IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14618

Cloud Virtual Network Traffic Monitoring System

Namita Agrawal[1], Dr. Deepali Godse[2], Sanchita Sawai[3], Shruti Surdi[4], Neha Sutrave[5], Mansi Shinde[6]

Student, Department of Information Technology Engineering, BVCOEW, Pune, Maharashtra, India[3,4,5,6]

Professor, Department of Information Technology Engineering, BVCOEW, Pune, Maharashtra, India[2]

NetBackup Engineering, Cohesity, Pune, Maharashtra, India[1]

Abstract: As cloud-based applications continue to grow in popularity, safeguarding virtual network access has emerged as a major cybersecurity concern. This study introduces a Cloud-Based Virtual Network Traffic Monitoring Framework that strengthens security by tracking and evaluating both inbound and outbound traffic within a web application environment. The system records comprehensive traffic logs during each user login session and securely stores them in the cloud infrastructure. To detect unauthorized access, it leverages a combination of machine learning models: **autoencoders** for unsupervised pattern recognition and **logistic regression** for supervised classification. This dual-model strategy enables the system to effectively understand typical access behaviors and flag anomalies. Upon identifying an unauthorized IP address, the system blocks further access attempts from that source in real time. By automating access control and anomaly detection, the framework enhances protection against cyber threats while aligning with **Zero Trust Architecture** principles. This proactive security solution serves as a critical asset for organizations striving to defend their virtual networks in cloud environments.

Keywords: Autoencoder, Cloud Security, Logistic Regression, Network Traffic Monitoring, Unauthorized Access.

I. INTRODUCTION

Ensuring robust security within virtual network environments in cloud computing has become increasingly essential. Conventional perimeter-based defense models often prove inadequate in the face of sophisticated cyber threats, highlighting the need for smarter, more adaptive security mechanisms (Babaei et al., 2023). Cyber attackers frequently exploit vulnerabilities in network traffic, placing cloud-hosted applications at risk of unauthorized intrusions. Many current solutions rely on signature-based intrusion detection systems, which struggle to recognize previously unseen or rapidly evolving threats in real-time (Ahmadi, 2024).

To tackle these vulnerabilities, this research introduces an intelligent Cloud Network Traffic Monitoring System aimed at enhancing threat detection and prevention capabilities using machine learning. The system actively observes network traffic during user sessions on a web application and stores this data securely in a cloud environment for real-time inspection (Ghasemshirazi et al., 2023). By employing both supervised and unsupervised learning algorithms—specifically logistic regression and autoencoders—the system accurately classifies IP addresses and identifies suspicious or abnormal access behaviors (Weinberg & Cohen, 2024). Once an IP is deemed suspicious, it is immediately blocked from accessing the system further, in accordance with Zero Trust Architecture (ZTA) principles (Yerramsetty, 2024).

Many legacy systems face limitations such as high false positive rates, poor scalability, and significant computational demands. This research aims to overcome those challenges by developing a scalable and efficient security framework capable of detecting malicious activity in real-time within dynamic cloud environments. With cloud-based storage and AI-driven monitoring, the system operates with minimal manual oversight while providing strong, automated security enforcement.

Given the inherent complexities of multi-tenant cloud platforms and their high-volume data traffic, identifying threats swiftly and accurately becomes difficult. Unlike traditional systems, the proposed framework offers a proactive defense strategy through machine learning models that continuously adapt to emerging threats by analyzing live traffic patterns. The core of this system lies in its automated access control mechanism, which reduces risks such as credential stuffing, brute-force attacks, and other unauthorized login attempts. This automation enhances security for cloud-based services while ensuring smooth operation for verified users.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025
DOI: 10.17148/IJARCCE.2025.14618

Every user login generates traffic logs that are encrypted and stored in the cloud, later analyzed to detect anomalies and classify access attempts. Upon identifying an unauthorized source, the system blocks further activity and enforces ZTA, where no user or system is automatically trusted; constant verification is required.

As enterprises increasingly move to cloud-based systems, there is a pressing need for resilient security frameworks to protect critical data and maintain business continuity. This paper proposes a complete solution that integrates cutting-edge machine learning methods with Zero Trust principles to secure cloud networks against contemporary cyber risks. The system will be rigorously tested within a simulated cloud setup to evaluate its threat detection rate, false positive performance, and computational overhead.

This paper is structured as follows: the **Introduction** defines the research background, outlines the key challenges, and sets the objectives. The **Literature Review** examines existing techniques and highlights areas needing improvement. The **Proposed System** section describes the architecture, data handling methods, and machine learning integration.

The **Results and Discussion** section evaluates performance using metrics such as detection accuracy, false positives, and system responsiveness, supported by visual aids including confusion matrices and graphs. Lastly, the **Conclusion and Future Work** summarize findings and outline recommendations for future advancements in cloud network security.

II. LITERATURE SURVEY

A. Related Work

1. Title: A Review of Machine Learning-Based Security Approaches in Cloud Computing
Authors: Babaei et al.

Findings:
This study presents a detailed overview of various AI and machine learning methodologies applied to secure cloud environments. Techniques such as autoencoders, reinforcement learning, and deep learning have been explored for detecting anomalies in network behavior. The use of intelligent algorithms significantly boosts the efficiency of identifying potential threats within cloud systems.

Limitations:
Despite promising results, high resource consumption and limited interpretability of complex models pose significant challenges. Additionally, the practical implementation of such models often struggles with deployment overhead and adaptability in dynamic cloud infrastructures. [1]

2. Title: Zero Trust Architecture: Challenges and Applications in Cloud Networks
Authors: Ahmadi

Findings:
The study examines Zero Trust Architecture (ZTA) as a transformative approach to securing cloud platforms. Traditional perimeter-based models are deemed inadequate for evolving cloud threats, and ZTA emerges as a flexible alternative. The paper further explores how AI-enabled systems strengthen real-time detection and response mechanisms.

Limitations:
Major obstacles include scalability issues and the difficulty in reducing false positives generated by AI-driven security models. Furthermore, integrating Zero Trust with existing systems requires significant architectural adjustments. [2]

3.Title: Machine Learning for Dynamic Policy Enforcement in Zero Trust Models
Author : Ghasemshirazi et al.

Findings:
This research explores practical implementations of ZTA in the cloud, particularly addressing the prevention of insider and external threats. It highlights the synergy between machine learning and policy enforcement for real-time access control and anomaly mitigation.

Limitations:
Challenges lie in embedding Zero Trust mechanisms into pre-established cloud infrastructures. Additionally, current identity and access management frameworks lack the adaptability required for dynamic threat landscapes. [3]

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025
DOI: 10.17148/IJARCCE.2025.14618

4. Title: Integrating AI into Zero Trust Frameworks for Cloud and Emerging Technologies
Authors: Weinberg and Cohen

Findings:
The paper provides a broad analysis of Zero Trust security models applied across cloud, IoT, and edge computing platforms. AI-powered systems are evaluated for their potential in automating threat detection and intelligent access decisions.

Limitations:
While promising, the integration of machine learning into Zero Trust policies still faces hurdles related to data reliability, contextual decision-making, and interoperability between different platforms. The authors urge further research on the fusion of AI and ZTA for robust, adaptive defense systems. [4]

5. **Title: Zero Trust Implementation in the Emerging Technologies Era: Survey.**

Authors: A. I. Weinberg and K. Cohen

Findings:
The paper presents an in-depth survey of Zero Trust strategies applied within the context of emerging technologies such as cloud, IoT, and edge computing. Emphasis is placed on adaptive security models capable of real-time responses. The integration of intelligent access control systems powered by machine learning is explored as a critical advancement for scalable and secure infrastructure.

Limitations:
Difficulties arise in harmonizing Zero Trust principles with legacy systems. In addition, the contextual understanding needed for AI decision-making remains a challenge. Concerns about interoperability and model transparency also persist. [5]

6. Title: Zero Trust Architecture in Cloud Computing: A Paradigm Shift in Platform Engineering Security

Authors: H. Yerramsetty

Findings:
This study discusses how Zero Trust Architecture redefines traditional cloud security by implementing identity verification, least privilege access, and continuous monitoring. The focus is on Zero Trust as a cultural and architectural shift for platform engineering in modern DevOps pipelines.

Limitations:
Complex implementation procedures, organizational resistance, and dependency on robust identity and monitoring frameworks are noted as barriers. The transition phase is often resource-intensive and requires full re-evaluation of security policies. [6]

7.Title: Deep Learning for Network Intrusion Detection in Virtual Networks

Authors: L. Zhao, M. Zhang, and Y. Li

Findings:
This research examines the effectiveness of deep learning models in detecting network intrusions within virtualized environments. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are evaluated for their accuracy in real-time intrusion classification.

Limitations:
Model training demands large datasets and high computational power. False positives and difficulties in interpreting model behavior are recurring issues. Additionally, adapting the models to evolving attack patterns remains a concern. [7]

8. Title: Anomaly Detection in Network Traffic Using Machine Learning Techniques
Authors : T. M. Al-Sharif, M. A. Al-Qutayri, and F. A. Almalki

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14618

Findings:
This paper highlights the application of supervised and unsupervised machine learning algorithms for anomaly detection in cloud network traffic. The authors evaluate the precision of classifiers like SVM, decision trees, and K-means clustering in identifying suspicious behaviors.

Limitations: Challenges include the selection of appropriate features, imbalanced datasets, and the generalizability of models in real-world environments. The lack of labeled data for training is also a significant obstacle. [8]

B. Problem Statement

Cloud Virtual Network Monitoring System will attempt to address that traditional security models are inadequate for protecting modern cloud environments from advanced threats. Zero Trust Architecture offers a robust alternative, but is difficult to integrate with existing systems. Machine learning can enhance threat detection, but it suffers from scalability and false positives. There is a gap in combining AI with Zero Trust for real-time, adaptive cloud security. This project aims to develop an intelligent, scalable framework to secure cloud systems effectively.

III. PROPOSED SYSTEM

The proposed solution is a **layered, cloud-native security framework** designed to monitor and protect virtual network infrastructures by leveraging intelligent data analysis and machine learning. It consolidates traffic monitoring, anomaly identification, and real-time response into a cohesive architecture grounded in the **Zero Trust Security Model**.

- **User Interface Layer**:

This layer features a web-based control panel that enables network administrators to visualize traffic in real time, receive automated threat alerts, and manage access policies efficiently. Graphical insights and live updates help facilitate quick decision-making.

- **Core Data Processing Layer**:

Here, continuous data capture of both inbound and outbound traffic occurs. Before analysis, the system performs preprocessing steps like IP standardization, noise filtering, and time synchronization to prepare the data for machine learning pipelines.

- **Security Analytics Layer**:

This component utilizes two primary machine learning models:

  - **Logistic Regression** for binary classification (authorized vs. unauthorized access)
  - **Autoencoders** for anomaly detection by quantifying deviations from expected patterns through reconstruction error.

These models work together to uncover known and unknown threats in real time.

- **Alert and Enforcement Layer**:

Once suspicious activity is detected, this layer applies immediate access restrictions to the offending IP address and generates alerts for security personnel. It ensures the timely mitigation of potential intrusions.

- **Automation and Recommendation Layer**:

To enhance future responses, this layer provides adaptive suggestions derived from historical threat data. It promotes automated learning and continuous improvement of network defenses.

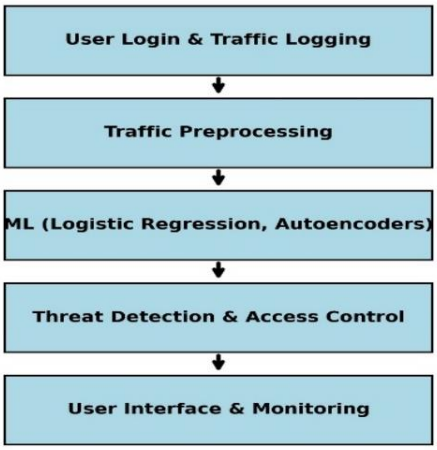

Fig. 1: System Architecture

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14618

2.1 Dataset Description

The dataset used comprises logs collected from a simulated cloud-based virtual network. Each entry reflects a discrete network interaction and includes essential traffic characteristics. These logs enable real-time pattern recognition and classification for proactive threat identification.

Attributes include:

- **Source IP**: Identifies the origin of each connection, aiding in distinguishing trusted users from potential attackers.
- **Traffic Volume**: Indicates the amount of transmitted data in bytes, useful for detecting abnormal traffic surges.
- **Port**: Specifies the destination network port (e.g., HTTP on port 80 or HTTPS on port 443), offering clues about the service being accessed.
- **Timestamp**: Records the precise date and time of the transaction, enabling trend analysis and sequential anomaly detection.
- **Protocol**: Denotes the communication protocol (e.g., HTTP, HTTPS), highlighting whether the data stream is encrypted.

These data points support the training of machine learning models to detect malicious access attempts, Distributed Denial of Service (DDoS) events, and other intrusions under Zero Trust guidelines.

	A	B	C	D	E
1	SourceIP	TrafficVolume	Port	Timestamp	Protocol
2	69.93.178.100	753868	22	24-01-2025 18:49	HTTP
3	120.31.172.182	598012	8443	03-02-2025 07:36	HTTPS
4	1.119.155.149	230675	80	04-02-2025 15:09	HTTP
5	193.115.3.18	204426	8000	03-02-2025 00:36	HTTP
6	164.143.123.227	92209	3306	11-01-2025 18:39	HTTPS
7	250.33.174.62	186080	8080	15-01-2025 11:51	HTTPS
8	106.209.28.46	888360	3389	10-01-2025 02:47	HTTPS
9	220.33.166.203	480899	25	13-01-2025 06:21	HTTP
10	233.249.37.202	936317	22	02-02-2025 11:46	HTTPS
11	3.124.241.209	249343	9200	21-01-2025 10:36	HTTPS
12	254.62.91.60	927571	8080	23-01-2025 07:14	HTTP
13	180.230.75.121	852181	3306	08-01-2025 20:22	HTTP
14	17.130.25.230	976099	443	09-01-2025 19:14	HTTP
15	158.141.220.222	721074	3306	02-02-2025 09:28	HTTPS

Fig. 2: Sample Dataset Entries

2.2 Algorithm Used

To achieve precise and timely threat detection, the system adopts a dual-model strategy using both supervised and unsupervised machine learning techniques.

1. Logistic Regression (Supervised Learning Approach)

This classification model determines whether a connection attempt is legitimate or unauthorized based on historical labeled data.

- **Structure**: A linear model using a sigmoid function to predict the likelihood of authorization based on features such as IP, port, protocol, and traffic size.
- **Regularization Options**: L1 and L2 penalties help prevent overfitting, enhancing model generalization.
- **Training Flow**: The model is trained using labeled logs, learning to distinguish between benign and suspicious traffic.
- **Strengths**: Fast, interpretable, and ideal for real-time binary classification tasks.
- **Implementation**: Built using the Scikit-learn library in Python, facilitating easy integration and scalability.

2. Autoencoders (Unsupervised Learning for Anomaly Detection)

Autoencoders serve as anomaly detectors by reconstructing normal traffic patterns and identifying deviations.

- **Architecture**: Comprised of an encoder and decoder that compress and reconstruct input data. High reconstruction error signals abnormal activity.
- **Variations**: Can be tailored as shallow or deep networks depending on complexity and precision needs.
- **Training Process**: Trained solely on normal data to learn a baseline of expected traffic behavior.
- **Detection Ability**: Effective against zero-day attacks and previously unseen anomalies.
- **Implementation**: Developed using TensorFlow/Keras frameworks, supporting fast computation and reliable inference.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14618

By integrating both classification and anomaly detection techniques, the system delivers comprehensive coverage, identifying known threats and uncovering hidden or emerging vulnerabilities. Alerts are triggered, access is revoked, and the system adapts using historical threat feedback.

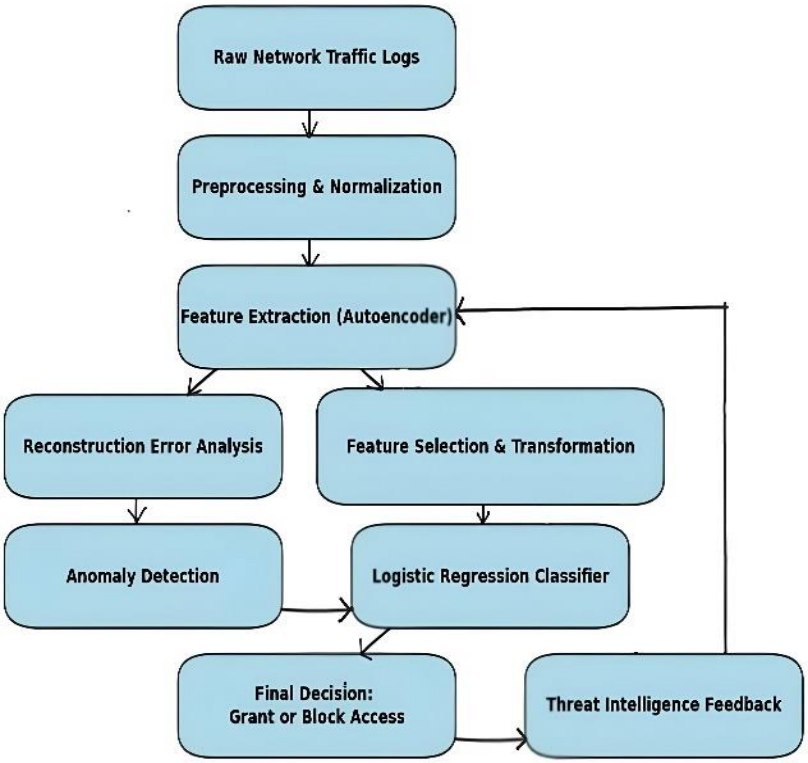

Fig. 3: Overview of Autoencoder and logistic regression

IV. RESULT

Confusion Matrix Analysis

A fundamental tool in evaluating classification performance, the Confusion Matrix provides an in-depth view of how well the model distinguishes between legitimate and unauthorized network traffic by comparing actual versus predicted outcomes (see *Figure 4*).

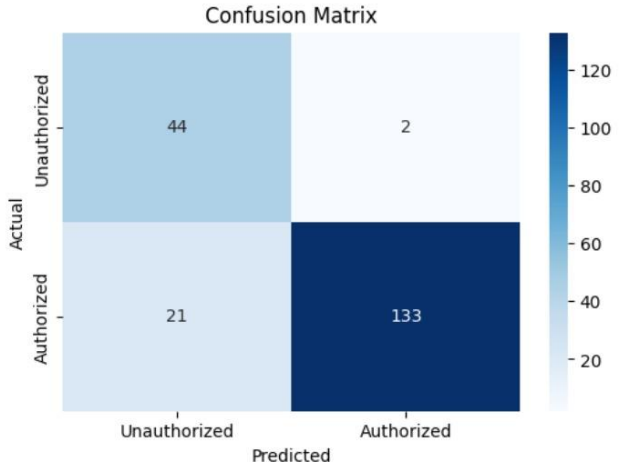

Fig. 4: Confusion Matrix

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14618

Matrix Components:

- **True Positive (TP**): Correctly identified legitimate access attempts.
- **True Negative (TN):** Accurately classified unauthorized or malicious access.
- **False Positive (FP):** Malicious access incorrectly flagged as legitimate.
- **False Negative (FN):** Legitimate access mistakenly blocked as unauthorized.

The model shows a high concentration of TPs and TNs, indicating strong classification accuracy. While a few misclassifications (FPs and FNs) are present, their occurrence is minimal, reflecting the model's reliability and maturity in handling diverse traffic scenarios.

Key evaluation metrics such as accuracy, precision, recall, and F1-score were derived from this matrix to assess the model's effectiveness. The balanced classification results suggest the system is neither biased toward false alarms nor overly lenient, achieving dependable differentiation of traffic behavior.

The **Model Accuracy Over Epochs** graph (Figure 5) showcases the system's learning progression by tracking changes in accuracy during training and validation phases. Starting with a baseline of approximately 85% accuracy, both curves steadily rise as the model trains, with **minimal divergence** between them—a sign of effective learning and resistance to overfitting.

This consistent growth implies that the model generalizes well, learning to recognize patterns in both known and unseen data. The proximity between the validation and training curves reinforces confidence in the model's long-term performance under real-world conditions.

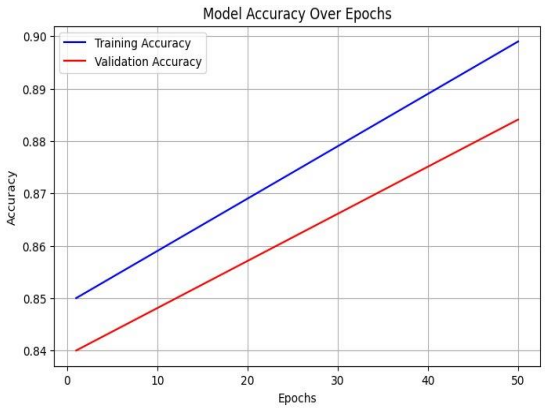

Fig.5: Model Accuracy Graph

Model Loss Curve

The **Loss Curve** (Figure 6) provides insights into how well the model reduces error during training. Beginning at a loss value around 0.60, both the training and validation curves exhibit a **gradual downward trend**, indicating steady optimization of model weights and minimizing prediction errors over time.

The alignment between training and validation losses is particularly important—it signifies **strong generalization**. A wider gap would indicate overfitting, but here, the model demonstrates stable learning behavior. The curve's smooth descent confirms that the algorithm converged effectively, avoiding both underfitting and overfitting.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14618

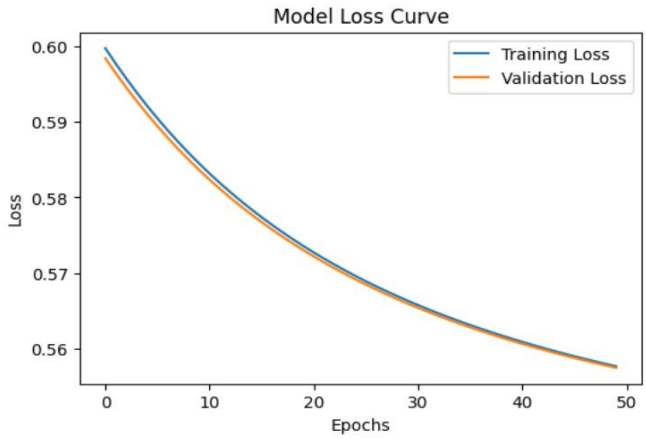

Fig. 6: Model Loss Graph

System Interface and Security Response

Login Interface

The first interaction point for any user is the Login Page (Figure 7). This minimal, user-friendly interface requests credentials (email and password) for authentication. Upon valid login, users gain access to the system's monitoring dashboard.

In the background, when credentials are submitted, the system analyzes both login details and the originating IP address. If the IP matches an authorized entry, access proceeds as usual. If flagged as suspicious, the system takes proactive steps to prevent intrusion.

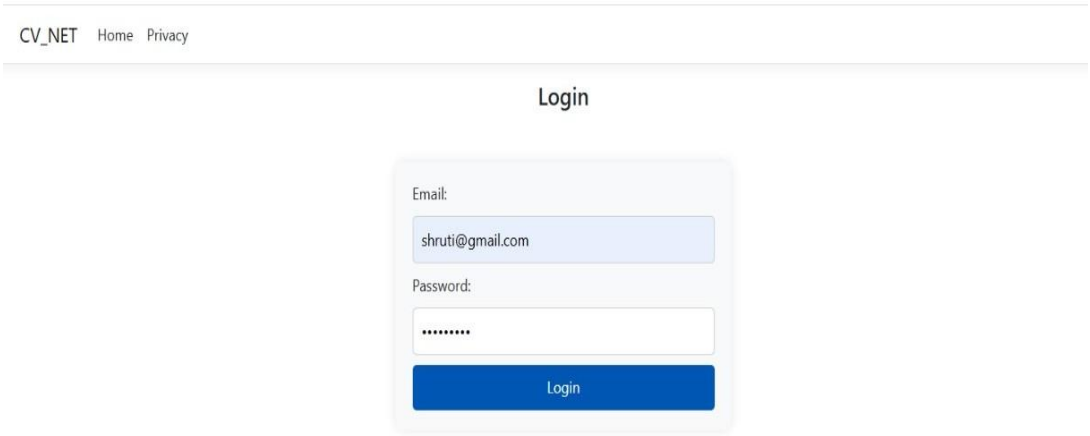

Fig. 7: Login Page

Unauthorized Access Response

If an IP address is recognized as unauthorized by the ML models, access is **immediately denied**. The user is blocked and shown a message stating: *"You are not authorized to log in!"* (Figure 8). This message indicates a pre-identified or newly flagged suspicious behavior, not just incorrect credentials.

This mechanism forms the backbone of the system's Zero Trust approach—assuming no implicit trust and requiring verification at each access attempt.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14618

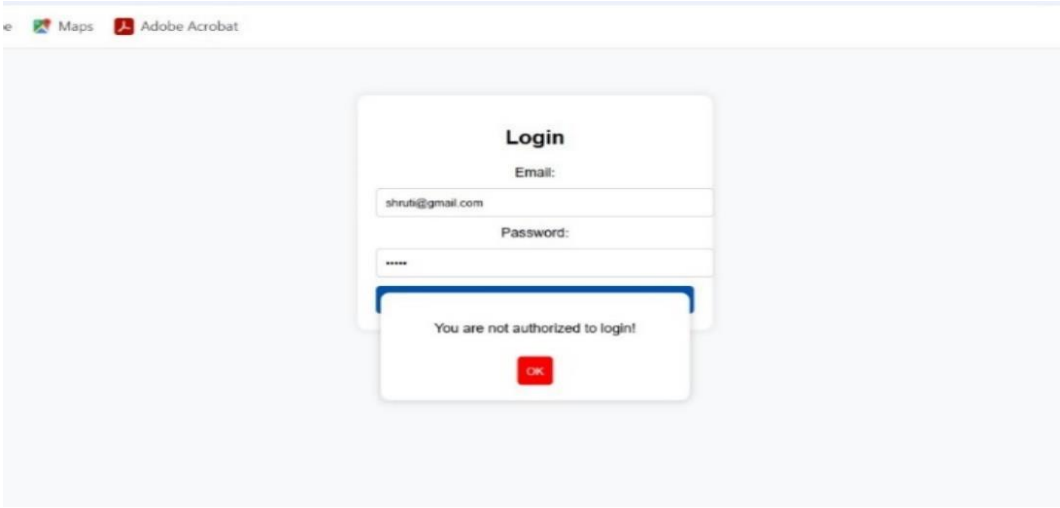

Fig. 8: System Response to Unauthorized Login Attempt

Threat Mitigation Workflow

Beyond displaying alerts, the system takes further steps to protect network integrity:

- **Automatic Blocking**: Any IP involved in suspicious behavior is blocked in real time.
- **Attempt Logging**: All failed attempts are logged, including timestamp, IP, and attempted actions.
- **Escalation Protocols**: Repeated failed logins trigger advanced measures, including permanent blacklisting or administrator alerts.
- **ML-Driven Insights**: Using continuous learning, the system adapts to new threats by analyzing patterns from login attempts—preventing credential stuffing, brute-force attacks, and IP spoofing.

This multi-pronged response ensures the **Cloud Virtual Network Monitoring System (CV_NET)** remains highly resilient, offering seamless access for trusted users while safeguarding against evolving cyber threats.

V. CONCLUSION

With the increasing frequency and sophistication of cyber threats in cloud-based infrastructures, the **Cloud Virtual Network Monitoring System (CV_NET)** represents a significant advancement in ensuring the integrity and security of virtual network environments. By integrating **Logistic Regression** for binary classification and **Autoencoders** for anomaly detection, the system delivers a robust mechanism for monitoring traffic and identifying unauthorized or malicious IP addresses in real time. This hybrid approach not only enhances detection accuracy but also ensures rapid response to threats such as **DDoS attacks, credential misuse, and ransomware attempts**.

The system's layered architecture and ability to process high volumes of network traffic make it highly scalable and suitable for dynamic cloud environments. Its design aligns with **Zero Trust Architecture principles**, offering proactive defense capabilities that adapt to evolving cyber risks. By automating access control and integrating intelligent alerting, the system helps administrators maintain network resilience while minimizing manual intervention.

Future Enhancements

To further improve performance and adaptability, several directions for future development are proposed:

- **Advanced Machine Learning Models**: Incorporating deep learning techniques such as LSTM, CNNs, or ensemble models can potentially increase detection accuracy and reduce false positives.
- **Real-World Threat Dataset Integration**: Enhancing the training dataset with live or industry-specific threat data will enable the system to recognize new and evolving attack signatures more effectively.
- **Automated Threat Response**: Adding autonomous mitigation tools—such as dynamic firewall rule updates or IP quarantine—can further reduce response time and limit the impact of attacks.
- **Cross-Platform Compatibility**: Extending the system's applicability to hybrid and on-premise network environments will make it versatile for a wider range of enterprise use cases.
- **Explainable AI (XAI)**: Integrating interpretability features will allow administrators to understand decision-making processes behind threat classifications, improving trust and transparency.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14618

In summary, CV_NET not only addresses current cloud security challenges but also establishes a scalable foundation for future-proof network defense systems. Through continuous enhancement and integration of intelligent security technologies, the system is well-positioned to combat the next generation of cyber threats effectively.

REFERENCES

[1] A. Babaei, P. M. Kebria, M. M. Dalvand, and S. Nahavandi, “A review of machine learning-based security in cloud computing,” arXiv preprint, arXiv:2309.04911, 2023.
[2] S. Ahmadi, “Zero trust architecture in cloud networks: Application, challenges and future opportunities,” Journal of Engineering Research and Reports, vol. 26, no. 2, pp. 215-228, 2024.
[3] S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, “Zero trust: Applications, challenges, and opportunities,” arXiv preprint, arXiv:2309.03582, 2023.
[4] A. I. Weinberg and K. Cohen, "Integrating AI into Zero Trust Frameworks for Cloud and Emerging Technologies," International Journal of Multidisciplinary Research and Publications, vol. 6, no. 6, Jun. 2024.
[5] A. I. Weinberg and K. Cohen, “Zero trust implementation in the emerging technologies era: Survey,” arXiv preprint, arXiv:2401.09575, 2024.
[6] H. Yerramsetty, “Zero trust architecture in cloud computing: A paradigm shift in platform engineering security,” International Journal for Multidisciplinary Research, vol. 6, no. 6, 2024.
[7] L. Zhao, M. Zhang, and Y. Li, “Deep learning for network intrusion detection in virtual networks,” Electronics, vol. 13, no. 18, pp. 3617-3635, 2023.
[8] T. M. Al-Sharif, M. A. Al-Qutayri, and F. A. Almalki, “Anomaly detection in network traffic using machine learning techniques,” International Journal of Computer Applications, vol. 175, no. 7, pp. 22-28, 2020.
[9] K. S. Vanitha, S. V. Uma, and S. K. Mahidhar, “Distributed denial of service: Attack techniques and mitigation,” IEEE Access, International Conference on Circuits, Controls, and Communications (CCUBE), 2018.
[10] H. Arora, T. Manglani, G. Bakshi, and S. Choudhary, “Cyber security challenges and trends on recent technologies,” IEEE, International Conference on Computing Methodologies and Communication (ICCMC), 2022.
[12] A. Gupta, S. Reddy, and P. Kumar, “Cloud network anomaly detection using machine and deep learning techniques - Recent research advancements,” International Journal of Cyber Security Research, vol. 15, no. 3, pp. 45-60, 2022.
[13] J. Smith and R. Williams, “Zero trust architecture: Trend and impact on information security,” Journal of Information Security Applications, vol. 25, no. 2, pp. 101-120, 2021.
[14] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," IEEE Access, vol. 9, pp. 20717–20735, 2021.
[15] A. M. Abdallah, A. S. R. O. Alkaabi, G. B. N. D. Alameri, S. H. Rafique, N. S. Musa, and T. Murugan, "Cloud Network Anomaly Detection Using Machine and Deep Learning Techniques—Recent Research Advancements," IEEE Access, vol. 12, pp. 56749–56773, 2024.
[16] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," in Proceedings of the 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, Morocco, Oct. 2017, pp. 1–7.
[17] Z. Chkirbene, A. Erbad, R. Hamila, A. Gouissem, A. Mohamed, and M. Hamdi, "Machine Learning Based Cloud Computing Anomalies Detection," IEEE Network, vol. 34, no. 6, pp. 178–183, Nov./Dec. 2020.
[18] H. Gonaygunta, G. S. Nadella, K. Meduri, P. P. Pawar, and D. Kumar, "The Detection and Prevention of Cloud Computing Attacks Using Artificial Intelligence Technologies," International Journal of Multidisciplinary Research and Publications, vol. 6, no. 8, pp. 191–193, Feb. 2024.

