ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/sri-ramya-deevi/652

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 2 & Iss: 2

Research Article

Next-Generation Intrusion Detection with Gen AI in Dynamic Cloud Infrastructure

Sri Ramya Deevi*

Citation: Deevi SR. Next-Generation Intrusion Detection with Gen AI in Dynamic Cloud Infrastructure. *J Artif Intell Mach Learn & Data Sci 2024* 2(2), 3217-3221. DOI: doi.org/10.51219/JAIMLD/sri-ramya-deevi/652

Received: 02 November, 2024; **Accepted:** 18 November, 2024; **Published:** 20 November, 2024

***Corresponding author:** Sri Ramya Deevi, USA

ABSTRACT

Cloud computing has become the foundation of modern digital enterprises, offering agility, scalability and cost efficiency. At the same time, the dynamic, multi-tenant and ephemeral nature of cloud infrastructure has introduced new security challenges. Traditional intrusion detection systems (IDS), primarily signature- or anomaly-based, struggle to adapt to these evolving environments and often fail to detect advanced persistent threats, zero-day exploits and insider-driven anomalies. This article examines how Generative Artificial Intelligence (Gen AI) can drive the next generation of IDS for dynamic cloud infrastructures. By leveraging large language models (LLMs) and generative adversarial networks (GANs), IDS can autonomously simulate diverse attack scenarios, enrich training datasets with synthetic samples and continuously refine detection models. This enables real-time, context-aware and adaptive defense mechanisms capable of responding to multi-vector intrusions across hybrid and multi-cloud systems.

The proposed Gen AI driven IDS framework integrates seamlessly with DevSecOps pipelines, enhancing proactive monitoring, automated mitigation and policy enforcement while reducing false positives. Key benefits include improved resilience, adaptability and predictive defense capabilities. Nonetheless, challenges remain in explainability, adversarial robustness, resource efficiency and regulatory compliance. This research outlines a roadmap for deploying Gen AI enabled IDS, positioning it as a cornerstone for building secure, resilient and intelligent next-generation cloud infrastructures.

Keywords: Intrusion Detection Systems (IDS), Generative Artificial Intelligence (Gen AI), Large Language Models (LLMs), Generative Adversarial Networks (GANs).

1. Introduction

Cloud computing has become the backbone of digital transformation, enabling organizations to achieve unprecedented scalability, flexibility and cost efficiency. Enterprises increasingly rely on cloud-native applications, containerized workloads and multi-cloud strategies to meet dynamic business demands. This evolution has also expanded the attack surface, introducing new complexities in securing highly distributed, elastic and ephemeral environments. Traditional intrusion detection systems (IDS), whether signature-based or anomaly-based, are often ill-suited for these conditions, as they struggle to adapt to the high variability and scale of modern cloud infrastructures[1].

Recent advances in Artificial Intelligence (AI), particularly machine learning, have improved anomaly detection and predictive defense. Yet, conventional machine learning methods face challenges in addressing zero-day exploits, insider threats and adversarial manipulation due to limited training data and static learning models. Generative Artificial Intelligence (Gen AI), encompassing large language models (LLMs) and generative adversarial networks (GANs), offers a transformative approach by enabling the synthesis of realistic attack scenarios, dynamic behavioral modeling and adaptive detection mechanisms. Such capabilities make Gen AI a promising candidate for enhancing IDS resilience in complex cloud ecosystems[2]. This paper explores how Gen AI can revolutionize intrusion detection in dynamic cloud environments. I propose a Gen AI-driven IDS framework, analyze its applications and limitations and present a roadmap for its integration into hybrid and multi-cloud infrastructures to ensure intelligent, proactive and trustworthy cybersecurity.

2. Literature Review

Intrusion Detection Systems (IDS) have evolved considerably over the past two decades, transitioning from signature-based detection toward anomaly-based and machine learning (ML)-driven approaches. Signature-based IDS, such as Snort and Suricata, remain effective for known threats but are inadequate against polymorphic malware and zero-day exploits due to their reliance on static rule sets[3]. Anomaly-based systems improved detection of previously unseen threats by modeling normal behavior, yet these approaches suffer from high false-positive rates in dynamic and heterogeneous environments such as cloud infrastructures.

The introduction of ML techniques significantly enhanced IDS capabilities by leveraging statistical learning, clustering and classification for anomaly detection. Approaches using support vector machines, random forests and deep learning architectures demonstrated higher detection accuracy across benchmark datasets like NSL-KDD and CICIDS2017[4]. These models often face challenges of data imbalance, lack of generalization across different cloud contexts and vulnerability to adversarial evasion attacks. The reliance on static training data limits their adaptability to ephemeral, multi-tenant and containerized workloads commonly found in modern cloud environments.

More recently research has explored generative models for cybersecurity applications. Generative Adversarial Networks (GANs) have been employed to create synthetic network traffic for IDS training, thereby addressing data scarcity and imbalance[5]. Large Language Models (LLMs) are emerging as tools for analyzing logs and contextual signals in real time, offering adaptive and context-aware insights. These advances highlight the potential of Generative AI to overcome limitations of traditional ML-based IDS and to serve as a foundation for next-generation cloud security architectures.

3. Role of Gen AI in Intrusion Detection

Generative Artificial Intelligence (Gen AI) has emerged as a powerful paradigm that extends beyond traditional machine learning by enabling systems to synthesize data, simulate attacks and adaptively refine detection models. Unlike conventional supervised approaches that rely heavily on labeled datasets, Gen AI techniques such as Large Language Models (LLMs) and Generative Adversarial Networks (GANs) allow IDS to dynamically evolve in response to novel and sophisticated cyber threats **(Figure 1)**.

One of the most significant contributions of Gen AI to IDS is its ability to generate synthetic data for training. Dynamic cloud infrastructures often lack comprehensive datasets that capture zero-day exploits, insider attacks or multi-vector intrusions. GANs can create realistic attack traffic that enhances the robustness of detection models by addressing data imbalance and augmenting underrepresented classes[5]. Reinforcement learning combined with generative modeling has been shown to improve adaptive defense mechanisms by simulating adversarial behavior[6]. LLMs provide context-aware analysis by processing heterogeneous data sources such as logs, configurations and network telemetry.

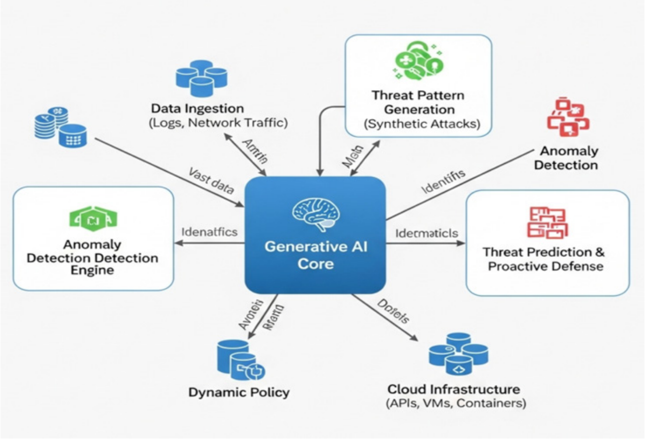

Figure 1: Gen AI in Intrusion Detection.

Recent studies demonstrate that LLMs can detect subtle anomalies, interpret sequences of events and recommend actionable responses with minimal human intervention[7]. This enables intrusion detection systems to shift from static monitoring toward intelligent, proactive security frameworks. Adversarial training using Gen AI strengthens IDS resilience against evasion attempts. By continuously exposing models to adversarially generated samples, systems can better anticipate evolving threat landscapes. This generative-adaptive cycle positions Gen AI as a cornerstone for next-generation IDS in highly dynamic, hybrid and multi-cloud environments[8].

4. Architecture of a Gen AI–Driven IDS for Cloud

The architecture of a Gen AI driven Intrusion Detection System (IDS) for cloud environments must be cloud-native, modular and highly scalable to accommodate dynamic workloads across multi-cloud and hybrid infrastructures. Unlike traditional IDS, which rely on fixed detection pipelines, a Gen AI enabled architecture integrates generative models into the core detection and response cycle, enabling adaptive learning and self-evolution.

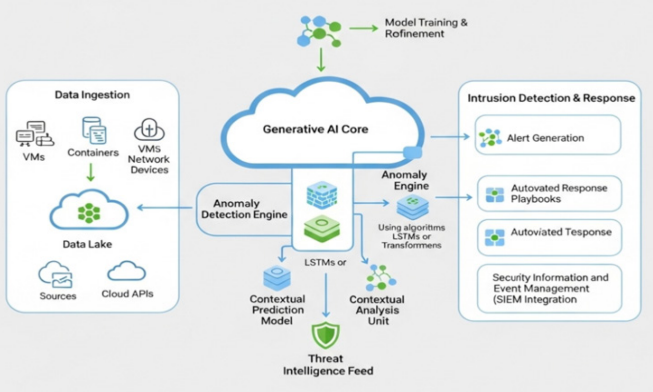

Figure 2: Architecture of a Gen AI–Driven IDS for Cloud.

The Data Collection Layer aggregates heterogeneous inputs including network traffic, application logs, container telemetry and API traces from distributed sources. Cloud-native monitoring tools such as Kubernetes audit logs and service mesh telemetry enhance visibility in microservices-based deployments[9]. The Gen AI Analysis Engine forms the intelligence layer of the architecture. It incorporates LLMs for contextual log analysis and GANs for synthetic threat simulation and adversarial training.

This dual approach improves anomaly detection accuracy and equips the IDS to handle zero-day exploits and insider threats. Reinforcement learning modules dynamically refine detection policies by continuously adapting to evolving attack patterns[10].

The Adaptive Response Module operationalizes findings from the analysis engine, automating mitigation actions such as dynamic access control, network segmentation or workload isolation. Integration with Security Orchestration, Automation and Response (SOAR) platforms enhances incident response efficiency[11].

The architecture supports seamless deployment within DevSecOps pipelines, ensuring continuous security monitoring across CI/CD workflows. Containerized microservices enable scalability, while federated learning provides privacy-preserving collaboration between distributed IDS nodes in multi-cloud ecosystems[12].

5. Use Cases and Applications

The integration of Generative AI into Intrusion Detection Systems (IDS) enables a wide spectrum of practical applications in dynamic cloud environments. These use cases demonstrate how Gen AI enhances adaptability, resilience and predictive defense against modern cyber threats **(Figure 3)**.

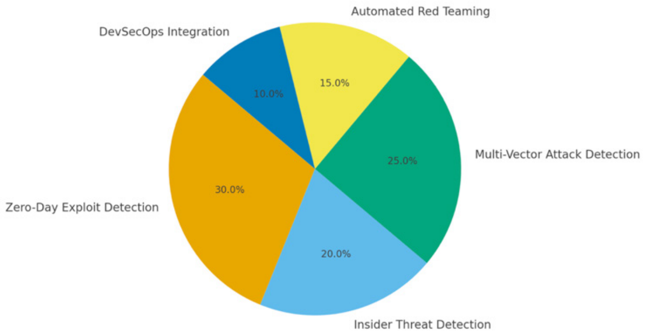

Figure 3: Distribution of Use Cases for Gen AI–Driven IDS in Cloud.

5.1. Real-time detection of zero-day exploits

One of the most significant challenges in cloud security is the detection of zero-day vulnerabilities. Gen AI models can simulate unseen attack vectors and generate synthetic exploit patterns to train IDS engines. Studies have shown that GAN-based models significantly improve detection rates of previously unknown attacks compared to conventional anomaly detection methods[5].

5.2. Insider threat detection

Insider attacks remain difficult to identify due to their subtle and context-driven nature. By leveraging Large Language Models (LLMs), IDS can analyze logs, user activity and communication patterns to detect anomalies indicative of privilege misuse or data exfiltration[7]. Context-aware analysis ensures lower false positives while capturing complex behavioral deviations.

5.3. Multi-vector attack detection across clouds

Cloud workloads frequently span hybrid and multi-cloud infrastructures, making them susceptible to distributed and coordinated attacks. Gen AI enables IDS to correlate heterogeneous telemetry data and simulate complex multi-vector attacks, enhancing detection accuracy across distributed environments[13].

5.4. Automated red teaming and threat simulation

Generative models can automatically generate attack scenarios that mimic adversarial tactics, techniques and procedures (TTPs). This capability not only strengthens IDS training but also supports proactive red teaming for continuous security validation[14].

5.5. Integration with DevSecOps pipelines

Cloud-native organizations require continuous monitoring integrated into CI/CD workflows. Gen AI–driven IDS can provide adaptive policy updates, synthetic test cases and automated feedback loops for DevSecOps pipelines, ensuring that evolving applications are resilient against emerging threats[12].

6. Evaluation and Performance Considerations

Evaluating the effectiveness of a Gen AI driven Intrusion Detection System (IDS) in dynamic cloud infrastructures requires a comprehensive approach that balances detection accuracy, scalability, latency and resilience. Unlike traditional IDS, performance metrics must account not only for precision and recall but also for adaptability to ephemeral cloud workloads, adversarial robustness and integration overhead.

6.1. Detection accuracy and false alarms

A key benchmark in IDS evaluation is the ability to maximize true positives while minimizing false positives and false negatives. Prior studies highlight that GAN-based IDS models significantly improve detection of minority-class intrusions while reducing false alarm rates[14]. Achieving high precision remains challenging in heterogeneous cloud workloads, where benign anomalies may be misclassified as threats.

6.2. Latency and scalability

Cloud-native IDS must operate in near real time without introducing bottlenecks. Deep learning and generative models often require substantial computational resources, which may increase detection latency. Research demonstrates that lightweight deep architectures and distributed deployments can mitigate these issues, enabling IDS to scale across hybrid and multi-cloud infrastructures[15].

6.3. Adversarial robustness

Gen AI introduces unique evaluation dimensions, particularly resilience against adversarial attacks. Adversarially crafted traffic can manipulate detection thresholds, necessitating continuous adversarial training and robust testing frameworks[8].

6.4. Cost-performance trade-offs

The overhead of deploying Gen AI models must be weighed against operational efficiency. Techniques such as federated learning and model compression reduce computational costs while preserving detection accuracy, making large-scale deployments viable[12].

7. Challenges and Limitations

While Generative AI offers transformative capabilities for Intrusion Detection Systems (IDS), its adoption in dynamic cloud infrastructures is accompanied by several challenges and limitations that must be critically examined.

7.1. Interpretability and explainability

One of the foremost challenges lies in the black-box nature of generative models. Although LLMs and GANs can enhance detection accuracy, their decision-making processes are often opaque, making it difficult for security analysts to validate or trust their outputs[16]. Lack of interpretability hinders compliance with regulatory frameworks and slows incident response.

7.2. Adversarial vulnerabilities

Gen AI models themselves are susceptible to adversarial manipulation. Attackers can craft malicious inputs to evade detection or poison training datasets, thereby reducing IDS reliability. Research has shown that adversarial examples can drastically degrade the performance of deep IDS models, necessitating robust adversarial training and continuous validation mechanisms[17].

7.3. Resource overhead and deployment complexity

Deploying Gen AI–driven IDS at scale introduces substantial computational and storage demands. High-throughput cloud environments generate vast volumes of data and running real-time generative analysis can lead to latency and cost inefficiencies. Techniques such as model compression, distributed inference and edge-assisted detection have been proposed, but challenges remain in balancing performance with efficiency[18].

8. Future Directions

The integration of Generative AI into Intrusion Detection Systems (IDS) for dynamic cloud environments is still in its early stages. As the technology matures, several future directions can guide research and practical adoption.

8.1. Federated and collaborative learning

A promising avenue is the adoption of federated learning techniques to train IDS across multiple organizations or cloud tenants without directly sharing sensitive data. This approach can enhance detection accuracy while preserving privacy, making large-scale collaborative defense feasible in multi-cloud environments.

8.2. Explainable and trustworthy AI

As interpretability remains a barrier to operational deployment, research on explainable AI (XAI) methods tailored to Gen AI-driven IDS will be critical. Future systems must provide human-understandable reasoning behind alerts, supporting compliance with regulatory requirements and increasing analyst trust.

8.3. Reinforcement learning for adaptive defense

Incorporating reinforcement learning alongside generative models could enable IDS to not only detect but also autonomously adapt mitigation strategies in real time. This self-learning loop would allow systems to evolve defense mechanisms dynamically in response to new attack vectors.

8.4. Integration with broader security ecosystems

Next-generation IDS will likely become a component of larger cybersecurity ecosystems, integrated with Security Information and Event Management (SIEM) systems, SOAR platforms and threat intelligence feeds. Such integration will foster end-to-end situational awareness and proactive defense.

9. Conclusion

The dynamic and distributed nature of modern cloud infrastructures has rendered traditional Intrusion Detection Systems (IDS) increasingly inadequate. Static, signature-based and even conventional anomaly detection methods often fail to keep pace with ephemeral workloads, zero-day exploits, insider threats and adversarial attacks. This article has explored how Generative Artificial Intelligence (Gen AI) encompassing Generative Adversarial Networks (GANs), Large Language Models (LLMs) and reinforcement learning can drive the development of next-generation IDS tailored for cloud environments. The proposed Gen AI driven IDS architecture integrates cloud-native telemetry collection, generative threat modeling and adaptive response mechanisms. Through its ability to simulate diverse attack scenarios, enrich datasets and continuously refine detection models, Gen AI enables IDS to operate proactively rather than reactively. Use cases such as zero-day detection, insider threat monitoring, multi-vector attack analysis and automated red teaming demonstrate its potential to strengthen resilience across hybrid and multi-cloud deployments.

Despite these advancements, significant challenges remain. Issues of interpretability, adversarial robustness and computational overhead must be addressed before Gen AI enabled IDS can achieve widespread adoption in mission-critical environments. Future directions including federated learning, explainable AI and integration with broader security ecosystems highlight the pathway toward scalable and trustworthy implementations. Generative AI represents a transformative shift in intrusion detection, bridging the gap between static defenses and adaptive, intelligent security. By embedding Gen AI into IDS frameworks organizations can move toward resilient, proactive and context-aware cybersecurity, establishing a foundation for secure digital ecosystems in the era of dynamic cloud infrastructure.

10. References

1. Khraisat A, Gondal I, Vamplew P, et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2019;2: 1-22.
2. Papernot N, McDaniel P, Sinha A, et al. SoK: Security and privacy in machine learning. IEEE European Symposium on Security and Privacy (EuroS&P), 2018: 399-414.
3. Roesch M. Snort - lightweight intrusion detection for networks. 13th USENIX Conf. on System Administration (LISA), 1999: 229-238.
4. Shone N, Ngoc TN, Phai VD, et al. A deep learning approach to network intrusion detection. IEEE Trans. Emerging Topics in Computational Intelligence, 2018;2: 41-50.
5. Lin H, Ye Y, Xu T. IDS-GAN: Generative adversarial networks for attack generation against intrusion detection. IEEE Int. Conf. Communications (ICC), 2020: 1-6.
6. Zhang J, Chen B, Xiang Y, et al. Adversarial reinforcement learning for adaptive cyber defense. IEEE Trans. Network and Service Management, 2021;18: 2160-2175.
7. Garg S, Hu J orgun MA. Context-aware intrusion detection using large language models. IEEE Int Conf Dependable. Autonomic and Secure Computing (DASC), 2023: 345-352.
8. Nguyen HT, Reddi K. Adversarial machine learning in network intrusion detection: A survey. ACM Computing Surveys, 2023;55: 1-36.
9. Modi C, Patel D, Borisaniya B, et al. A survey on security issues and solutions at different layers of Cloud computing. J Supercomputing, 2013;63: 561-592.

10. Zhang J, Chen B, Xiang Y, et al. Adversarial reinforcement learning for adaptive cyber defense. IEEE Trans. Network and Service Management, 2021;18: 2160-2175.
11. Scarfone K, Mell P. Guide to intrusion detection and prevention systems (IDPS). NIST Special Publication, 2007: 800-894.
12. Qu Y, Li W, Hu C. Privacy-preserving federated learning for cyber intrusion detection in cloud environments. Future Generation Computer Systems, 2022;128: 175-184.
13. Fadlullah ZM, Tang F, Mao B, et al. State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems. IEEE Commun. Surveys & Tutorials, 2017;19: 2432-2455.
14. Ferdowsi A, Saad W. Generative adversarial networks for distributed intrusion detection in the Internet of Things. IEEE Global Communications Conf (GLOBECOM), 2019: 1-6.
15. Xin Y, Kong L, Liu Z, et al. Machine learning and deep learning methods for cybersecurity. IEEE Access, 2018;6: 35365-35381.
16. Molnar C. Interpretable Machine Learning: A Guide for Making Black Box Models Explainable, 2nd ed. Independently published, 2022.
17. Goodfellow IJ, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. Int Conf Learning Representations (ICLR), 2015: 1-11.
18. Xie Z, Deng RH, Guo S. et al. Resource-efficient federated learning for intrusion detection in cloud environments. Cloud Computing, 2023;11: 2200-2215.