaan Ahamad, [5]B Peddaiah, [6]B Noor Mohammed

[1,2,3,4,5,6]Department of Computer Science Engineering (Data Science), GATES Institute of Technology, Gooty, Andhra Pradesh, India
E-mails: [1]jubedashaik123@gmail.com, [2]oshin4jesus2003@gmail.com, [3]shamshunnisamakam@gmail.com, [4]afaanahamed18@gmail.com, [5]boyapeddaiah1840@gmail.com, [6]noormohammed8688@gmail.com

Abstract: Cloud computing has become the backbone of modern digital infrastructure, enabling scalable and flexible services for organizations worldwide. However, the rapid growth of cloud environments has also introduced significant security challenges such as unauthorized access, data breaches, and sophisticated cyberattacks. Traditional security systems rely on rule-based detection mechanisms that often fail to identify unknown threats. This paper proposes a Generative Artificial Intelligence based framework for real-time cloud security monitoring. The proposed system utilizes advanced generative models to analyse cloud logs, network traffic, and user behaviour to identify abnormal patterns that may indicate potential security threats. By leveraging deep learning and generative AI capabilities, the system improves the accuracy and speed of anomaly detection. The proposed approach enhances cloud security by providing intelligent threat detection and real-time monitoring capabilities.

Keywords: Generative AI, Cloud Security, Anomaly Detection, GPT Models, Cybersecurity, Machine Learning.

I. INTRODUCTION

Cloud computing has transformed the way organizations manage digital resources, enabling on- demand access to computing infrastructure, storage, and applications. Major cloud service providers offer highly scalable platforms that allow businesses to deploy services rapidly without investing heavily in physical infrastructure. Despite these advantages, cloud environments face numerous security challenges due to their distributed architecture, multi-tenant nature, and exposure to the internet.

As organizations increasingly migrate sensitive data and critical services to cloud platforms, protecting cloud infrastructure from cyberattacks has become a major concern. Security threats in cloud environments include data breaches, account hijacking, insider attacks, malware infections, and distributed denial-of-service attacks. Traditional cloud security systems rely primarily on signature-based detection or predefined security rules. While these approaches are effective for known threats, they are often unable to detect new or evolving attack patterns.

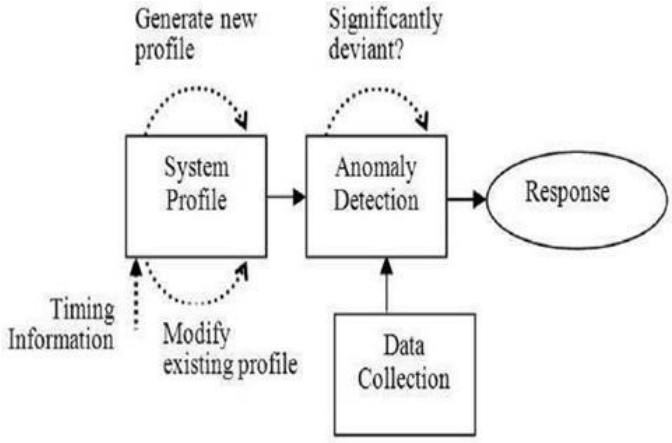
Cloud computing has fundamentally transformed how enter- prises handle data management and storage, offering scalable and flexible solutions that have reshaped business operations across industries. However, with this shift towards cloud infrastructures comes a new set of vulnerabilities that demand more sophisticated security measures. Traditional anomaly detection systems, which rely heavily on predefined rules or the recognition of known threat signatures, have become increasingly inadequate in today's complex cloud environments. These systems struggle to identify zero-day attacks or previously unknown threats, both of which have grown in frequency and sophistication as cyber attackers exploit the dynamic nature of cloud ecosystems. As cloud environments evolve and become more distributed, the limitations of conventional security mechanisms become more pronounced, creating an urgent need for more advanced, real-time, and adaptive anomaly detection techniques to safeguard cloud infrastructures from emerging threats.

In response to these growing challenges, researchers and industry experts have turned to machine learning models, particularly those that can adapt to new patterns and behaviours within cloud environments. Recent advancements in artificial intelligence have

Copyright © 2026 CJESR All Rights Reserved

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

introduced generative models, such as Llama and OpenAI's GPT architectures, as promising candidates for addressing cloud security concerns. These models possess a unique ability to generate and recognize complex patterns in large and diverse datasets, making them ideal for anomaly detection tasks. Unlike traditional methods, which often require frequent updates to keep pace with evolving threats, generative models offer a more flexible and intelligent solution by learning from the data itself, continuously adapting to new forms of attacks as they arise. This capacity for self- learning and adaptation marks a significant shift in how cloud security can be managed, offering a pathway to more resilient and proactive threat detection mechanisms.



The core of this research is the development of a real- time anomaly detection framework based on generative AI models, specifically focusing on the use of Llama and GPT architectures. Our framework is designed to analyse various datasets generated within cloud environments, including cloud logs, network traffic, user behaviour, and system activities, to identify abnormal patterns that may signal a security breach. Traditional anomaly detection systems are often limited in scope, analysing only a narrow range of data sources or failing to provide real-time insights. By contrast, the generative AI approach proposed in this paper leverages the power of largescale models to provide more comprehensive and timely threat detection capabilities. The flexibility of these models also allows for their deployment in multi-cloud environments, addressing one of the key gaps in current research: the need for scalable security solutions that can operate effectively across This study not only explores the theoretical advantages of applying generative AI to cloud security but also seeks to address critical gaps in existing research. One major gap is the limited exploration of generative models for real-time anomaly detection, particularly in the context of cloud computing.

Previous work has largely focused on static or rule- based approaches, which do not account for the dynamic and rapidly changing nature of modern cloud environments. Furthermore, there is a growing need for security frameworks that can scale to accommodate the increasing complexity of multi- cloud deployments, where multiple cloud providers are used simultaneously by enterprises to optimize performance and reduce costs. Our proposed framework offers a novel solution to these challenges, integrating generative AI models that not only enhance the detection of novel threats but also ensure that security measures can scale in line with the expanding use of cloud technologies in enterprise settings.

II. RELATED WORK

Previous studies have significantly advanced the application of machine learning (ML) techniques in the domain of cloud security, particularly focusing on anomaly detection to safeguard cloud infrastructures. Early research in this area often employed supervised learning models, such as decision trees and support vector machines (SVM), to detect abnormal patterns and potential threats in cloud environments. These models have proven effective in identifying known attack vectors by relying on labelled datasets that provide clear distinctions between normal and malicious activities. However, supervised learning approaches face considerable challenges diverse and distributed cloud infrastructures. When dealing with novel, previously unknown threats. The requirement for large,

Copyright © 2026 CJESR All Rights Reserved

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

labelled datasets for accurate training becomes a critical limitation, as such datasets may not always be available or may not capture the full spectrum of potential threats, particularly in the case of emerging or sophisticated cyberattacks.

This dependency on labelled data hinders the adaptability of these models in real time, dynamic cloud environments, where threats evolve rapidly. Moreover, rule-based anomaly detection systems, which have long been a staple in traditional cloud security frameworks, offer limited flexibility when faced with new types of attacks. These systems typically operate by using predefined signatures or behavioural patterns associated with known threats. While effective for identifying well-documented attack vectors, rule-based systems are inherently static and unable to detect novel threats that deviate from pre-established norms.

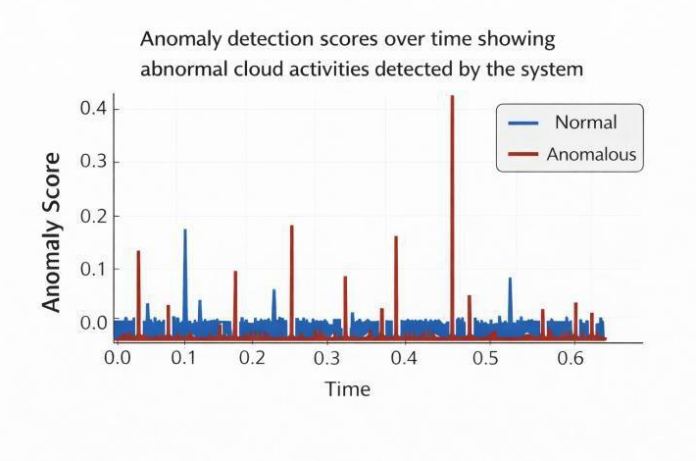
As cyberattacks become more sophisticated and tailored to specific vulnerabilities within cloud environments, the static nature of rule-based systems renders them increasingly ineffective. Attackers can easily modify their methods to avoid detection, thereby bypassing security systems that do not account for previously unseen behaviours. This growing inadequacy of rule based and supervised learning systems has prompted researchers to seek more adaptive and intelligent solutions for anomaly detection in cloud infrastructures.

In contrast to these traditional approaches, recent advancements in generative AI have shown immense potential in revolutionizing cloud security through more adaptive and robust anomaly detection methods. Generative models, particularly those based on architectures such as OpenAI's GPT, have demonstrated their ability to handle large, complex

datasets and extract meaningful patterns from them without the need for extensive labelled data. These models utilize unsupervised or semi-supervised learning techniques, enabling them to detect anomalies based on the structure and relationships within the data itself. By generating predictions from unseen data, generative AI models offer a dynamic approach to identifying threats in cloud environments, adapting to evolving attack patterns in real-time. This adaptability marks a significant departure from the static, rule-based systems, providing a much-needed solution for detecting zero- day attacks and other novel security threats that may go unnoticed by traditional methods.

III. PROPOSED SYSTEM

The proposed system introduces a Generative AI- based architecture for detecting anomalies in cloud environments in real time. The system continuously monitors cloud infrastructure activities and analyses system logs to identify potential security threats.



The architecture consists of several modules. The first module collects log data from cloud platforms such as AWS CloudTrail,

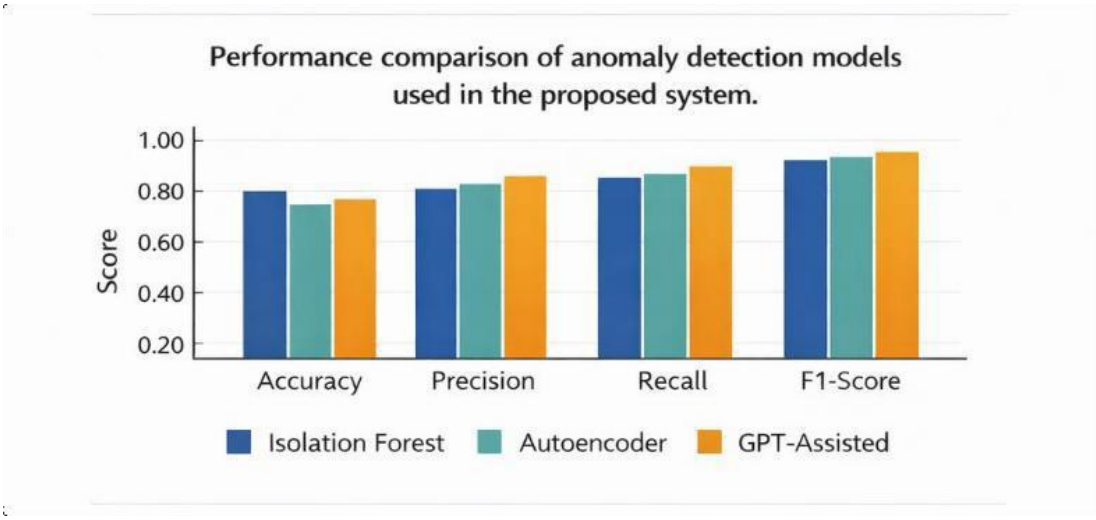
Copyright © 2026 CJESR All Rights Reserved

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

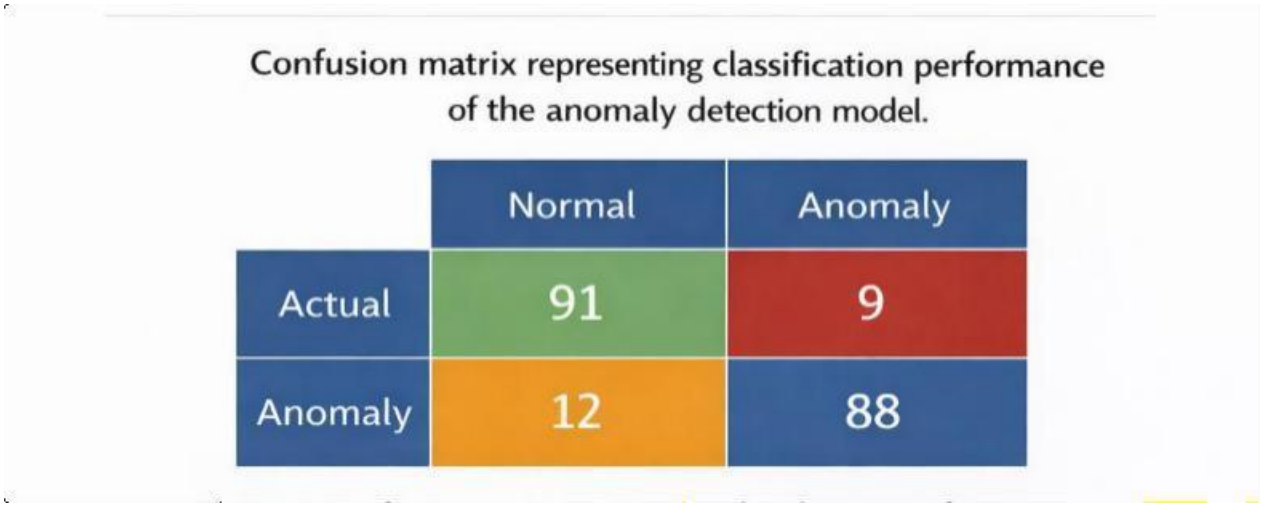
system logs, and network traffic logs. These logs contain information about user activities, system events, and application operation.

The collected data is then passed to a preprocessing module where noise and irrelevant data are removed. This step converts raw log files into structured datasets suitable for machine learning.

After preprocessing, anomaly detection models such as Isolation Forest and Autoencoder models to detect abnormal patterns in system activities. These algorithms learn normal behaviour patterns from historical data and identify unusual events that deviate from these patterns.



Once anomalies are detected, a GPT-based analysis module processes the suspicious log entries and generates contextual explanations for the anomalies. The GPT model helps identify possible attack patterns and provides insights that assist security analysts in understanding potential threats.



Finally, the system generates real-time alerts and notifications for system administrators, enabling faster response and improved cloud security monitoring.

Copyright © 2026 CJESR All Rights Reserved

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

IV. SYSTEM ARCHITECTURE

The proposed system architecture is designed to monitor cloud environments in real time and detect abnormal activities using machine learning and Generative AI models. The architecture consists of several interconnected modules responsible for data intelligent threat analysis.

1. Cloud Data Sources:

The system collects data from multiple cloud infrastructure components. These include cloud service logs, network traffic logs, authentication records, and user activity logs generated from cloud platforms such as AWS, Azure, or Google Cloud. These logs contain valuable information about system operations, login attempts, file access activities, and network communications.

2. Data Collection Module:

The data collection module gathers real-time logs from various cloud monitoring services such as CloudTrail, system monitoring tools, and application servers. These logs are continuously streamed into the monitoring system to ensure that suspicious activities can be detected immediately.

3. Data Preprocessing Module:

Before applying machine learning algorithms, the collected log data undergoes preprocessing. This step involves cleaning the data, removing duplicate or irrelevant records, handling missing values, and converting log entries into structured formats suitable for machine learning analysis. Feature extraction techniques are also applied to identify important attributes such as login frequency, IP address behaviour, access patterns, and system event frequency.

4. Anomaly Detection Engine;

The processed data is then passed to the anomaly detection engine, which uses machine learning algorithms such as Isolation Forest and Autoencoder models. These models learn the normal behaviour patterns of the cloud environment. Any activity that deviates significantly from the learned patterns is identified as a potential anomaly.

5. GPT-Based Log Analysis:

Once anomalies are detected, the suspicious log entries are analysed using GPT-based Generative AI model. The GPT model interprets the log data and generates contextual explanations about the detected anomalies. This helps security analysts understand whether the activity indicates a potential cyberattack, insider threat, or abnormal system behaviour.

6. Alert and Response System:

When an anomaly is confirmed, the system generates real-time alerts for administrators and security teams. These alerts include detailed information about the detected threat, including the type of anomaly, affected resources, and possible causes suggested by the GPT analysis.

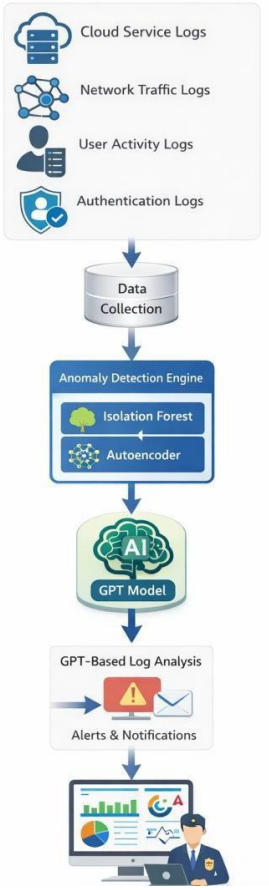
7. Dashboard and Visualization:

The final component of the system is a monitoring dashboard that provides visual insights into system activities, anomaly detection

Copyright © 2026 CJESR All Rights Reserved

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

results, and security alerts. The dashboard allows administrators to monitor cloud security in real time and take necessary actions to mitigate threats.



V. MODELS

1. Isolation Forest:

Isolation Forest is an unsupervised machine learning algorithm designed for anomaly detection. The algorithm isolates abnormal data points by randomly partitioning the dataset. Since anomalies are rare and different from normal observations, they can be isolated more quickly than regular data points. This makes Isolation Forest suitable for detecting unusual patterns in cloud system logs.

2. Autoencoder:

Autoencoders are deep learning models used for unsupervised anomaly detection. The model learns to reconstruct input data by compressing it into a lower- dimensional representation and then reconstructing it back to its original form. When abnormal data is provided as input, the reconstruction error becomes significantly higher, indicating potential anomalies in the system.

3. GPT Model:

Generative Pre-trained Transformer (GPT) is a large language model capable of analysing textual data and generating meaningful

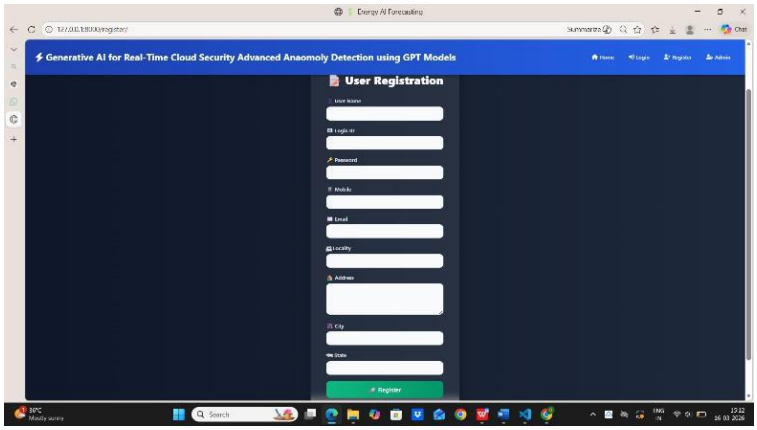
Copyright © 2026 CJESR All Rights Reserved

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

insights. In the proposed system, the GPT model analyses suspicious log entries and provides contextual explanations for detected anomalies. This helps security analysts understand the nature of potential threats and improves the efficiency of incident response.

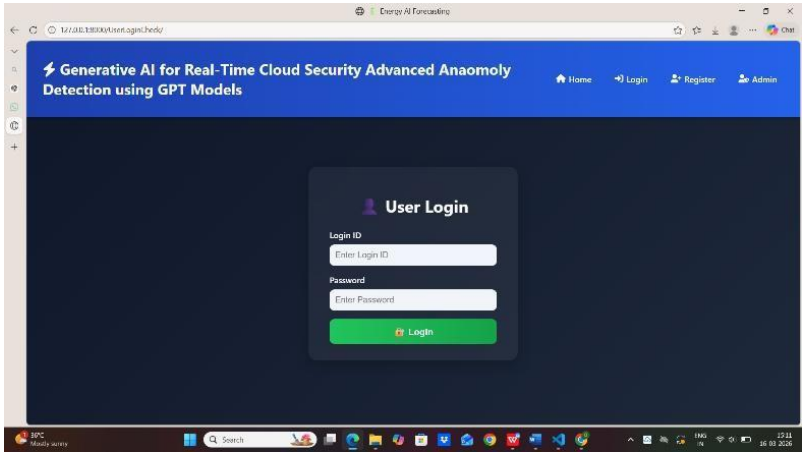
VI. RESULTS

The proposed system was evaluated using cloud system log datasets containing both normal operational activities and simulated attack scenarios. The anomaly detection models were trained using normal system behavior data and tested using datasets containing abnormal patterns. The objective of the evaluation was to analyze the capability of the system to identify suspicious activities and unusual patterns within cloud environments.



To support system access and interaction, a user registration interface was implemented. This interface allows new users to create an account by providin the required credentials, enabling them to access the system features.

After successful registration, users can log in to the system using their credentials through the login interface. This ensures that only authorized users are able to access the anomaly detection functionalities and interact with the system securely.

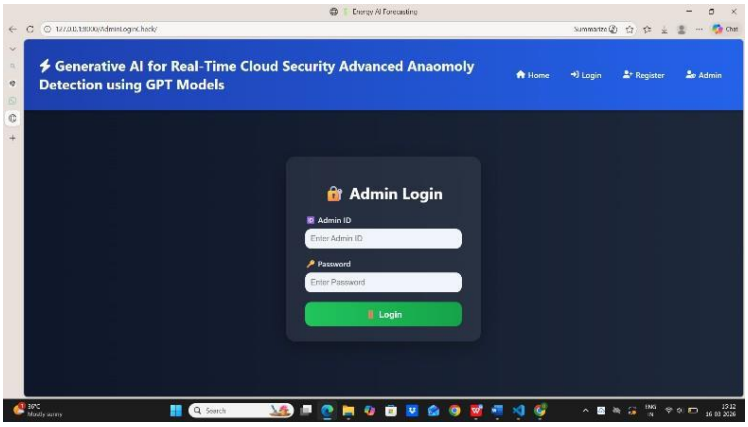


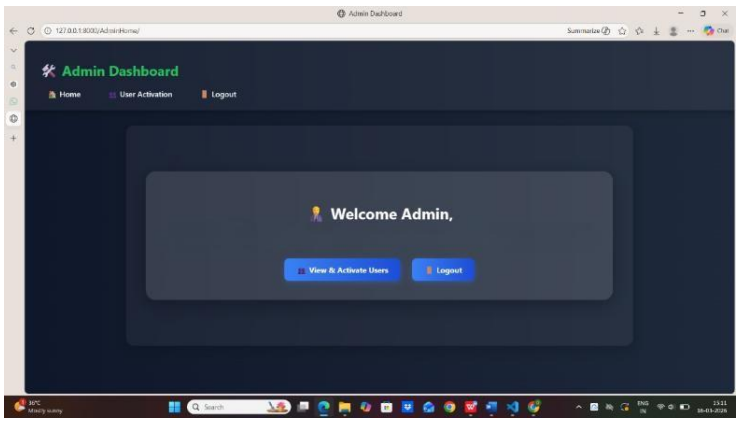
Administrative access is provided through a dedicated login interface. The administrator is responsible for monitoring system activities, managing users, and controlling access permissions. This separation of user and administrator roles helps maintain proper system management and security.

Copyright © 2026 CJESR All Rights Reserved

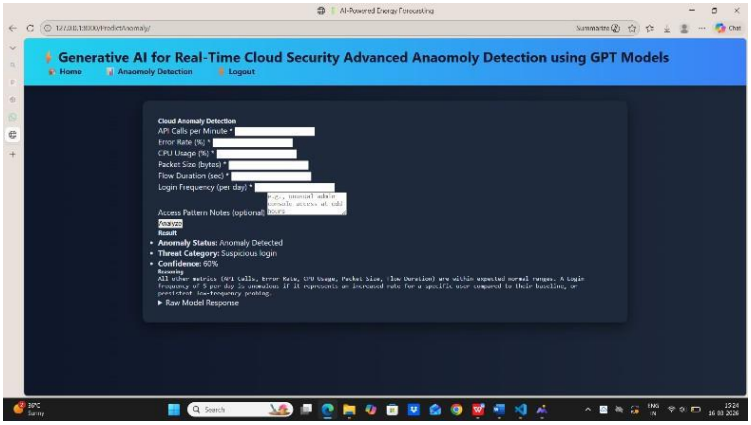
Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

Once authenticated, the administrator can access the dashboard which provides options to view and manage registered users as well as monitor system operations. The dashboard serves as the central interface for performing administrative actions.





'To detect abnormal activities, the system allows log data to be submitted for analysis. The anomaly detection module processes the input data and applies machine learning techniques to identify patterns that deviate from normal system behavior.



After processing the log data, the system produces results highlighting the detected anomalies. These results indicate unusual patterns

Copyright © 2026 CJESR All Rights Reserved

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

within the logs and help in identifying potential security threats or suspicious activities in the cloud environment.

VII. CONCLUSION

This research presented a Generative AI-based framework for real-time cloud security monitoring using GPT models for advanced anomaly detection. The proposed system integrates machine learning algorithms with GPT-based contextual analysis to detect suspicious activities in cloud environments.

The results demonstrate that the proposed approach improves anomaly detection performance and enables intelligent analysis of system logs. The integration of Generative AI enhances the ability of security monitoring systems to identify complex cyber threats and provide meaningful explanations for detected anomalies.

Future work may focus on integrating the proposed system with large-scale cloud infrastructures and exploring more advanced transformer-based models for improved threat detection accuracy.

REFERENCES

1) I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

2) A. Vaswani et al., “Attention Is All You Need,” in Proceedings of the 31st Conference on Neural Information Processing Systems (NeurIPS), 2017.

3) T. Brown et al., “Language Models are Few-Shot Learners,” in Advances in Neural Information Processing Systems, vol. 33, 2020.

4) F. T. Liu, K. M. Ting, and Z. H. Zhou, “Isolation Forest,” in Proceedings of the IEEE International Conference on Data Mining (ICDM), 2008, pp. 413– 422.

5) J. An and S. Cho, “Variational Autoencoder based Anomaly Detection using Reconstruction Probability,” Special Lecture on IE, vol. 2, no. 1, pp. 1–18, 2015.

6) M. Ahmed, A. N. Mahmood, and J. Hu, “A Survey of Network Anomaly Detection Techniques,” Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.

7) H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, “A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems,” IEEE Access, vol. 8, pp. 104650–104675, 2020.

8) D. B. Rawat and C. Bajracharya, “Cybersecurity for Cloud Computing: Techniques and Applications,” IEEE Access, vol. 7, pp. 47502–47516, 2019.

9) P. Mishra, V. Varadharajan, and U. Tupakula, “Cloud Security Challenges and Solutions,” IEEE Cloud Computing, vol. 5, no. 1, pp. 20–29, 2018.

10) S. Axelsson, “The Base-Rate Fallacy and Its Implications for Intrusion Detection,” in Proceedings of the ACM Conference on Computer and Communications Security, 2000, pp. 1–7.

11) S. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A Deep Learning Approach to Network Intrusion Detection,” IEEE Transactions

Copyright © 2026 CJESR All Rights Reserved

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 11-20, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304002
Available Online at https://www.cjesr.com

on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41– 50, 2018.

12) E. Alpaydin, Introduction to Machine Learning, 4th ed. Cambridge, MA, USA: MIT Press, 2020.

13) OpenAI, "GPT-4 Technical Report," 2023.

14) J. Dean and S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," Communications of the ACM, vol. 51, no. 1, pp. 107– 113, 2008.

15) R. Buyya, J. Broberg, and A. Goscinski, Cloud Computing: Principles and Paradigms. Wiley, 2011.

****

Copyright © 2026 CJESR All Rights Reserved