Universal Library of Innovative Research and Studies Research Article

ISSN: 3065-0003 | Volume 3, Issue 1

Open Access | PP: 28-32

DOI: https://doi.org/10.70315/uloap.ulirs.2026.0301005

Trends in Using Machine Learning for Network Anomaly Monitoring in Cloud Platforms

Praveen Ravula

Software Engineer at Amazon, Arlington, VA, USA.

Abstract

The article examines emerging trends in the application of machine learning methods for detecting network anomalies in cloud platforms, taking into account the influence of virtualization and the dynamics of infrastructure. The study is based on a systematization of publications addressing traffic and resource-metric monitoring, labeling scarcity, multilayer encapsulation, and the limited observability of distributed systems. The paper compares ensemble and hybrid architectures, convolutional and recurrent models, unsupervised autoencoders, as well as graph-based and contrastive approaches, enabling an assessment of how architectural choices affect anomaly-recognition robustness under distribution shifts and changes in packet structure. Special attention is given to the roles of temporal dependencies, node-interaction topology, and the effects of virtual-machine migration, which introduce distortions in input data and create opaque zones within virtual networks. The findings show that shifting from models relying on local features to spatiotemporal and graph-based architectures improves monitoring adaptability to cloud-infrastructure variability and partial labeling, although this transition is accompanied by increased model complexity and higher requirements for representation quality. The article may be of interest to professionals working in cloud-platform operations, network security, and reliability engineering for distributed systems.

Keywords: *Cloud Platforms, Network Anomalies, Machine Learning, Virtual Networks, Monitoring, Graph-Based Models, Virtualization.*

INTRODUCTION

The growth of scalable cloud platforms and virtualized network environments enhances the dependency of services on infrastructure stability, thereby increasing the importance of timely anomaly detection. Traditional monitoring mechanisms capture violations but adapt poorly to the dynamics of virtual networks, where configurations change rapidly and traffic undergoes multilayer encapsulation.

Machine learning methods expand monitoring capabilities; however, classical rules and signatures remain vulnerable to encryption and traffic variability. Deep models improve accuracy but face challenges regarding labeling scarcity and incomplete data observability [4]. Graph and contrastive approaches account for structure and temporal dynamics, yet their behavior under virtualization conditions remains insufficiently studied.

It remains unclear how distinct architectures, ranging from CNNs to hybrid models with GraphGRU, respond to encapsulation, virtual machine migration, and high flow variability. A holistic concept unifying architectural solutions with the specific characteristics of cloud data is currently lacking, as existing research covers only isolated elements of the problem.

The objective of this study is to systematize trends in the application of machine learning methods for detecting network anomalies in cloud platforms by comparing architectural approaches, experimental results, and model limitations under virtualization conditions.

The hypothesis posits that the transition from classical machine learning methods to spatiotemporal and contrastive models increases the resilience of monitoring systems to cloud infrastructure variability, reduces sensitivity to the lack of labeling, and ensures higher accuracy when working with dynamic network flows.

The scientific contribution consists of formulating an analytical framework that reveals how architectural characteristics of models—such as the use of graph structures, contrastive learning, reconstruction, or hybrid CNN-LSTM networks—influence the ability of systems to correctly identify anomalies in real-world cloud conditions. The work generalizes the differences between approaches, identifies the causes of reduced accuracy in virtualized

Citation: Praveen Ravula, "Trends in Using Machine Learning for Network Anomaly Monitoring in Cloud Platforms", Universal Library of Innovative Research and Studies, 2026; 3(1): 28-32. DOI: https://doi.org/10.70315/uloap.ulirs.2026.0301005.

networks, and demonstrates which architectural solutions allow for the compensation of these effects.

The scope of the study is defined by the task of detecting network anomalies in cloud environments. Issues regarding cryptographic protection, vulnerability management, application-level intrusion prevention, and network protocol optimization remain outside the framework of this analysis, as they touch upon adjacent fields but do not constitute the immediate subject of this research.

MATERIALS AND METHODS

The study is based on scientific publications from 2022–2025 dedicated to monitoring network and resource anomalies in cloud environments and the application of machine learning to the analysis of traffic, time series, and topological dependencies. Works addressing the problems of labeling deficits, the influence of virtualization on network packet structure, the necessity of accounting for cloud system topology, and the development of reconstruction and contrastive learning approaches were utilized. These materials form the theoretical basis necessary for analyzing trends in the application of ML methods for anomaly monitoring on cloud platforms.

Specifics of analyzing unlabeled time series in cloud systems are examined in the study by Al-Ghuwairi et al. [1]. The problematic aspects of ensuring data integrity and constructing ML models for anomaly detection are outlined in the work of Devineni et al. [2]. Adaptation of models to changing network traffic and incremental learning on edge nodes are presented by Glavan & Croitoru [3]. Scalability and limited observability of industrial clouds are analyzed in the research by Islam et al. [4]. The use of knowledge graph embedding for anomaly detection is described by Mitropoulou et al. [5]. Methods for unlabeled detection of network packets using autoencoders are revealed in the work of Park et al. [6]. Architectures for ML monitoring of network anomalies are systematized by Schummer et al. [7]. The capabilities of ensembles for multiclass classification of cloud anomalies are considered by Shahzad et al. [8]. The influence of virtualization, encapsulation, and virtual machine migration on classification accuracy is analyzed by Spiekermann et al. [9]. Graph and contrastive models for integrating the topology and temporal dynamics of cloud systems are detailed in the study by Zhang et al. [10].

The methodological basis of the research included content analysis of scientific publications aimed at identifying key approaches to anomaly detection in cloud platforms and classifying the applied ML architectures. A comparative analysis of models—reconstruction, classification, graph-based, and contrastive—was applied to reveal differences in their resilience to virtualization artifacts, labeling deficits, and traffic variability. Functional-structural modeling was used, focusing on reconstructing the operational logic of various architectures, including autoencoders, convolutional networks, and hybrid graph models.

RESULTS

The increasing complexity of cloud platforms intensifies the requirements for anomaly detection models. They must react correctly to variable network conditions, high loads, virtualization, and the dynamics of internodal connections. During the source analysis, the primary behavioral features of modern machine learning models were identified, reflecting differences in architectures, task types, and the nature of network traffic.

The results of the study by Park et al. [6] demonstrate that unsupervised methods maintain stability during changes in network structure but are sensitive to disruptions in baseline traffic distributions. This highlights the differences between models dependent on labeling and methods relying on data properties. Summary indicators are presented in Table 1.

Table 1. Comparison of anomaly detection model accuracy (Compiled by the author based on the sources: [8, 9, 10])

Model / Source	Task Type	Metric	Value
Ensemble (SGD + LR + Ridge) – CAD	Binary anomaly detection	Accuracy	97.06%
CNN-LSTM CAD model	Multiclass detection	Accuracy	99.91%
CNN-NIDS	Classic network flows	Accuracy	98.7%
CNN-NIDS	VXLAN/GENEVE traffic	Accuracy	Significant decrease
GCAD	Performance anomaly detection	Precision	0.915
GCAD	Performance anomaly detection	Fullness	0.512
GCAD	Performance anomaly detection	F1	0.932

Note: The "Task Type" column denotes the type of task for which the model was trained, including binary classification, multiclass recognition, or flow traffic analysis. The "Metric" column reflects the quality indicator used, such as accuracy, precision, recall, or the F1-metric. The "Value" column contains the final value of the corresponding metric as cited in the original source.

Continuing the examination of algorithm performance patterns in cloud environments, it is important to highlight how model architecture determines its reaction to the network and computational features of the platform. The study by Al-Ghuwairi et al. [1] shows that models focused on temporal dependencies in data streams form more robust features under load changes, enhancing the ability to detect rare and transient states. The work of Glavan and Croitoru [3] demonstrates that sequential learning methods face changes in traffic structure as data arrives, and the architecture plays a key role in such conditions. Models that do not account for the context of packet appearance quickly

lose sensitivity. The research by Mitropoulou et al. [5] emphasizes the importance of structural links between network objects, making topological architectures more resilient to the increasing complexity of the cloud environment. Furthermore, Schummer et al. [7] show that architectures built around the modular processing of network features adapt better to changes in the component composition of traffic. To systematize the main trends, summary characteristics of architectures are provided in Table 2.

Table 2. Architectural trends in ML models for anomaly monitoring (Compiled by the author based on the sources: [3, 4, 9])

Architecture	Key Properties
Ensemble + CNN-LSTM	Accuracy increase due to hybrid ML schemes
CNN	Accuracy degradation caused by encapsulation (VXLAN/GENEVE)
GraphGRU + contrastive learning	Integration of topology + temporal dynamics improves accuracy

Table 2 indicates that architectural differences determine the mechanism for processing network features and the nature of the model's reaction to structural data changes. The study by Al-Ghuwairi et al. [1] demonstrates the advantages of temporal models in environments with high load variability. Such a structure makes the algorithm less dependent on the network interaction graph but more resilient to the dynamics of incoming packets. The results of Glavan and Croitoru [3] confirm that architectures not utilizing context and connections between events tend to decrease in accuracy during the transformation of network structures.

Thus, architectures incorporating topological representation allow for the detection of interconnected anomalies arising on multiple nodes simultaneously. In cloud platform conditions, where routes, loads, and connections change dynamically, such differences become key for the stable operation of monitoring systems.

DISCUSSION

The development of approaches to anomaly monitoring in cloud environments demonstrates a steady transition from methods based on local features to architectures capable of capturing structural and temporal dependencies. The study by Al-Ghuwairi et al. [1] shows that classical ML models applied to a stream of metrics detect anomalies with high speed, but their resilience is limited due to the failure to account for the topology and dynamics of distributed systems. Such models work well on homogeneous network data; however, they are sensitive to the variability of cloud loads, flexible routing, and virtualization effects.

Additional limitations are noted in the work of Glavan et al. [3], which emphasizes that even incremental learning schemes are insufficiently adaptive when rare or short-term anomalies appear. Under conditions of high traffic flow variability, sequential architectures struggle to correctly interpret the interconnections between cloud nodes. Similar patterns are identified in the research by Shahzad et al. [8], where CNN and LSTM models demonstrate high accuracy on network datasets but lose effectiveness with increasing traffic structure complexity and the appearance of tunneling. This indicates a need for architectures capable of modeling temporal dynamics and interaction structures.

In response to these limitations, the scientific literature is increasingly focusing on methods capable of describing cloud environment topology. In the study by Mitropoulou et al. [5], it is noted that structural features improve model resilience when system component configurations change. A similar emphasis is present in Schummer et al. [7], where it was found that anomalies propagate through chains of node dependencies, meaning spatial relationships must be integrated into the learning process.

It is within this logic that the GCAD architecture, presented in the study by Zhang et al. [10], is developed. It is based on combining graph processing and a representation matching mechanism, which forms robust feature vectors even in the absence of labeling. As seen in Figure 1, modern approaches rely on the spatiotemporal integration of resources and topology.

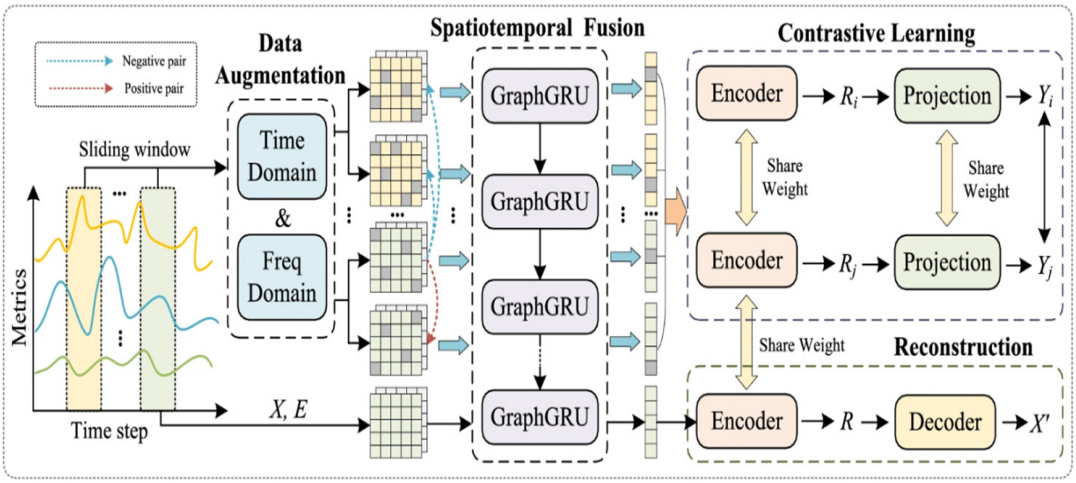

Figure 1. GCAD Architecture (Source: [10])

Virtual network environments create a qualitatively different context for anomaly detection compared to classical infrastructures. The main difficulty lies in the fact that traffic in the cloud ceases to be homogeneous. It is encapsulated in tunnels, reassembled, passes through service layers of virtualization, and changes structure depending on load or computing resource migration. These changes form distortions that completely violate the habitual assumptions of ML models regarding the form and distribution of features. Consequently, even robust architectures encounter situations where the system no longer provides data in a format similar to the training set.

VXLAN and GENEVE encapsulation exacerbates this problem by adding additional header layers and hiding part of the semantics of network behavior. Virtual headers absorb information about flow direction and interaction structure. The study by Spiekermann et al. [9] demonstrates that the reconfiguration of network paths and changes in packet structure lead to a significant decrease in the accuracy of models relying on packet sequence analysis.

Another source of limitation is related to temporal dynamics. Cloud systems generate irregular load fluctuations, short-term peaks, and periods of asymmetric resource distribution. These fluctuations are not fully-fledged anomalies, but their form is similar. The study by Al-Ghuwairi et al. [1] emphasizes that such states blur the boundaries between normality and violation.

Topology also acts as a critical factor. The structure of the cloud environment is dynamic. Nodes interact through virtual channels, processes migrate between servers, and connections change direction. In classical approaches, this dynamics is not reflected, as the model works only with local metrics. In the study by Mitropoulou et al. [5], it is noted that ignoring structural dependencies leads to a loss of context for network events and reduces the ability to capture system violations. Consequently, interpreting network behavior requires analyzing interaction schemes between nodes rather than individual packets. The situation is complicated by the fact that part of the network activity is hidden within service virtualization protocols. The research by Schummer et al. [7] shows that these hidden layers form "opaque zones" where traditional methods cannot observe state transitions. Therefore, the model works with a truncated picture of events and loses the ability to correctly correlate metrics.

These limitations explain the interest in architectures that account for the structure and dynamics of the environment. The study by Zhang et al. [10] proposes an approach that processes network dependencies as a graph structure and compares sequence representations through a contrastive mechanism. This transition is driven by the fact that virtual networks require the analysis of interconnections, not just the features of individual flows. Thus, the promise of graph models reflects a fundamental shift in understanding the nature of cloud anomalies.

CONCLUSION

The conducted analysis revealed that the efficacy of network anomaly detection in cloud platforms is determined by the choice of metrics and data, and primarily by model architecture. Classical ML approaches and ensembles maintain high accuracy on stable and well-described traffic sets; however, their resilience drops sharply with the appearance of virtualization, tunneling, and dynamic routing. Models relying solely on local features are bound to assumptions about packet structure that are systematically violated in a cloud environment.

Virtual networks with VXLAN and GENEVE encapsulation, virtual machine migration, and variable node topology form distribution shifts and zones of incomplete observability. Under these conditions, architectures focused only on packet sequences or static features lose the ability to reliably separate normality from anomalies, especially with short-term or weakly expressed violations.

Hybrid, graph-based, and contrastive models demonstrate higher resilience to cloud environment dynamics by accounting for topology, temporal dependencies, and the ability to learn with limited labeling. The inclusion of structural links between nodes and mechanisms for forming robust representations allows for better handling of distributed anomalies and complex load patterns. At the same time, limitations remain related to sensitivity to weak anomalies, architectural complexity, and high requirements for the quality of input representations. For sustainable progress in the field of anomaly monitoring, general benchmarks emulating VXLAN/GENEVE scenes and VM migrations are necessary, as well as jointly supported repositories with open datasets and method code (benchmark + open artifacts).

The practical conclusion is that the design of monitoring systems for cloud platforms must rely on architectures that explicitly account for virtualization, multilayer traffic structure, interaction topology, and temporal dynamics. Promising directions for development include the creation of unified benchmarks for virtual networks, the integration of graph and temporal modules, and the development of unsupervised methods and those using partially labeled data under conditions of incomplete observability. Such a shift in focus from local features to spatiotemporal and structural analysis defines the next phase in the evolution of ML approaches to anomaly monitoring in cloud environments.

REFERENCES

1. Al-Ghuwairi, A. R., Sharrab, Y., Al-Fraihat, D., & others. (2023). Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. Journal of Cloud Computing, 12, Article 127. https://doi.org/10.1186/s13677-023-00491-x
2. Devineni, S. K., Kathiriya, S., & Shende, A. (2023). Machine learning-powered anomaly detection: Enhancing data security and integrity. Journal of Artificial Intelligence &

Cloud Computing, 2(2), 1–9. https://doi.org/10.47363/JAICC/2023(2)184

3. Glavan, A., & Croitoru, V. (2023). Incremental learning for edge network intrusion detection. Revue Roumaine des Sciences Techniques – Série Électrotechnique et Énergétique, 68(3). https://doi.org/10.59277/RRST-EE.2023.3.9
4. Islam, M. S., Rakha, M. S., Pourmajidi, W., Sivaloganathan, J., Steinbacher, J., & Miranskyy, A. (2025). Anomaly detection in large-scale cloud systems: An industry case and dataset (arXiv Preprint No. 2411.09047v2). arXiv. https://arxiv.org/abs/2411.09047v2
5. Mitropoulou, K., Kokkinos, P., Soumplis, P., & others. (2024). Anomaly detection in cloud computing using knowledge graph embedding and machine learning mechanisms. Journal of Grid Computing, 22, Article 6. https://doi.org/10.1007/s10723-023-09727-1
6. Park, H., Shin, D., Park, C., Jang, J., & Shin, D. (2025). Unsupervised machine learning methods for anomaly detection in network packets. Electronics, 14(14), 2779. https://doi.org/10.3390/electronics14142779
7. Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., & Llorente, Á. (2024). Machine learning-based network anomaly detection: Design, implementation, and evaluation. AI, 5(4), 2967–2983. https://doi.org/10.3390/ai5040143
8. Shahzad, F., Mannan, A., Javed, A. R., & others. (2022). Cloud-based multiclass anomaly detection and categorization using ensemble learning. Journal of Cloud Computing, 11, Article 74. https://doi.org/10.1186/s13677-022-00329-y
9. Spiekermann, D., Eggendorfer, T., & Keller, J. (2024). Deep learning for network intrusion detection in virtual networks. Electronics, 13(18), 3617. https://doi.org/10.3390/electronics13183617
10. Zhang, Z., Zhu, Z., Xu, C., & others. (2025). Towards accurate anomaly detection for cloud systems via graph-enhanced contrastive learning. Complex & Intelligent Systems, 11(1), Article 23. https://doi.org/10.1007/s40747-024-01659-x